Dataset Pruning for Resource-constrained Spoofed Audio Detection

Abdul Hameed Azeemi, Ihsan Ayyub Qazi, Agha Ali Raza

Lahore University of Management Sciences
21030027@lums.edu.pk, ihsan.qazi@lums.edu.pk, agha.ali.raza@lums.edu.pk

Abstract

The performance of neural anti-spoofing models has rapidly improved in recent years due to larger network architectures and better training methodologies. However, these systems require considerable training data for achieving high performance, which makes it challenging to train them in computer-restricted environments. To make these systems accessible in resource-constrained environments, we consider the task of training neural anti-spoofing models with limited training data. We apply multiple dataset pruning techniques to the ASVspoof 2019 dataset for selecting the most informative training examples and pruning a significant chunk of the data with minimal decrease in performance. We find that the existing pruning metrics are not simultaneously granular and stable. To address this problem and further improve the performance of anti-spoofing models on pruned data, we propose a new metric, Forgetting Norm, to score individual training examples with higher granularity. Extensive experiments on two anti-spoofing models, AASIST-L and RawNet2, and several pruning settings demonstrate up to 23% relative improvement with forgetting norm over other baseline pruning heuristics. We also demonstrate the desirable properties of the proposed metric by analyzing the training landscape of the neural anti-spoofing models.

Index Terms: Spoofing, data pruning, subset selection, automatic speaker verification, ASVspoof, fake audio.

1. Introduction

There has been significant progress recently towards better voice conversion and speech synthesis systems. These systems have numerous applications within assistive technologies, gaming, and human-computer interaction [1]. However, they can also be used to generate natural-sounding audios which can defeat biometric identification methods and automatic speaker verification (ASV) systems. This can lead to the potential misuse of these systems, e.g., voice-based security systems can be fooled via fake audios thereby granting access to protected information and restricted areas. Moreover, such techniques can also be used for spreading misinformation. Given these negative impacts of spoofed audios, it is important to design systems that can accurately distinguish between bonafide and synthetic audios generated using a wide range of techniques.

The ASVspoof community has devised a series of challenges and datasets to facilitate the research on spoofing detection systems [2, 3, 4, 5]. The two primary scenarios considered in these challenges are logical access and physical access. Logical access (LA) consists of the attacks through voice conversion and speech synthesis systems including text-to-speech models, whereas the physical access pertains to the attacks via replayed audios. Several deep learning-based models have been proposed to tackle the LA attacks which have demonstrated high performance through specialized architectures that can automatically detect the spoofing artefacts present within spectral and temporal domains [6, 7]. However, these models require a significant amount of training data to achieve high performance and a low equal error rate (EER) on the test set, which presents a significant challenge when training these models within resource-constrained settings and compute-restricted environments.

The strategies proposed for resource-constrained spoofing detection include the construction of lightweight, robust deep learning-based models with limited parameters [7] or the use of acoustic microfeatures in knowledge-driven models, which can distinguish between spoofed and bonafide audios [1, 8, 9, 10]. However, the methods for reducing the size of the training data (or data pruning approaches) have not yet been explored in the context of spoofed audio detection. In this work, we consider the task of automatically pruning the ASVspoof 2019 dataset to obtain a representative subset that can be used for training deep learning-based anti-spoofing models in resource-constrained settings (Figure 1). We consider several heuristics and scoring metrics to select the most informative training examples and prune the rest of the data.

1.1. Contributions

The presented research makes the following contributions:

- We apply dataset pruning to neural anti-spoofing models by scoring individual training examples using different metrics (normed error, forgetting score) and selecting a subset of the examples for training, using these scores.
- We propose a new scoring metric, the forgetting norm, for better dataset pruning.
- Our empirical evaluation on the ASVspoof dataset [11] and two deep learning-based anti-spoofing models shows that training the model on the subset selected by forgetting norm performs better than the existing metrics (random pruning, normed error, and forgetting scores).

