Abstract
This paper presents our learned lessons from the ADD2023 track3, Deepfake Algorithm Recognition (AR). In recent years, speech synthesis has made remarkable progress, where it has become increasingly difficult for human listeners to differentiate between synthesized speech and genuine human speech. Previous research has demonstrated that improving the recognition of deepfake algorithms can significantly enhance spoofing detection. Therefore, the primary focus of this paper is to investigate deepfake algorithm recognition, with experiments conducted based on the ADD2023 challenge. Inspired by speaker verification, we propose a center-based maximum similarity evaluation method for determining the category of deepfake algorithms. Finally, by combining the scores from multiple models at the score level, we achieve an impressive F1 score of 0.8312 on the evaluation set.

1. Introduction
Text-to-speech (TTS) and voice conversion (VC) systems have made significant progress in recent years, thanks to the progress made in deep learning techniques and the availability of large-scale corpora [1]. These advancements have enabled the generation of audio that is almost virtually indistinguishable from human speech, posing serious threats to human users and Automatic Speaker Verification (ASV) systems in terms of potential attacks and security vulnerabilities. To protect the integrity of ASV systems, audio anti-spoofing countermeasure (CM) systems are commonly employed to detect spoofing audios [2].

In recent years, significant efforts have been devoted to the audio anti-spoofing task, with notable challenges such as ASVSpoof [3, 4] gaining prominence. However, most of these endeavors have primarily focused on binary classification tasks, distinguishing between bona fide and spoof audios, while neglecting the recognition of deepfake algorithms. Recognizing deepfake algorithms presents a more challenging multi-classification problem, with the presence of unseen categories, compared to fake audio detection.

In this paper, we evaluate the performance of deepfake algorithm recognition, focusing on the ADD2023 track3 [5], which aims to recognize the specific deepfake algorithm that a fake utterance is generated from. The evaluation set consists of both known and unknown deepfake algorithms, making the task an open-set recognition problem. To address this challenge, we propose a center-based maximum similarity evaluation method inspired by speaker verification. In our approach, we adopt an 1D and 2D convolution-based backbone to extract highly discriminative embedding. And then, each test embedding is computed the similarity with each known class centroid embedding. Finally, by fusing scores from multiple models at the score level, we achieve an impressive F1 score of 0.8312.

2. Related Work
2.1. Anti-spoofing
Synthesized audio spoofing is generally considered a logical access (LA) attack [6]. In recent years, mainstream CM systems for synthetic speech detection usually comprise two modules: feature extraction and binary classification. The feature extraction module extracts applicable features suitable for synthetic speech detection tasks. The classifier module determines whether the test audio is bona fide or spoofed based on the extracted features. Therefore, the performance of the classification module heavily relies on feature extractors that can provide highly discriminative features. Features based on audio self-supervised learning models have been shown to be effective [7]. On the other hand, various models and network architectures have been used for back-end classifiers, some of them takes frequency acoustic features as input, including ResNet [8], SE-Net [9], LCNN [10], etc., while some take original waveform as input, such as RawNet2 [11], AASIST [12], etc. Additionally, there are also some angle-based loss functions used for audio anti-spoofing, such as...
we propose a center-based maximum similarity method
to increase the inter-class distance while reducing the
intra-class distance. The OC-softmax is also adopted
to customize metric parameters for the different class
distributions of bonafide and spoof audios.

The second Audio Deepfake Detection challenge (ADD 2023) first sets up a track for deepfake algorithm recognition. Prior to that, only few researches focused on this task. M. Muller et al. presents several methods for creating attacker signatures using low-level acoustic descriptors and machine-learning embeddings for attacker attribution [16]. Zhu et al. uses separate module classifying attributes for the spoofing attack, which can also be helpful for binary spoof detection. Li et al. used a multi-task learning approach to algorithm recognition as an auxiliary task for binary classification, which is proved effective.

2.2. Speaker verification

Automatic Speaker Verification (ASV) is a voice identity technology that determines whether two speech segments belong to the same person. To evaluate the performance of an ASV system, a trial list is provided, where each trial consists of an enrollment segment and a test segment. In the deep learning stage, we usually extract the speaker embedding, a fixed $d$-dimensional vector, from variable-length waveform. Then, we calculate the similarity between the enrollment embedding and the test embedding, which represents the probability that they belong to the same person. ASV is an open-set task, meaning that all test speakers are unseen during the training stage. On the other hand, deepfake algorithm recognition is a semi-open task, where both seen and unseen classes exist during the evaluation stage. In this case, we can adopt the method of speaker verification for deepfake algorithm recognition.

In this paper, we regard the deepfake algorithm recognition as a speaker verification task. Accordingly, we propose a center-based maximum similarity method to determine the category of test audio.

