© 2019 IJSRSET | Volume 6 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET1962141

Different Types of Attacks and Performance Evaluation Factors in Digital Audio Watermarking

Krunalkumar N. Patel
Department of Computer Science and Engineering, Madhuben & Bhanubhai Patel Women ICT College, New Vallabh Vidhyanagar, Gujarat, India
* Corresponding Author: krunalpatel10287@gmail.com

ABSTRACT

The 21st century is the digital world, the utilization of digital information like multimedia that contains image, audio and video is massively expanding because of the progression in innovation and web transformation. With this headway to achieve the one's proprietorship and copyrights for this advanced information is the greatest test. Digital watermarking is one of the procedures to accomplish one's proprietorship and copyrights with safely and securely. Digital watermarking is the strategy in which the proprietor's copyright data can be installed into the original media either as an image, audio or video. There are two fundamental components we have to consider for this digital audio watermarking to get the high robustness and also imperceptibility against the piracy, malevolent assaults, and different kind of transformation attacks. Despite the fact that there are numerous difficulties to accomplish these outcomes, in this paper, our proposed audio watermarking system is utilized to enhance the robustness, reliability and imperceptibility of the embedded data with security. For Security, in our proposed work we are utilizing DSSS encryption algorithm and some vital transformation techniques utilized that are DWT (Discreet Wavelet Transformation) up to 4-level to get most reduced frequency sub-band and after that DFT(Discrete Fourier Transform) is applied to get least frequency component from sub-band found by DWT in which the alterations are done and after that SVD (Singular esteem Decomposition)is used to it, so unique audio document does not have any effect of watermark bits to improve robustness and imperceptibility. This algorithm is implemented in MATLAB software that is used for numerical computation and data analysis. The GUI is presented in this paper for audio watermarking with different calculations.

Keywords : Digital Audio watermarking, DWT, DFT, SVD, DSSS, watermark embedding and extraction, robustness, imperceptibilty, SNR,BER.

I. INTRODUCTION

In the previous couple of years, a need has emerged for ensuring copyright responsibility for media. Intense and low-cost PCs enable individuals to effectively make and duplicate interactive media content, and the Internet has made it conceivable to disperse this data requiring little to no effort. However, these empowering advancements likewise make it simple to unlawfully duplicate, change, and redistribute sight and sound information without respect for copyright proprietorship. An ongoing case of this issue is the discussion with respect to robbery of high-quality music over the Web [1].

Due to this the gigantic utilization of online asset sharing and getting to which may incorporate duplicating and downloading. Today, the sharing of audio files and video documents over the web is getting to be simpler in everyday life. By thinking about these specific situations, securing the scholarly assets privileges of such advanced neutralizes malignant client assaults and piracy has turned into a sweltering observation point that requires basic arrangements. A standout amongst the most encouraging methodology that has genuinely pulled in a considerable lot of the specialists as of late is digital watermarking [2]. In prior days it was hazardous to transmit the genuine computerized data safely, yet after that some conventional strategies like cryptography and steganography are found to achieve this protected encompassing. Stenography techniques are not robust against different assaults or adjustment of information that may happen during transmission. Before this strategy's individuals were utilizing undetectable ink idea with composing data, blending two pictures to make another one to conceal the data, drawing a standard painting with some little alterations, shearing the header data of the delegate as a message and so forth. [3]. Stenography endeavors to achieve an unexpected objective in comparison to that of cryptography. While cryptographic plans endeavor to limit the interpretation of an encoded message, which is possibly sent over an open correspondences channel to confided in parties, stenography procedures endeavor to conceal data inside a generally harmless signal, for example, a picture or sound. One of the essential employments of stenography is watermarking, which attempts to ensure the nearness of some concealed data in a cover motion without bringing discernible bending into the cover signal [4]. Cryptography is utilized to secure the critical data which will be exchanged, nonetheless, there is a disadvantage of this strategy is before the information is encoded it is elusive where the adjustment of the data has been finished [5]. Today, with fast development of sharing and getting to the data over the web numerous applications like recorded audio files and sharing of music files, they are not considering copyright assurance issue habitually because of its multifaceted nature. Yet, in the wake of considering this copyright infringement issues advanced watermarking approach turns into the most encouraging arrangement contrasted with cryptographic and stenography forms, against the treating and adjustment of intellectual belongings [5]-[6]. When contrasted with image and video watermarking, audio watermarking techniques are difficult because of Human Auditory System (HAS) is touchier than Human Visual System (HVS) [7]. Because of low sampling frequency, a little measure of commotion in HAS framework can be distinguished by ear. It is an extremely famous research region in digital media information stowing away [8]. Audio watermarking is additionally testing at that point image and video watermarking in light of the fact that hearing capacity is touchier then visual guide of human as per. Thus, audio watermarking strategy turns out to be most prominent procedure than image and video watermarking to secure scholarly possessions like sharing on the web music, chronicles over the web [9]. In addition, we can embed less amount of data in audio watermarking [10]. Rest of the paper is organized as follows, Section I contains the introduction of the watermarking techniques, Section II contain the related work of various digital audio watermarking techniques, Section III contains the methodology proposed in this research work with flow diagrams, Section IV describes results and discussion with various comparisons, Section V concludes research work with future directions.