2. Background Work

A number of methods have been proposed to quantify the importance of individual training examples in deep learning models for standard classification tasks [12, 13, 14, 15, 16, 17, 18]. These approaches emphasize the identification of informative training examples via different heuristics and removing non-representative samples from the dataset. Toneva et al. [19] consider the ‘forgetfulness’ of a training example by measuring the number of times it is misclassified after being classified correctly during training. The number of such incorrect classifications represents the forgetting score of a particular example. The examples that are repeatedly forgotten are selected to construct a smaller training subset without significantly affecting the generalization performance. Paul et al. [17] propose to score the examples by the norm of the gradient (Grad) and the norm of the error vector (El2N). Both these measures are found to be correlated and any of these can be used for removing a large number of less informative examples while retaining the test
accuracy on multiple standard vision datasets (CIFAR-10 and CIFAR-100) and convolutional neural networks (ResNet). Another interesting finding is that the loss landscape in the early training epochs contains sufficient information which can be leveraged to construct a smaller subset of the training data without training the neural network for all the epochs.

Coreset selection is another approach of reducing the dataset size by extracting representative samples [20, 21, 22, 23]. To construct the theoretical error boundaries, many coreset selection algorithms require the problem to demonstrate a special structure like convexity. Hence, the application of coreset algorithms is limited in deep learning tasks and optimal solution is seldom guaranteed for the downstream tasks. In speech tasks, especially automatic speech recognition (ASR), subset selection algorithms focus on the generation of phonetically rich and diverse subsets through phoneme level error models [24, 25, 26, 27, 28, 29, 30, 31, 32]. Awasthi et al. [32] propose an objective function to select a subset of sentences for training an ASR personalization model. The created subset contains more challenging and informative sentences than a random selection approach. These error models for ASR and other speech tasks can provide good insights on the properties of representative subsets but are not directly applicable to anti-spoofing due to the different nature of the anti-spoofing problem.

3. Preliminaries

Consider a neural anti-spoofing model \( f(x; \theta) (\theta \in \mathbb{R}^d) \) that is trained on a labelled dataset \( x \in \mathcal{D}_i \) (e.g., ASVspoof). \( \mathcal{D}_i \) consists of pairs of audio and the corresponding label (bonafide or spoof) and \( \theta \) represents the neural network parameters. Our goal is to prune \( \mathcal{D}_i \) to obtain a subset \( \mathcal{B}_i \) such that the performance of the anti-spoofing model \( f(x; \theta) \) after training on \( \mathcal{B}_i \) is better than random pruning. The performance of anti-spoofing is commonly evaluated via equal error rate (EER) or the ASV-centric tandem decision cost function (t-DCF) [33].

Let \( \sigma \) be the softmax function given by \( \sigma(z_1, \ldots, z_K)_k = \exp \{ z_k \} / \sum_{k'=1}^{K} \exp \{ z_{k'} \} \). The output of the anti-spoofing model is then a probability vector \( \mu(x, \theta) = \sigma(f(x, \theta)) \), where \( f(x; \theta) \) are the logit outputs of the neural anti-spoofing model.

4. Method

We now describe three metrics for scoring individual training which can facilitate dataset pruning. The scores calculated via these metrics are used by the pruning algorithm to construct a subset of the training data by selecting the highest error (most informative) examples.

4.1. EL2N score [17]

The normed error (or the EL2N score) [17] of a training example \((x_i, y_i)\) at epoch \( t \) is defined as,

\[
\mathbb{E} \| f(x_i; \theta^t) - y_i \|_2
\]

(1)

It is essentially the norm of the difference between the predicted class probabilities (for spoof and bonafide classes) and the ground-truth label encoded as one-hot vector. An example that is more difficult to classify will have a high normed error as compared to an easier example. A desirable property of the EL2N score is that it captures the difficulty of a training example with greater granularity as compared to the other metrics that are discrete, e.g., forgetting scores. Hence, the error normed scores computed after a few training epochs can be used for data pruning. We refer to the EL2N score computed at epoch \( t \) as \( EL2N_t \).

