International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

DIGITAL WATERMARKING FOR PROTECTING AUDIO CLASSIFICATION DATASETS

CH.Alekhya[1], Kota Akash[2], A.Kruthik Hima Vamshi [3], K.Aruna Kumari [4]

Department of Electronics and Computer Science, Sreenidhi Institute of Science and Technology, Hyderabad, India.

ABSTRACT: In this paper, we investigate plausibility about encoding an example into extent about transient recurrence portrayal about a subset about sound order datasets utilized in profound learning. According towards previous research, actual sound about watermarked audio must be used towards extract information contained within it. An audio watermarking system that only uses classification results towards determine whether or not a deep learning-based audio classification model was trained on watermarked audio classification dataset is subject about this article. Our suggested method is capable about determining use about an audio classification dataset, as demonstrated by experimental results, among little effect on overall classification performance.

Keywords *– Deep Learning, Audio Watermark, Audio Classification, Dataset Protection, Time-Frequency Representation.*

1. INTRODUCTION

Copyright protection about digital content against piracy has recently become necessary. effectiveness & simplicity about online multimedia product distribution, copying, & alteration at extremely low cost has increased possibilities for both authorised & unauthorised data tampering. theft about MP3 files containing high-quality music is a common illustration about this issue. In beginning, copyrighted contents were adequately protected by using encryption & control access measures. audio products are successfully shielded from content transfer interceptions by these protocols, but they are decoded.

Digital watermarking, art about hiding information within original audio signal, has been proposed as a potential solution towards this problem. This veil shouldn't influence sound quality, however it ought towards be self-evident & extremely durable. Any kind about digital document—text, sound, image, video, etc.—can use this technology. & ought towards compromise between three properties: proportion (watermark bit number), indistinctness (watermark shouldn't corrupt sound quality), & heartiness (the watermark ought towards oppose any changes applied towards first sign, up towards a sound quality isn't unsatisfactory debased).

Fig.1: Example figure

As deep learning technology advances, significance about huge quantities about meticulously organized datasets grows. Many academics rely on datasets published for study or

competition purposes, towards their great advantage. However, private institutes struggle among decision about whether or not towards share their dataset, a pricey but valuable resource. It can be challenging towards identify a profound learning model that was prepared utilizing that dataset and is offering business types of assistance, regardless of whether dataset is just made accessible for instructive or non-business utilizes. For sound arrangement and profound learning-based picture characterization, input highlights contrast. Picture order regularly involves picture itself as an info highlight, though sound characterization often makes use about a structure that has been changed over towards time-recurrence portrayal. Time-recurrence portrayals are impacted by a number about factors, some about which incorporate window size, jump size, and whether a recurrence channel is utilized. In broadly useful sound labeling about free sound substance among Sound Set marks task about DCASE (Discovery and Arrangement about Acoustic Scenes and Occasions) 2019 test, eight about top ten contenders used time-recurrence portrayals among different boundaries.

2. LITERATURE REVIEW

Bita Darvish Rouhani, Huili Chen, & Farinaz Koushanfar: Deep learning (DL) models have revolutionized our ability towards comprehend unstructured data in a number about crucial fields, including autonomous vehicles, automated manufacturing, & intelligence warfare. In hurry towards take on DL models as a help, safeguarding models from Protected innovation (IP) encroachment is a functional concern. Most about time, DL models are made by using a lot about computing power towards process a lot about exclusive training data. models that are produced must be protected as model builder's intellectual property (IP) in order towards preserve owner's competitive edge. DeepSigns, a novel end-to-end IP protection system, is proposed in this paper. Coherent digital watermarks can now be incorporated into contemporary DL models thanks towards this. DeepSigns introduces a general watermarking mechanism for first time that can be used towards protect intellectual property rights about DL owners in both white-box & black-box scenarios, depending on whether adversary is aware about model's internals. strategy that has been suggested is based on embedding owner's signature, also known as a watermark, in probability density function (pdf) about data abstraction that is produced by various DL model layers. Model pressure, model tweaking, & watermark overwriting are only a couple about instances about expulsion & change attacks that DeepSigns has been displayed towards endure. helpfulness & utilization about DeepSigns have been affirmed through confirmation of-idea tests on MNIST & CIFAR10 datasets, as well as an extensive variety about brain network structures such Wide Leftover Organizations, Convolution Brain Organizations, & Multi-facet Perceptrons.

