JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DIGITAL WATERMARKING FOR AUDIO CLASSIFICATION DATASETS USING LSB BASED FEATURE CLASSIFICATION FOREST APPROACH

[1]Dr.S.Saravanan ,[2]P.Divya Sai,[3]P.Rekha,[4]Sk.Nawaz ,[5]P.Sarath Chandra Reddy
[1]Associate Professor,[2,3,4,5]UG Scholar, Dept .Of ECE
[1,2,3,4,5]N.B.K.R Institute of Science & Technology (Autonomous), Vidyanagar.

ABSTRACT:

In this project, we intend to investigate the ability to preserve audio classification datasets used in deep learning by fitting models to the dynamic range of the time-frequency signal of a segment. of the dataset. Previous research on audio watermarking technology required the actual sound of the watermarked audio to extract the information embedded in it. Whether the information classification model is trained using a set of watermarked information or simply using the classification results.

I.INTRODUCTION:

Advances in deep learning technologies increase the importance of large, well-organized data sets. Collections published for research or competition purposes are of great benefit to researchers, and many researchers rely on them. But for private companies, it is not an easy decision to share their data collection, which is a valuable asset that they have created at a high cost. Although the datasets are provided for academic, non-commercial purposes only, it is difficult to find commercial services using deep learning models trained on these datasets. If it is possible to determine whether a model was trained on a particular data set, private institutions will be more likely to open up their data sets and contribute significantly to the development of relevant research. Recently, there has been research on the protection of deep learning models [1, 2, 3, 4]. These studies aim to protect the trained deep learning models and encourage the expression of trained deep learning models and model parameters. In addition, a method of using text watermarks or noise has been proposed to protect sets of classification images [5]. However, to the best of our knowledge, no research has been conducted to preserve message classification datasets. The difference between using deep learning for image classification and audio classification lies in the input parameters. In the case of image classification, the image itself is used as an input component, but in audio classification, the inversion of the time-frequency signal is used. The shape of the time-frequency depends on various factors, including the size of the window, the size of the frequency jump, and the use of a frequency filter. In the process of general audio labeling of Freesound content using AudioSet signals in the 2019 DCASE challenge (Analysis and Analysis) the organization that generates the data set does not know which time frequency representation will therefore, watermarks used to protect message classification datasets must be robust to time-varying conditions. Traditional digital audio watermarking technology incorporates watermarks in the time domain, frequency domain, and coding domain to include information that cannot be recognized by the human auditory system

(HAS) [7]. In audio watermarking research that integrates information in the frequency domain, many studies use the dynamic component of the time-frequency signal as an input component for deep learning models [8, 9]. . These studies can hide information when audio files are changed by MP3 conversion, over-the-air conversion, noise insertion, etc., but in the process of extracting input data In hidden watermarks, they should be marked as time-stamped characters. This watermark cannot be considered to be robust against the changing conditions of time.

II.LITERATURE SURVEY:

1.Embedding watermarks into deep neural networks,

There have been significant advances in deep neural networks recently. Sharing training models for deep neural networks is essential for progress in the research and development of these systems. At the same time, the right to share trained students must be protected. For this, we recommend using digital watermarking technology to protect intellectual property rights and detect intellectual property violations when using trained models. First, we present a new problem: embedding watermarks in deep neural networks. Second, we propose a general framework for fitting watermarks to model parameters using parameter regularizers. Our approach does not affect the performance of the network where the watermark is placed, because the watermark is installed during training of the host network. Finally, we will conduct comprehensive experiments to demonstrate the potential of deep neural networks selected as the basis for this new research. We show that our framework can incorporate watermarks when training a deep neural network from the time of calibration and calibration without reducing its performance. Even after parameter adjustment or trimming, the embedded watermark will not disappear; even after cutting 65% parameters, the watermark remains.