II. AUDIO WATERMARKING

Digital watermarking needs to install bits of data into a digital media for ensuring it against copyright violations and other unapproved applications. Digital audio watermarking needs to do with securing digital audio document against illicit replicating. A great deal of works has been done on digital watermarking of different media such as image and video, yet this

specific survey will center around digital watermarking of audio record. Digital audio documents are especially the most manhandled for copyright violations since they can be downloaded and duplicated easily.

Digital audio watermarks are uncommon signals inserted into digital audio signals. These signals are separated by recognition mechanisms furthermore, decoded. Audio watermarking algorithms are depending on the imperfection of the human auditory system. Nonetheless, human ear is significantly more delicate than other tangible engines. In this way, great audio watermarking algorithms are hard to outline [11].

Digital audio watermarking is a method that implants data with particular importance into the host media without noticeable impedance to the original quality. As a supplement to ordinary encryption procedures, watermarking gives great devices to ensuring the copyright of audio files and has turn into a functioning examination territory lately. Other than being unclear to human ears, the watermark should likewise have the capacity to withstand audio signal preparing and time-space synchronization assaults [12]. There are numerous difficulties to information covering up in audio. The watermark does not have any mutilation; it ought to be discernable, must be powerful to signal processing and not evacuated by assaults.

III. WORKING PRINCIPLE OF DIGITAL AUDIO WATERMARKING

Here, in this section we are going to discuss basic working process of digital watermarking. Digital watermarking contains mainly two steps.

1. Watermark Embedding Process
2. Watermark Extraction Process

A. Watermark Embedding Process

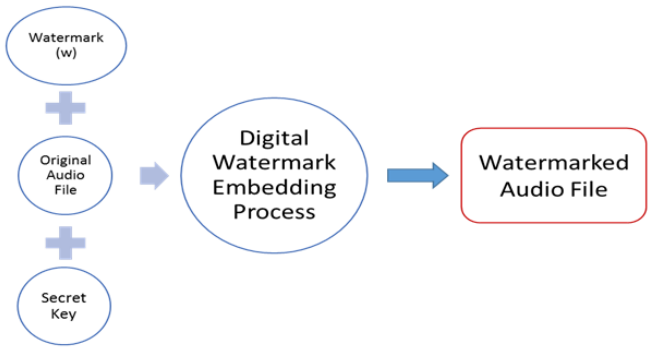

Fig. 1. Watermark Embedding Process

First step is watermark embedding and Second step is watermark extraction. In watermark embedding process the watermark data that may be any text or image is embedded in the original data. For increasing the security of the content security key is also embedded with it for unauthorized access by third parties. By combining all this watermark embedding process is carried out. The basic watermark embedding process is depicted in the figure 1.

Fig. 2. Watermark Extraction Process

Now, for the watermark extraction process the above generated watermarked data is used as an input and the secret key is used for the authentication. After that successfully we can extract the watermark data by digital watermark extraction process. The basic watermark process is depicted in the figure 2.