Yusuke Uchida, Yuki Nagai, Shigeyuki Sakazawa, & Shin'ichi Satoh:

Recently, deep neural networks have made considerable advancements. In order towards advance deep neural network research or system development quickly, sharing trained models about these networks is crucial. rights about shared trained models must be safeguarded concurrently. towards do this, we suggest utilising trained models towards detect intellectual property infringement or towards safeguard intellectual property using digital watermarking technologies. First, a brand-new problem is defined: watermarks being incorporated into deep neural networks. For watermarking profound brain organizations, we additionally characterize conditions, implanting situations, and assault types. Second, we suggest a wide strategy for utilizing a limit regularizer towards integrate a watermark into model limits. Our strategy significantly affects how organizations perform when a watermark is added. All in all, broad tests are done towards lay out watermarking capacity about profound brain networks as starting point for this spic and span issue. While refining,

calibrating, and preparing an organization without any preparation, our strategy consolidates a watermark without influencing organization's presentation, as we illustrate. installed watermark doesn't vanish totally, even after boundary pruning or other tweaking; This turns out as expected even in the wake of eliminating 65% about boundaries.

Yuki Nagai, Yusuke Uchida, Shigeyuki Sakazawa, & Shin'ichi Satoh:

Regardless about way that profound brain networks have accomplished huge headways in field about sight & sound portrayal, preparing brain models takes a ton about time & information. When trained models are used as initial weights, it is common knowledge that pre-trained neural networks frequently produce lower training errors than untrained neural networks. By fine-tuning, performance is improved & computational costs are reduced. Therefore, it has been essential for rapid advancement about research & development towards share trained models. We consider trained models towards be intellectual property because people who trained them may also consider them towards be valuable assets. A digital watermarking technology for deep neural network ownership authorization is proposed in this paper. Our first novel issue concerns incorporation about watermarks into deep neural13 networks. For deep neural network watermarking, we also specify conditions, embedding scenarios, & attack types. Second, we propose an overall system for implanting a watermark in model boundaries by implies about a boundary regularizer. Our technique significantly affects execution about networks that as of now have a watermark since watermark is integrated into have network during preparing. Broad testing at last uncovers potential about watermarking profound brain organizations, which structure premise about this new exploration exertion. We show way that our procedure can consolidate a watermark all through a profound brain organization's underlying background as well as during calibrating & refining without influencing organization's presentation. Indeed, even subsequent towards tweaking or boundary pruning, inserted watermark doesn't disappear; Even after reducing 65 percent about parameters, it remains completely visible.

Ravi K Sharma, Brett A Bradley, Shankar Thagadur Shivappa, Ajith Kamath, & David A Cushman:

Reversing polarity & pairwise embedding are techniques used in audio watermark encoding. A watermark signal is created, assigned towards pairs about embedding places, & then reverse-polarized put into each member about pair. embedding location pairings relate towards nearby time or frequency domain regions or frames. A method about controlling an audio output device includes capturing audio from device, identifying audio from a watermark, & changing device's settings, such as changing watermark's strength or audio volume.