2.Audio watermark encoding with reversing polarity and pairwise embedding,"

Audio signal processing improves the integration and detection of audio watermarks. Audio signal processing involves audio classification and correction of watermark input and detection based on the classification. Advances in audio watermarking design include adaptive watermarking data structure protocols, visual models, and embedding techniques. Visual and robustness assessments are included in audio watermarking inputs to optimize audio quality compared to the original signal and to optimize robustness or data capacity. This technique is applied to audio tracks in an audio input and monitor configuration to support real-time processing. Adaptive subtraction and matching is also used to insert and detect audio watermarks.

3."Comparative study of digital audio steganography techniques,"

The rapid development of digital data in many real applications has resulted in new and effective methods to ensure its security. Privacy can be achieved through the use of encryption methods. A new method has been proposed with many audio steganography functions. The goal of the steganography system is to obtain a secure and reliable method for hiding large amounts of confidential information. In this article we focus on digital audio steganography, which has become an important source of hidden data in modern telecommunication technologies such as voice overlay over IP, audio conferencing, etc. Many steganography standards have resulted in different design methods for these systems. In this paper, we review current digital audio steganography techniques and evaluate their performance in terms of robustness, security, and secrecy metrics. Another contribution of this paper is to provide a classification based on the robustness of the steganographic models based on the situation during the installation. This paper also discusses the research on key aspects of audio steganography applications.

III.EXISTING METHOD:

In recent years, many researchers have developed algorithms to hide data in audio signals. Some exercises aimed at achieving resilience and increasing strength are presented here. A scheme is proposed that uses the concept of frequency masking and wavelet coefficients to hide speech signals into speech signals by indirect LSB replacement. There are four steps: post-processing and pre-processing are performed using a discrete wavelet transform (DWT), and the DWT coefficients are converted from binary to binary. Next, the wavelet coefficients of the charges are selected and masked by an indirect LSB substitution operation. Finally, the output signal is reconstructed using a microwave converter. Although it can save useful data, it requires a lot of calculations and consumes a lot of time. Yan et al. A new steganography algorithm is proposed to protect MP3 audio files. Their algorithm is based on windowing technology, which is part of the MP3 compression standard used to control the previous broadcast. It works by establishing a correlation between hidden bit parity, window type, and hiding hidden messages in MP3 audio. This algorithm follows the MP3 compression standards, normal MP3 players can complete the stego audio decoding process correctly, but it can only get the hidden information by decoding the information in the hidden process, but it cannot be fully analyzed.

DISADVANTAGES:

1.)Implements Too many computations.

2.) Computationally very complex.

3.) Hidden message could only retrieved by parsing without fully decoding it.

4.) The message length affected the sound quality of the cover file, and whenever the message size got bigger.

5.) Implements an empensive architecture.

IV.PROPOSED METHOD:

In this project, we propose a hybrid information security privacy system using watermarking and encryption technologies. Audio file. In this project, a simple, low-complexity encryption and decryption method for text files is proposed to protect them from prying eyes. This hybrid system provides excellent security to messages and ensures reliability and authenticity. It is difficult to determine the expansion or rotation point of a bit, unless the range finder has full information about its expansion or rotation. They also need to know how to convert audio files to the American Standard Code for Information Interchange (ASCII) used in the system. watermark. Text messages are encrypted using a new algorithm based on shifting bit spaces around key symbols and then hiding them in a masked sound file in the time domain using the method LSB modulated and randomly distributed. It is difficult to determine the expansion or rotation point of a bit, unless the range finder has full information about its expansion or rotation. They also need to know how to convert audio files to the American Standard Code for Information Interchange (ASCII) used in the system. This is the second part of system security measures. The password message is hidden in a stereo channel audio file in *.wav file format. It uses a modified LSB method to hide bits in random locations in the secondary channel mask file. The LSB is determined by dividing each sample value by the number representing the LSB search key.

Structural Symmetry Index Measurement (SSIM) is an image quality metric that is considered the first choice for all traditional metrics such as PSNR and MSE. This measurement defines image distortion as a change to the structural data of the image. The concept of SSIM is based on the principle that spatially locked image pixels are strongly interdependent. Delivery is lost. In addition, the PSNR, MSE, and SSIM of audio files before and after inserting messages of different lengths are calculated.