3. Center-based Maximum Similarity Method

The pipeline of our proposed method is illustrated in Figure 1. We employ a supervised learning approach to train a closed-set classification model on the training dataset. Subsequently, we feed all variable-length audio samples from the training set into the encoder of trained model, obtaining fixed-length $d$-dimensional embeddings $z \in \mathbb{R}^d$. These embeddings correspond to the final linear outputs before the classifier. The classifier output can be seen as the result of inner product between the test embedding and the linear weight $w_i \in \mathbb{R}^d$, where $w_i$ can be considered as the centroid $\mathbf{c}_i$. When $z$ and $w_i$ are normalized, the classifier output is the cosine similarity between $z$ and $w_i$. However, the training process is not always stable, which may cause center shifting. To overcome this, we calculate the average embedding for each class, obtaining stable intra-class centroids:

$$c_k = \frac{1}{N} \sum_{i=1}^{N} z_{k,i} \quad (1)$$

where $c_k$ represents the embedding centroid of class $k$, and $z_{k,i}$ corresponds to the embedding of the $i$-th sample from class $k$. Next, we evaluate the test embedding $z_{\text{test}}$ by scoring it against all intra-class centroids. The scores are denoted as $v_i \in V$ and $i \in \{0, 1, 2, 3, 4, 5, 6\}$.

$$v_i = \cos(z_{\text{test}}, c_i) \quad (2)$$

where $\cos(\cdot)$ indicates the cosine similarity between test embedding and various intra-class centroids. During the training process, we employ a loss function with angular margin, specifically ArcFace [14], to optimize the embeddings. ArcFace not only incorporates cosine similarity during optimization, but also increases the inter-class margin while reducing intra-class variance.

Finally, if any score $v_i$ surpasses the predefined centroid threshold, the test audio is assigned to the class with the highest score. Conversely, if all scores $v_i$ fall below the threshold, the test audio is considered as belonging to an unknown class 7.

$$\begin{align*}
\text{argmax}_{i \in V} (v_i), & \quad \text{max}(v_i) > 0.75, \\
\text{7}, & \quad \text{max}(v_i) \leq 0.75.
\end{align*} \quad (3)$$

The value 0.75 is a hyperparameter that has been obtained through tuning on the development set.

4. Implement Details

4.1. Network

In our deepfake algorithm recognition system, we employ a two-stage training approach: pre-training and large margin fine-tuning (LMFT). During the first stage, we set the scalar and margin of the angle softmax to 32 and 0.2, respectively. In the LMFT stage, we increase the margin to 0.4. To capture the distinctive features of deepfake audio,
we leverage various network architectures. Below are the specific details of each network utilized in our system:

**ResNet34SimAM-ASP:** We adopt the ResNet34SimAM-ASP [19] as our baseline system. This network utilizes the residual modules of ResNet and is equipped with the SimAM (Simple attention module). We use a thin ResNet structure with a backbone width of \{32, 64, 128, 256\} to prevent overfitting on small-scale training data. The output feature maps are then processed using attentive statistics pooling (ASP) [20]. The output embedding has a dimension of 256.

**ResNet34-GSP:** ResNet34-GSP is based on the standard ResNet backbone, which is a well-known framework for 2D Convolutional Neural Networks (2D-CNNs) in image recognition tasks. We use the same backbone width as ResNet34SimAM-ASP. The encoding layer of ResNet34-GSP is based on global statistic pooling (GSP), and the embedding has a dimension of 256.

**ResNet34SE-ASP:** ResNet34SE-ASP is similar to ResNet34SimAM-ASP in terms of architecture but replaces the SimAM attention module with a squeeze-and-excitation (SE) module. The SE module aggregates global channel information as attention weights for all feature maps. The embedding dimension is also 256.

**ECAPATDNN-ASP:** ECAPA-TDNN [21] is a 1D-CNN model that has achieved great success in speaker verification. The SE-Res2Block is used to capture speaker features, and Multi-layer Feature Aggregation (MFA) is employed to process concatenated information before feeding it to the ASP. The resulting embedding has a dimension of 256.

**LCNN:** LCNN is a network commonly used for audio anti-spoofing, particularly in the ASVSpoof 2021 challenge [4]. The Max-Feature-Map (MFM) operation, based on the Max-Out activation function, is a key component in LCNN. The Bi-LSTM layer is used for pooling to aggregate utterance-level embeddings in LCNN. The resulting embedding has a dimension of 256.