IV. PERFORMANCE EVALUATION FACTORS

Any efficient audio watermarking should meet the desired requirements like robustness, security and perceptibility with accurate information [13]- [14]. Here each term has their specific meaning to fulfill the objective of desired results. The first objective is robustness refers to where original content is not to

be altered under different attacks and tempering of original media. In addition, the watermark detecting rate should be high to prove the ownership [15] [16]. Second perceptibility refers to quality must be maintained against various distortion means the signal to noise ratio must be maintained within the desirable range and modified signal must not be captured by human [17]- [18]. Lastly, security is the main concern of copyright content that must be fulfil with accuracy [19].

To check robustness and perceptual transparency we can use Signal-to-noise ratio (SNR), Robustness ( ), Bit Error Rate (BER).

A. Signal-to-noise ratio

SNR is a statistical difference metric which is used to measure the similitude between the undistorted original audio signal and the distorted watermarked audio signal. The SNR computation is done according to Eq. (1), where A corresponds to the original signal, and A' corresponds to the watermarked signal.

Although SNR is a simple metric to measure the noise introduced by the embedded watermark and can give a general idea of imperceptibility, it does not take into account the specific characteristics of the human auditory system.

$$\mathrm{SNR(dB)} = 10\log_{10}\frac{\sum_n An2}{\sum_n (An - A'n)2} \qquad (1)$$

B. Robustness

Watermarked audio digital signals may undergo common signal processing operations such as linear filtering, lossy compression, among many others. Although these operations may not affect the perceived quality of the host signal, they may corrupt the watermark image embedded within the signal. To evaluate robustness of the proposed algorithm, we implemented a set of attacks that commonly affect audio signals. Most of these attacks have been defined:

$$r(\hat{w}, \hat{w}) = \frac{\sum_1^n w_i \hat{w}}{\sqrt{\sum_{i=1}^n w_i^2 \sum_{i=1}^n \hat{w}^2}} \qquad (2)$$

C. Bit Error Rate

Robustness is measured using the bit error rate (BER) metric since the watermark used in the simulation is a binary image. BER is defined as the ratio of incorrect extracted bits to the total amount of embedded bits, as expressed in Equation:

$$\mathrm{BER} = \frac{100}{l}\sum_{n=0}^{i-1}\begin{Bmatrix}1, W'n = Wn\\ 0, W'n \neq Wn\end{Bmatrix} \qquad (3)$$

where l is the watermark length, Wn is the nth bit of the embedded watermark, and W'n is the nth bit of the extracted watermark. Reliability is measured using BER (bit error rate).

D. Security

Security can be utilized as verification and substance uprightness components in an assortment of ways. This suggests the watermark is an anchored connect meaningful just by authorized people with the learning about the secrecy. Watermark security alludes to the powerlessness by unapproved clients to approach the crude watermarking channel.

E. Computational complexity

This alludes to the processing required to insert information into the host signal or potentially to extricate information from the signal. A disclosure of strategy to fulfill these limitations will prompt a method for ensuring digital audio. Algorithm complexity is essential to know, for it might impact the decision of execution structure.

V. DIFFERENT TYPES OF ATTACKS

The fundamental necessities of a capable watermarking algorithms are the robustness and imperceptibility. There is a tradeoff between these two necessities; regardless, by testing the watermark algorithm with the audio signal handling attacks that

opening can be made unimportant. Every application has its specific requirements, and gives a contrasting option to pick high quality reimbursing with the idea of the signal and a different way. Without any progressions and attacks each watermarking technique performs profitably. Likely the most broadly perceived sorts of systems an audio signal encounters when transmitted through a medium are according to the accompanying [20] [21] [22].

A. Noise

It is normal practice to see the nearness of noise in a signal when transmitted. Henceforth, watermarking algorithm should make the system strong against the commotion assaults. It is prescribed to check the calculation for this kind of noise by including the host signal by an additive white Gaussian noise (AWGN) to check its robustness.

B. Cropping attack

Cropping is another technique that might be utilized by an enemy to change the perspective proportion without extending the signal or filling the clear spaces. An editing assault may influence the watermark with little change to the cover audio. That is relying upon the watermark strategy and its power. The cropping might be executed on some portion of the original signal. The editing assault expels a few segments of the watermarked picture, decreasing the extent of the host signal, which may make a portion of the shrouded data be lost. It is significant that editing additionally causes a synchronization issue for information concealing plans.