ADVANTAGES:

1.) Highly immune to most attacks.

2.) These systems can provide an adequate security to the confidential information.

3.) These systems are reliable.

4.) Implements an simple and inexpensive architecture.

Fig(1): Block Diagram of the proposed system

RESULTS:

Fig 2:Input Text

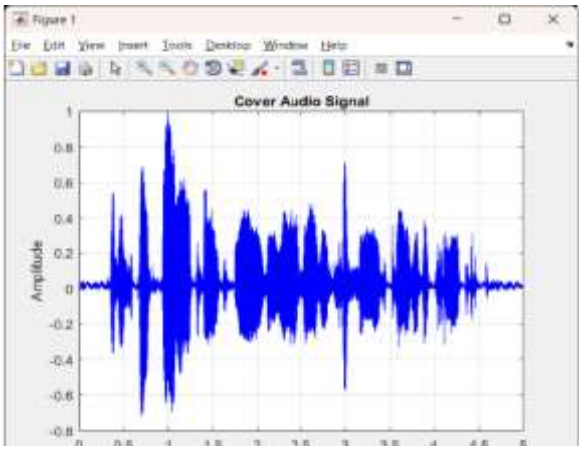

Fig 3:Cover audio signal

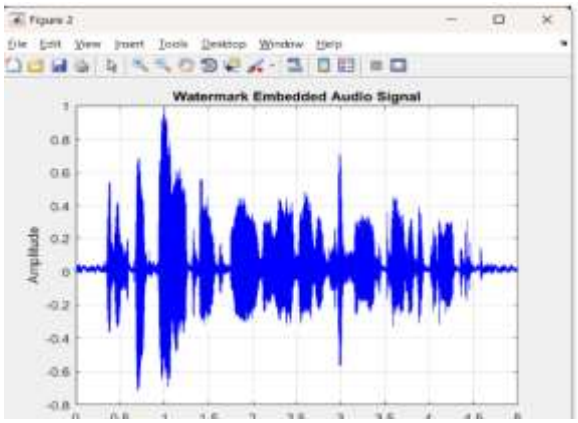

Fig 4:Watermark embedded audio signal

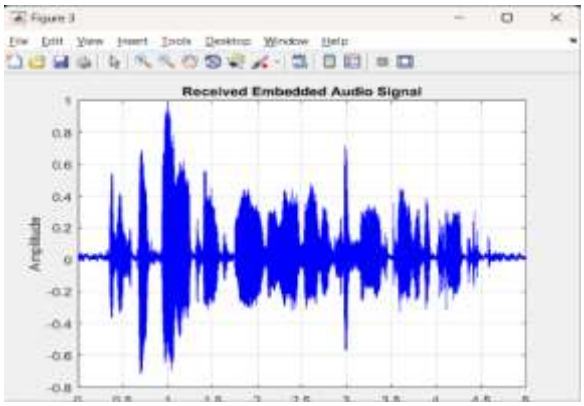

Fig 5:Recieved embedded audio signal

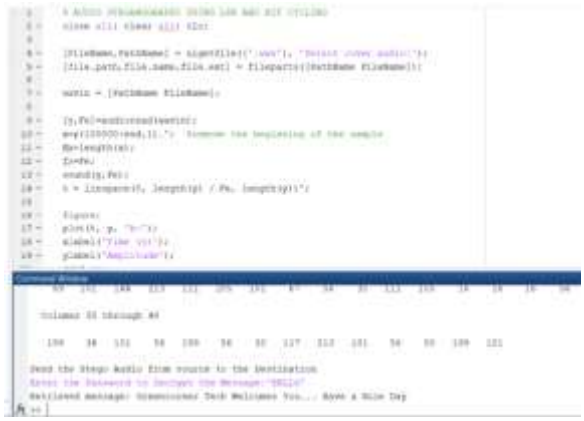

Fig 6:Output text

V.CONCLUSION:

We propose an elegant watermarking framework with possible watermarks to protect information datasets. The proposed watermarking for embedding distinct patterns in the amplitude domain of the time-frequency signal is evaluated based on various input parameters, models and datasets. Although the performance varies depending on the settings, the watermark effect is displayed in all cases. The effects of adding noise and using two or more watermarks in a data set will be studied later. Next, we examine the effectiveness of our proposed watermarking using an audio sound classification model and an aerial watermarking sound.