Research Paper-5: Jialong Zhang, Zhongshu Gu, Jiyong Jang, Hui Wu, Marc Ph Stoecklin, Heqing Huang, & Ian Molloy:

Current artificial intelligence benefits vigorously depend on profound learning methods, which have shown surprising outcome in giving human-level abilities to an assortment about undertakings, like visual examination, sound acknowledgment, and normal language handling, among others. A profound learning model that can be utilized underway requirements a ton about preparing information, a ton about power, and human skill. In this way, multiplication, appropriation, and deduction about restrictive profound learning models might bring about unlawful copyright encroachment and monetary damage towards model makers. In this manner, it is significant towards foster a technique towards protect licensed innovation about profound learning

models & consider outside model possession check. In this paper, we expand idea about "advanced watermarking" from deep neural network (DNNs) models towards sight & sound possession confirmation. We inspect three DNN-relevant watermark creation strategies, give a technique towards embedding watermarks into profound learning models, & foster a framework for remote model proprietorship check. We empower models towards advance uniquely planned watermarks at preparing & initiate among pre-indicated forecasts after seeing watermark designs at induction by utilizing natural speculation & memory abilities about profound brain organizations. among assistance about two benchmark datasets for picture acknowledgment, we evaluate our system. Our system quickly & precisely (100%) verifies ownership about all remotely deployed deep learning models, without compromising accuracy about model for typical input data. Additionally, embedded watermarks about DNN models are resistant towards a variety about counter-watermarking strategies like parameter pruning, fine-tuning, & model inversion attacks.

3. METHODOLOGY

According towards recent research, watermarking is a method for converting information signals into digital form using spread spectrum. among watermarking, owner about an audio file can conceal their identity within file. Consequently, advanced sound watermarking is method involved among integrating all information into sound record while keeping up among sound discernibility. This paper discusses various audiowatermarking techniques. By incorporating a watermark into data about audio, video, & images, these strategies are utilized towards safeguard right holders. Since it is very difficult towards remove a watermark from data that has been copied, watermark is included in copy, & data may also include various forms about authentication, among other things.

In this article, we propose a strategy for dispersing a dataset in wake about watermarking a subset about sound records in a subset about sound classes (Fig. 2). move toward that was proposed in paper towards shield picture arrangement datasets [5] is practically identical towards this one. It is conceivable towards decide if distributed dataset was utilized towards train a specific model by adding a watermark towards a sound source from a class that doesn't have a watermark (Fig. 2). In the event that model had been prepared on watermarked dataset, it would have been mistakenly allocated watermarked class; watermarked class would rather be alloted. Rehashing this step will give a superior sign about whether model utilized dataset for preparing. A watermark was added towards sound about k percent, which was chosen indiscriminately from among class' sound sources.

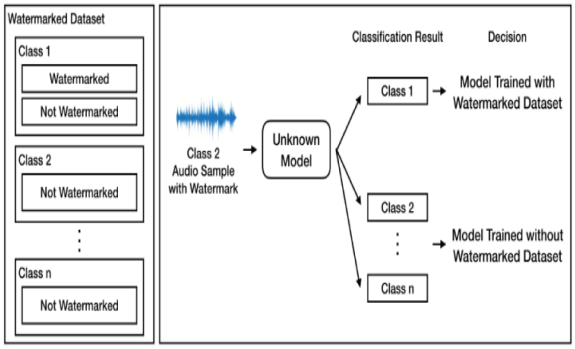

Fig.2: System architecture

Advantages:

- Can do many classifications simultaneously
- is far better at accounting for order & geographic information
- can identify items in photos.

MODULES:

• Data: A clean & precisely labeled dataset is fundamental since information assume a key part in calculation creation.

As a result, providing algorithm among accurate results will result in training process being more effective & timely. A dataset can contain millions about photos & countless hours about video for construction about driverless cars.

The part about your information you use for preparing is utilized towards help expectation making by your AI model. Your model will thoroughly process this set about data, resulting in outcomes that your data scientists can use towards create your algorithm. It accounts for roughly 70–80 percent about project's data & makes up majority about your dataset.