C. Dynamics:

The amplitude change and the attenuation change are the progression of the assaults. capacity, expansion and compression are a type of more convoluted applications which are the non-direct adjustments. A portion of these sorts of assaults are re-quantization

D. Amplify

The watermarked audio is intensified at various enhancement rate. Through this assault the watermarking plans that install the watermark in the adequacy of the individual examples ends up powerless as the amplitude is adjusted.

E. Filtering:

Filtering is common practice, which is used to amplify or attenuate some part of the signal. The basic low pass and high pass filters can be used to achieve these types of attacks.

F. Adding Echo

Echoes with various deferrals are added to the watermarked audios. This assault fundamentally is the counter for echo addition conspires that includes the watermark bit as echoes with various deferrals.

G. Ambience:

In a few circumstances the audio signal gets deferred or there are circumstances where in individual's record motion from a source and claim that the track is theirs. Those circumstances can be mimicked in a room, which is of incredible significance to check the execution of an audio signal.

H. Removal Attack:

Removal assaults expect to expel the watermark information from the watermarked audio signal. Such assaults misuse the way that the watermark is typically an added additive noise signal introduce in the host signal.

VI. APPPICATIONS OF AUDIO WATERMARKING

Watermarking systems can be to a great degree accommodating in a couple of domains of interest. The requirements that a watermarking system needs to comply with depends on the specific sort of utilization. As per that there is some regular utilization of this are as per the following concurring to [23] [24] [25].

A. Copyright protection

The proprietor identification can be composed on the spreads or said some place on the protest. For instance, a music companies turns out with its CD/DVD by the recognizable proof characteristic of a sound organization on the CD case or the sign of the paper maker on top corner of the paper. These sorts of watermarks can be essentially isolated by picking the picture or by tearing the part that has the recognizable proof. Computerized watermarking encourages to crush this issue by embedding the watermark as bits and shaping a fundamental piece of the substance.

B. Authentication

Digital information can be watermarked to show that the computerized content can't be unlawfully repeated. Devices equipped for replication would then be able to identify such watermarks and anticipate unapproved replication of the substance.

C. Tamper proofing

In this application digital watermark data is inserted in the original signal and can be utilized to check if the original signal is altered. This circumstance is essential since it is important to think about the altering caused to the audio signal. The altering is at some point a reason for manufacturing of the watermark which must be stayed away from. If the watermark extracted is used for authentication of the original content.

D. Broadcast monitoring

It is imperative for creation organizations to counteract illicit rebroadcasting exercises. For this situation, digital watermarks can be utilized to naturally screen broadcasting streams at satellite hubs everywhere throughout the world and distinguish any unlawful communicate material. Also, numerous associations are keen on secure techniques for getting the greater part of the broadcast appointment they buy from supporters. Procedures for registering can be ordered with two sorts: inactive checking that endeavors to specifically perceive the substance being communicated, and dynamic observing which depends on related data that is communicated alongside the substance.

E. Finger printing

A fingerprinting strategy for the most part used to delineate the wellspring of unlawful duplicate. Each duplicate accessible can be watermarked with a solitary piece grouping. For the proprietor, embedding a novel serial number-like watermark is a fine method to detect clients who break their permit assertion by duplicating the ensured information and providing it to an outsider.

F. Media forensics

In forensic watermark applications upgrade a substance proprietor's capacity to identify and react to abuse of its advantages. Measurable watermarking is utilized to assemble prove for criminal procedures, as well as to uphold authoritative use assent ions between a substance proprietor and the general population or organizations with which it shares its substance.

G. Medical application

In this watermarking strategy, the names of the patients can be imprinted on the X-ray reports and MRI examines. The medical reports assume an extremely critical part in the treatment offered to the patient. In the event that there is a misunderstanding in the reports of two patients this could prompt a disaster. Consequently, embedding the date and patient's name in X-ray or MRI pictures could expand the secrecy of restorative data and also the security.

H. Picture authentication

In a picture verification application, the expectation is to identify adjustments to the information. The qualities of the picture, for example, its edges, are installed and contrasted and the present pictures for contrasts. An answer for this issue could be acquired from cryptography, where advanced mark has been

examined as a message verification strategy. One case of computerized signature innovation being utilized for picture validation is the reliable advanced camera.