4.2. Forgetting score [19]

Let the binary variable \( acc_i^t = \mathbb{1}_{y_i = y_{\hat{y}_i}} \) indicate whether the training example \( i \) is correctly classified at epoch \( t \). A forgetting event is a point in training when the neural network misclassifies a training example after classifying it correctly, i.e., \( acc_i^t < acc_i^{t-1} \) [19]. The forgetting score of a particular training example is the number of times a training example undergoes a forgetting event.

\[
\sum_{t=1}^{N} \mathbb{1}_{acc_i^t < acc_i^{t-1}}
\]

(2)

Toneva et al. [19] demonstrate that the examples with a higher forgetting score are more informative examples and can be used to create a smaller subset for training the neural network. As forgetting events occur throughout the training, the forgetting scores are calculated towards the end of the training. Hence, they are more stable than the other metrics which are calculated on a particular training epoch early in training, e.g., EL2N score.

4.3. Forgetting norm

We introduce a new scoring metric, forgetting norm, which is defined as the increase in normed error across two successive epochs. Let \( n_i^t = \mathbb{1}_{EL2N_i^t > EL2N_i^{t-1}} \) be a binary variable indicating whether the EL2N score at epoch \( t \) is greater than the EL2N score at epoch \( t-1 \). Forgetting norm is then defined to be,

\[
\sum_{t=1}^{N} n_i^t \times (EL2N_i^t - EL2N_i^{t-1})
\]

(3)
which expands to,

$$\sum_{i=1}^{N} n_i \cdot (\| f(x; \theta_{i}) - y_i \|_2 - \| f(x; \theta_{i-1}) - y_i \|_2) \quad (4)$$

In other words, the forgetting norm is the cumulative sum of the difference of EL2N scores over \( n \) training epochs, computed in the epochs where EL2N \( \geq \) EL2N \( \leq \) (and not only the epochs where a forgetting event occurs). Compared to the forgetting score that only gets incremented in case of an actual misclassification (as normed error crosses a threshold), forgetting norm captures the more subtle error increase that may result in a misclassification in later epochs. Hence, forgetting norm combines the granularity of normed error (EL2N) with the stability of forgetting scores.

### 4.4. Dataset Pruning Algorithm

We now present the dataset pruning algorithm for neural anti-spoofing models (Algorithm 1). We train the model on the ASVspoof dataset and calculate the score for each example according to the selected metric. We then sort the examples in a descending order of the calculated scores and select the highest scoring examples.

**Algorithm 1:** Dataset Pruning for Neural Anti-Spoofing Models

**Input:** Anti-Spoofing Model \( f \), Dataset \( D \), Pruning Fraction \( f \), Pruning Strategy \( s \), Training Epoch \( e \)

\[
S \leftarrow \text{Train } f \text{ on } D; \text{ compute scores for each training example on epoch } e \text{ according to strategy } s \\
\text{subsetSize} \leftarrow (1-f) \times \text{len}(D) \\
S \leftarrow \text{sort}(S, \text{descending} = \text{true}) \\
B_i \leftarrow S[0 : \text{subsetSize}] 
\]

### 5. Experiments

#### 5.1. Models


**AASIST-L:** AASIST-L [7] is a lightweight end-to-end audio anti-spoofing model based on graph neural networks. The graph modules and heterogeneous stacking graph attention layer can efficiently model spoofing artefacts present in temporal and spectral domains. The max graph operation detects various spoofing artefacts in parallel and combines them.

**RawNet2:** RawNet2 [6] is also an end-to-end audio anti-spoofing model. It is based on a convolutional neural network architecture that ingests raw speech and outputs the prediction: bonafide or spoof. An important part of the RawNet2 architecture is a GRU layer containing 1024 hidden nodes which can produce a single utterance-level representation by aggregating frame-level representations.