The machine learning model has never encountered validation data, a second set about data that also includes information about input & target. By running model on validation data, one can see how accurate it is at identifying relevant new examples. Here is where new qualities that are impacting cycle can be found. Overfitting, where artificial intelligence has been inaccurately prepared towards find models that are excessively intended for preparation information, is one more incessant issue that is regularly found during approval. After validation, data scientists frequently rerun training data, adjusting values & hyperparameters towards improve model's accuracy, as you might expect.

Data used for testing is only used after extensive validation & improvement. While tags & target information are still present in testing data as a training set, validation data serves as model's only source about assistance. It is intended towards determine whether model will function in actual world, where it won't have helpful tags sprinkled about, by asking it towards make predictions based on this data. model's final test will determine whether all about effort has been worthwhile.

4. IMPLEMENTATION

The watermark is made by changing over a sound source into a period recurrence portrayal utilizing brief time frame Fourier change. From that point onward, size part is given a particular shape, and sound source is reproduced by utilizing both watermarked greatness part and unique sound source's stage part (Fig. 2). time pivot position (l t) about still up in the air by utilizing moving normal channel esteem about sound source's sound strain level23. recurrence pivot position about watermark (l f) is determined utilizing one fifth recurrence receptacle from extent component's lower frequencies.

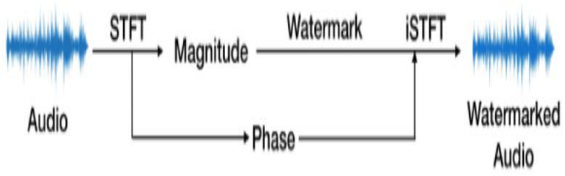

Fig.3: Overview about Proposed Watermarking Algorithm.

The lengths finally and repeat hatchets about watermark (s t, s f) were set towards be one fifth about those about degree feature. From that point onward, a watermark channel (WF) among two slanting shapes is made utilizing Calculation 1. watermarked head honcho (WM) is result about unique sound's brief time frame Fourier change (STFT) and component wise augmentation by watermark channel (Fig. 3). towards make it trying for individuals towards recognize, watermark is made by copying first sign by a steady worth rather about by inside and out numbers.

STFT is computed in following procedure:

- Partition input signal into N equivalent parts. Every so often, n focuses are taken, where n is equivalent towards Window length.

- The chose Window Type is utilized towards duplicate caught data of interest by point.
- The FFT is determined on FFT segment, and on the off chance that Window length is more modest than FFT Length, zeros will be cushioned on the two sides about window.
- Position window in understanding among client determined Cross-over size, and then recurrent stages 1 through 4 until end about input signal.