I. Airline traffic monitoring

Watermarking is utilized as a part of air movement observing. The pilot speaks with a ground observing framework through voice at a specific frequency. In any case, it can be effectively caught and assaulted, and is one of the reasons for miss correspondence. To maintain a strategic distance from such issues, the flight number is installed into the voice correspondence between the ground administrator and the flight pilot. As the flight numbers are one of a kind the following of flights will turn out to be more secure and simple.

J. Communication of ownership

Computerized content keeps on multiplying as the present customers look for data and diversion on their PCs, cell phones and other advanced gadgets. In our digital culture, advanced has turned into an essential method for correspondence and articulation. The mix of access and new apparatuses empowers advanced substance to movement speedier and more remote than any time in recent memory as it is transferred, scattered, seen, downloaded, altered and re purposed at amazing velocity. Regardless of whether you are a worldwide media partnership or an independent picture taker, the capacity to convey your copyright possession and use rights is basic.

VII. CONCLUSION AND FUTURE SCOPE

Numerous strategies have been proposed for audio watermarking, the power of a watermark relies upon the method utilized, audio and the signal processing activities. The diverse plans have favorable circumstances and burdens. There are two principal issues in audio watermarking: First is robustness and other is imperceptibility. The watermarking scheme relies upon the sort of utilization. We have exhibited a diagram about various audio watermarking systems also, applications for Audio Watermarking. In last also the calculated robustness values for different music types after applying the different attacks have been shown. The results show that after applying the different malicious attacks still we got the high robustness values under different circumstances. And we have recovered the watermark with o bit error rate.

VIII. REFERENCES

[1]. H. J. Kim, Y. H. Choi, J. W. Seok, and J. W. Hong, Audio watermarking techniques, ser. Innovative Intelligence. World Scientific Publishing Co., 2004, vol. 7 (Intelligent Watermarking Techniques), ch. 8, pp. 185–218.

[2]. J. C. Davis, “Protecting intellectual property in cyberspace,” IEEE Technology and Society Magazine, vol. 17, no. 2, pp. 12 – 25, Summer 1998.

[3]. Johnson, N. F., & Katzenbeisser, S. C., “A survey of steganographic techniques”, F. A. P. Petitcolas & S. Katzenbeisser (Eds.), Information hiding: Techniques for steganography and digital watermarking (1 ed., pp. 43-78), 2000.

[4]. P. Dutta, D. Bhattacharyya, and T. Kim, “Data Hiding in Audio Signal: A Review,” in International Journal of Database Theory and Application, vol. 2, no. 2, June 2009.

[5]. Arnold, M., “Audio watermarking: features, applications and algorithms”, IEEE International Conference Multimedia and Expo, vol. 2, pp. 1013- 1016, 2000.

[6]. Natgunanathan, I., Xiang, Y., Rong, Y., Zhou, W. and Guo, S. (2012) Robust Patchwork-Based Embedding and Decoding Scheme for Digital Audio Watermarking. IEEE Transactions on Audio, Speech, and Language Processing, 20, 2232-2239.

[7]. Elshazly, A. R., M. M. Fouad, and M. E. Nasr. "Secure and robust high quality DWT domain audio watermarking algorithm with binary image." Computer Engineering & Systems

(ICCES), 2012 Seventh International Conference on. IEEE, 2012.

[8]. He, X. (2008) Watermarking in Audio: Key Techniques and Technologies. Cambria Press, Youngstown.

[9]. Himeur Yassine, Boudraa Bachir, Khelalef Aziz "A Secure and High Robust Audio Watermarking System for Copyright Protection" International Journal of Computer Applications (0975 – 8887) Volume 53– No.17, September 2012, pp.33-39.

[10]. Seitz, J. (2005) Digital Watermarking for Digital Media. Information Science, Hershey.

[11]. Ms. Komal V. Goenka, "Overview of Audio Watermarking Techniques", Volume 2, Issue 2, February 2012.

[12]. Wei Li, Xiangyang Xue, and Peizhong Lu,"Localized Audio Watermarking Technique Robust Against Time-Scale Modification", VOL.8, NO. 1, FEBRUARY 2006.