#### 5.2. Dataset

The experiments are carried out on the logical access (LA) part of the ASVspoof 2019 dataset [11]. This dataset is split into three parts: train, development, and evaluation set. The attacks present in the train and development sets were created from six spoofing algorithms (A01-A06). The attacks in the evaluation set were created from thirteen algorithms (A07-A19). The pruning is done on the train set only, and the evaluation is done on the original (complete) evaluation set. We consider three pruning percentages: 30%, 60%, and 90% to mirror the low, moderate, and extreme resource-constrained settings. The pruning is performed separately on the spoof and bonafide portions in order to maintain the ratio defined in the ASVspoof dataset.
5.3. Metrics
To evaluate the performance of the anti-spoofing model on the pruned dataset, we use equal error rate (EER) and the minimum tandem detection cost function (t-DCF) [33]. EER measures the performance of standalone anti-spoofing system whereas min t-DCF evaluates the combined performance of the automatic speaker verification system and the anti-spoofing system.

5.4. Implementation Details
The scoring metrics are implemented using the PyTorch library in Python. The official implementation of AASIST-L and RawNet is used. We use a single 40GB NVIDIA A100 GPU for running all the experiments. For calculating the scores for each training example, we initiate a computation step after each epoch and record the score (EL2N, forgetting Score, forgetting norm). The scores in each epoch are averaged over 10 runs and then used for a particular pruning strategy. We then train the model for 5 epochs on the pruned dataset. For each test EER and min t-DCF reported, we do three independent runs (with independent model initialization) and calculate the average.

5.5. Results
Table 1 shows the results of pruning experiments via different pruning strategies across multiple neural anti-spoofing models. For each architecture and the scoring metric, we consider multiple pruning percentages and report the pooled EER. We find that forgetting norm consistently performs better than the pruning performed on the basis of random, EL2N, and forgetting scores for the majority of pruning percentages. For AASIST-L and 60% pruning percentage, we notice a 23% relative drop in the EER as compared to the random pruning (15.14% vs 11.63%) and an 8% relative drop as compared to the forgetting score (12.69% vs 11.63%).

Comparison of individual attacks. Table 2 shows a performance comparison for each of the individual attacks present in the ASVspoof LA evaluation subset. We again observe a consistent improvement in pooled EER and pooled min t-DCF for forgetting norm. For multiple attacks, substantial improvements are observed for forgetting norm as compared to the forgetting score, e.g., for the A09 attack, forgetting norm shows a 65% relative improvement (1.20% vs 0.41%).

Properties of Forgetting Norm. To understand the underlying properties of the forgetting norm which contribute to its better performance, we analyze the training landscape by computing the scores (forgetting score and forgetting norm) for each example in every epoch (Figure 2). We find that the forgetting norm demonstrates a continuous behavior as compared to the forgetting score which only has discrete increments. This allows the forgetting norm to be used for pruning effectively, a property that is not present in the forgetting scores. We also study the correlation between forgetting scores and forgetting norm for each training example in ASVspoof (Figure 3). We find that multiple examples with the same forgetting score can have different values of the forgetting norm, e.g., if an example is misclassified once, the forgetting norm will assign a continuous score to that event whereas the forgetting score will have the discrete value of one. Additionally, the forgetting norm can be non-zero even in the cases where the forgetting score is zero, which can facilitate the early prediction of a misclassification event when it has not yet oc-

6. Limitations and Conclusion
We now discuss some limitations of our approach and the potential future directions for resource-constrained spoofed audio detection. Our pruning experiments were performed on two end-to-end (E2E) neural anti-spoofing models. It needs to be investigated if data pruning is applicable to other types of anti-spoofing architectures that do not operate directly on raw speech waveform. While we investigated the pruning approaches for anti-spoofing on the standard ASVspoof dataset, it needs to be examined if the techniques are applicable to any other datasets that are used in training spoofing countermeasure models. Additionally, it should be explored if the ASVspoof subsets created through the presented pruning approach demonstrate reasonable performance on other spoofing countermeasures too, e.g., GMM-based classifiers for separating spoofed audio from bonafide speech. For future work, it will be interesting to explore the properties of the subsets of ASVspoof created via data pruning approaches and analyze the composition of various types of attacks in those subsets. It will also be useful to leverage data pruning for other related tasks like partially spoofed audio detection, replay attack identification, and spoofing aware speaker verification.
7. References