REFERENCES:

1] Bita Darvish Rouhani, Huili Chen, and Farinaz Koushanfar, "Deepsigns: A generic watermarking framework for ip protection of deep learning models," arXiv preprint arXiv:1804.00750, 2018.

[2] Yusuke Uchida, Yuki Nagai, Shigeyuki Sakazawa, and Shin'ichi Satoh, "Embedding watermarks into deep neural networks," in Proceedings of the 2017 ACM on International Conference on Multimedia Retrieval. ACM, 2017, pp. 269–277.

[3] Yuki Nagai, Yusuke Uchida, Shigeyuki Sakazawa, and Shin'ichi Satoh, "Digital watermarking for deep neural networks," International Journal of Multimedia Information Retrieval, vol. 7, no. 1, pp. 3–16, 2018.

[4] Ravi K Sharma, Brett A Bradley, Shankar Thagadur Shivappa, Ajith Kamath, and David A Cushman, "Audio watermark encoding with reversing polarity and pairwise embedding," Apr. 5 2016, US Patent 9,305,559.

[5] Jialong Zhang, Zhongshu Gu, Jiyong Jang, Hui Wu, Marc Ph Stoecklin, Heqing Huang, and Ian Molloy, "Protecting intellectual property of deep neural networks with watermarking," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security. ACM, 2018, pp. 159–172.

[6] Annamaria Mesaros, Toni Heittola, and Tuomas Virtanen, "A multi-device dataset for urban acoustic scene classification," in Proceedings of the Detection and Classification of Acoustic Scenes and Events 2018 Workshop (DCASE2018), November 2018, pp. 9–13.

[7] Mohammad Ali Nematollahi, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales, Digital watermarking, Springer, 2017.

[8] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, and Habib Hamam, "Comparative study of digital audio steganography techniques," EURASIP Journal on Audio, Speech, and Music Processing, vol. 2012, no. 1, pp. 25, 2012.

[9] Driss Guerchi, Harmain Harmain, Tamer Rabie, and Emad Mohamed Abd Elatief, "Speech secrecy: An fftbased approach," International Journal of Mathematics and Computer Science, vol. 3, 01 2008.

[10] Zohar Jackson, Cesar Souza, Jason Flaks, Yuxin Pan, ´ Hereman Nicolas, and Adhish Thite, "Jakobovski/freespoken-digit-dataset: v1.0.8," Aug 2018.

[11] Justin Salamon, Christopher Jacoby, and Juan Pablo Bello, "A dataset and taxonomy for urban sound research," in Proceedings of the 22nd ACM international conference on Multimedia. ACM, 2014, pp. 1041–1044.

[12] Shawn Hershey, Sourish Chaudhuri, Daniel P. W. Ellis, Jort F. Gemmeke, Aren Jansen, Channing Moore, Manoj Plakal, Devin Platt, Rif A. Saurous, Bryan Seybold, Malcolm Slaney, Ron Weiss, and Kevin Wilson, "Cnn architectures for large-scale audio classification," in International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2017.

[13] Sergey Ioffe and Christian Szegedy, "Batch normalization: Accelerating deep network training by reducing internal covariate shift," arXiv preprint arXiv:1502.03167, 2015.

[14] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan

Salakhutdinov, “Dropout: a simple way to prevent neural networks from overfitting,” The journal of machine learning research, vol. 15, no. 1, pp. 1929–1958, 2014.

[15] Vinod Nair and Geoffrey E Hinton, “Rectified linear units improve restricted boltzmann machines,” in Proceedings of the 27th international conference on machine learning (ICML-10), 2010, pp. 807–814.

[16] Diederik P Kingma and Jimmy Ba, “Adam: A method for stochastic optimization,” arXiv preprint arXiv:1412.6980, 2014.