[13]. Ai, H., Liu, Q. and Jiang, X. (2013) Synchronization Audio Watermarking Algorithm Based on DCT and DWT. Proceedings of IEEE Conference Anthology, Shanghai, 1-8 January 2013, 1-4.

[14]. Can, Y.S. and Alagoz, F. (2013) Robust Frequency Hopping and Direct Sequence Spread Spectrum Audio Watermarking Technique on Wavelet Domain. Proceedings of 2013 International Conference on Electronics, Computer and Computation (ICECCO), Ankara, 7-9 November 2013, 382-385.

[15]. Dhar, P.K. and Shimamura, T. (2013) Entropy-Based Audio Watermarking Using Singular Value Decomposition and Log-Polar Transformation. Proceedings of 2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), Columbus, 4-7 August 2013, 1224-1227.

[16]. Shahriar, M.R., Cho, S. and Chong, U. (2012) Time-Domain Audio Watermarking Using Multiple Marking Spaces. Proceedings of 2012 International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, 18-19 May 2012, 974-979.

[17]. Cvejic, N. and Seppänen, T. (2008) Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks. IGI Global Snippet, Hershey.

[18]. Lei, B.Y., Soon, I.Y. and Tan, E.-L. (2013) Robust SVD-Based Audio Watermarking Scheme with Differential Evolution Optimization. IEEE Transactions on Audio, Speech, and Language Processing, 21, 2368-2378.

[19]. Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T. (1997) Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing, 6, 1673-1687

[20]. M. Steinebach, F. Petitcolas, F. Raynal, J. Dittmann, C. Fontaine, S. Seibel, et al., "Stirmark benchmark: Audio watermarking attacks," Proceedings of the International Conference on Information Technology: Coding and Computing, pp. 49-54, 2001, Las Vegas, Nevada.

[21]. T. K. Tewari, V. Saxena, J. P. Gupta, "Audio Watermarking: Current State of Art and Future Objectives", International Journal of Digital Content Technology and its Applications, vol. 5, no.7, pp. 306- 314, July 2011

[22]. T. K. Tewari, V. Saxena, J. P. Gupta, "A Novel Approach to Generate Watermarks Using Auditory Features for Audio Watermarking", Journal of Theoretical and Applied Information Technology, vol. 32, no. 2, pp. 155- 162, Jan 2012

[23]. Michael Arnold, Audio watermarking: features, applications, and algorithms. In IEEE International Conference on Multimedia and Expo (II). Citeseer,2000.

[24]. Manjushree A. Shete1, Prof.V.S.Kolkure, "A Review on Digital Watermarking, its features, need and various techniques" International Journal for Research in Applied Science &

Engineering Technology (IJRASET), ISSN: 2321-9653, Volume 4 Issue X, October 2016

[25]. K. Hofbauer, and H. Hering, "Noise Robust Speech Watermarking with Bit Synchronisation for the Aeronautical Radio," LNCS 4567, Springger-Verlag Berlin Heidelberg, pp. 252-266, 2007.

[26]. Al-Haj, A., Mohammad, A. and Bata, L. (2011) DWT-Based Audio Watermarking. The International Arab Journal of Information Technology, 8, 326-333.

[27]. Al-Yaman, M.S., Al-Taee, M.A., Shahrour, A.T. and Al-Husseini, I.A. (2011) Biometric Based Audio Ownership Verification Using Discrete Wavelet Transform and SVD Techniques. Proceedings of the 8th International Multi-Conference on Systems, Signals and Devices (SSD'11), Sousse, 22-25 March 2011, 1-5.

[28]. Khalid A. Darabkh, Imperceptible and Robust DWT-SVD-Based Digital Audio Watermarking Algorithm, Journal of Software Engineering and Applications, 2014, 7, 859-871.

[29]. A. B. Watson, "Image Compression Using the Discrete Cosine Transform," Mathematical Journal, vol. 4(1), pp. 81-88, 1994.

[30]. S. Katzenbeisser, and F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Publishers, 2000.

Cite this article as :

Krunalkumar N. Patel, "Different Types of Attacks and Performance Evaluation Factors in Digital Audio Watermarking ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 2, pp. 754-762, March-April 2019. Available at doi : https://doi.org/10.32628/IJSRSET1962141
Journal URL : https://ijsrset.com/IJSRSET1962141