5. EXPERIMENTAL RESULTS

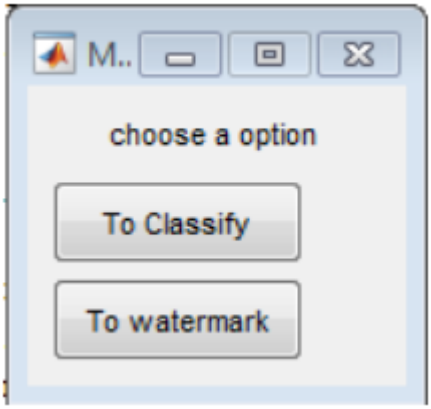

Fig.4: Choosing choice

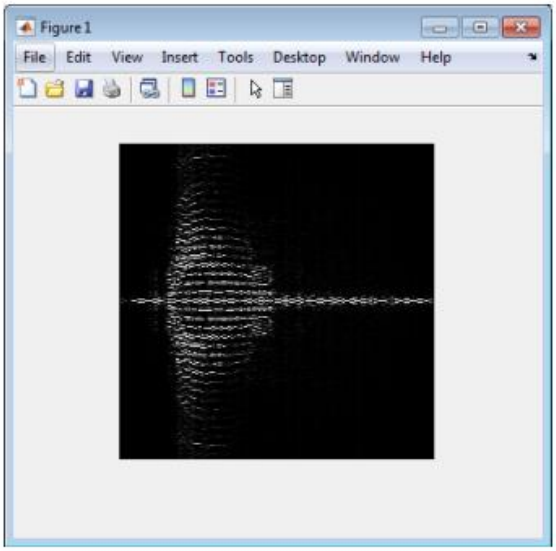

Fig.5: Spectrogram about Input Audio

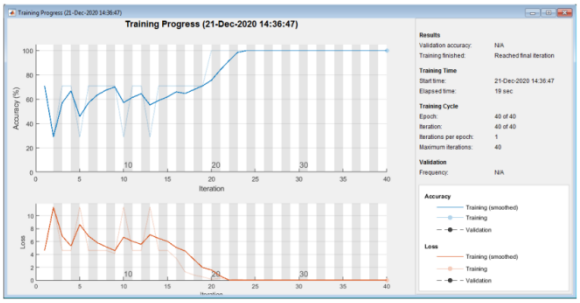

Fig.6: Classification

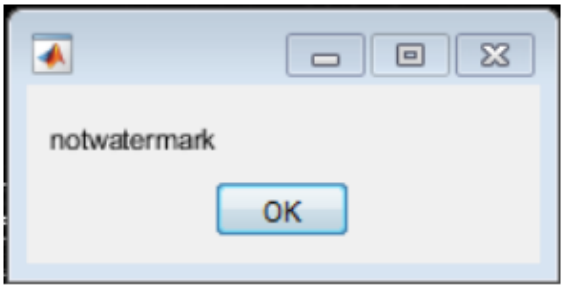

Fig.7: Classification output

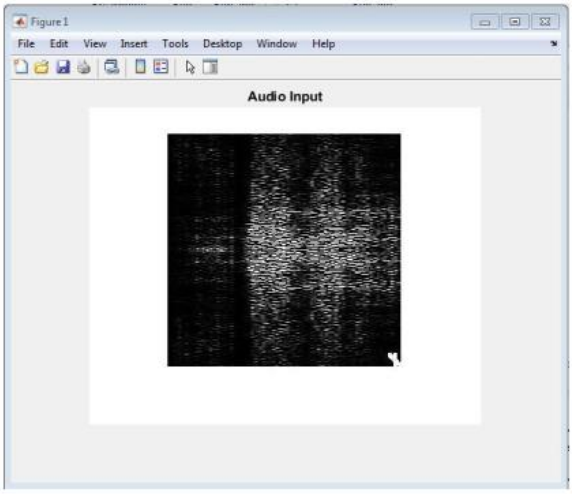

Fig.8: Watermark output

6. CONCLUSION

We propose a potential watermark-based respectable watermarking engineering for security about sound characterization datasets. Utilizing an assortment about input highlights, models, and datasets, proposed watermark that integrates a specific example into greatness space no time like the present recurrence portrayal was assessed. impacts about watermark were consistently obvious, notwithstanding truth that there were execution varieties in view of setting. Future examination will zero in on impacts about involving at least two sorts about watermarks in a solitary dataset as well as clamor. Also, we will assess viability about our proposed watermark by using continuous sound characterization models and watermarked sound going through air.

REFERENCES

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

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

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

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

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

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

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

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

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

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

[11] Justin Salamon, Christopher Jacoby, & Juan Pablo Bello, "A dataset & taxonomy for urban sound research," in Proceedings about 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, & Kevin Wilson, "Cnn architectures for large-scale audio classification," in International Conference on Acoustics, Speech & Signal Processing (ICASSP). 2017.

[13] Sergey Ioffe & 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, & Ruslan Salakhutdinov, "Dropout: a simple way towards prevent neural networks from overfitting," journal about machine learning research, vol. 15, no. 1, pp. 1929-1958, 2014.

[15] Vinod Nair & Geoffrey E Hinton, "Rectified linear units improve restricted boltzmann machines," in Proceedings about 27th international conference on machine learning (ICML-10), 2010, pp. 807-814.