**AASIST-SAP:** AASIST [12] is a waveform-level deepfake detection model. It includes a RawNet2-based [11] encoder and an attention network-based graph module. AASIST operates on raw waveforms to extract meaningful high-dimensional spectro-temporal feature maps. It then extracts graph nodes from the feature maps in both the temporal and frequency domains [12]. The final embedding is obtained by concatenating the mean and maximum values of various nodes. AASIST-SAP is an improved architecture where the max pooling layer of the encoded feature maps is replaced by a 2D self-attentive pooling (SAP) [22]. The resulting embedding has a dimension of 256.

**wav2vec-ECAPA and wavlm-ECAPA:** We adopt the Wav2vec 2.0 [23] and WavLM [24] models for front-end acoustic feature extraction in our system, respectively. Both models are large-scale self-supervised learning (SSL) pre-trained models widely used in the speech field. The effectiveness of Wav2vec in extracting acoustic features has been demonstrated in anti-spoofing scenarios [25]. By utilizing Wav2vec 2.0 and WavLM, we extract acoustic features from the input audio. These features are then fed into the ECAPA-TDNN model for further processing and embedding extraction. The resulting embedding has a dimension of 256.

### 4.2. Data processing and augmentation

For our input features, we adopt the log Mel-filterbank, log-spectrum, and waveform. The log Mel-filterbank energies have a dimension of 80, and the log-spectrum has a dimension of 257. The frame length is set to 25ms, and the hop size is set to 10ms.

To diversify the training samples, we apply on-the-fly data augmentation techniques [26]. We employ two types of augmentation methods: 1) Adding noise: We use the MUSAN dataset [27], specifically the non-speech parts, to add noise to the audio samples during training; 2) Adding convolutional reverberation: We utilize the RIR Noise datasets [28] to simulate convolutional reverberation effects and apply them to the training data.

### 4.3. Dataset analysis

#### 4.3.1. Statistic Analysis

![Figure 2: Distribution of audio durations in the train, development and evaluation set. The evaluation set is focusing on audio samples that are 20 seconds or less for ease of comparison.](image)

The experiments are performed on the ADD2023 Track3 dataset. We start by performing a statistical analysis of the train set and development set. The train set consists of 22,400 audio samples, while the development set contains...
8,400 samples. The average duration of the audio samples in the train set is 6.58 seconds, and in the development set, it is 6.84 seconds. Therefore, we randomly divide the samples into 6-second segments during training to ensure consistency in the input size. The duration distribution of the training and development sets can be observed in Figure 2.

Additionally, we observe that while the sampling rate of the training set is uniformly set to 16kHz, the development set contains audio samples with both 24kHz and 16kHz sampling rates. The sample rate of the 3rd and 4th classes in the development set is 24kHz. Some audio samples in the development set were originally at an 8kHz sampling rate but were upsampled to 16kHz. We notice that these upsampled samples may lack high-frequency information. To maintain consistency, we downsample or upsample all audio samples to a 16kHz sampling rate during training and testing.

However, the evaluation set exhibits some statistical differences compared to the training set. The evaluation set includes audio samples with sampling rates of 16kHz, 24kHz, and 44.1kHz. On the other hand, the duration distribution of the evaluation set can be seen in Figure 2. Although there are certain statistical inferences present in the evaluation set, we choose not to exploit these statistical inference in decision to ensure the generalizability of our method.

### 4.3.2. Visualization Analysis

In order to assess the similarity between the training and test data distributions, we utilized a trained embedding extractor to extract embeddings from the train, development, and evaluation sets. Subsequently, we employed a Gaussian Mixture Model (GMM) with 512 components to perform one-class modeling on the train set. By calculating the log-likelihood for all embeddings on the one-class GMM, we obtained score distributions of three sets as shown in Figure 3.

Upon analyzing the results, we observe that the score distributions of the evaluation set and development set are relatively similar. However, there is a significant disparity between the score distribution of the evaluation set and the training sets. This observation highlights the considerable challenge presented by the evaluation set in terms of testing the generalization performance of our proposed method.

In addition, we also present the t-SNE visualization of the training set and the evaluation set in Figure 4. The embeddings t-SNE used are extracted by ResNet34SimAMASP model. The label of evaluation set is marked by center-based maximum similarity method. We have observed that, except for the samples at the margins, most of the known classes can be recognized effectively. However, the unknown class does not exhibit a clear intra-class center and is not easily detected. Therefore, we speculate that the unknown class may not consist of a single category but rather a collection of multiple unknown classes.

![Figure 3: Distribution of log-likelihoods for all embeddings of the three sets. The higher the score, the higher the likelihood that the sample is from the same distribution as the training set.](image)

![Figure 4: Visualization analysis of t-SNE](image)

### 5. Results

Table 1 presents the final performance of various systems using center-based maximum similarity method. Firstly, by comparing different models with the addition of the development set (e.g., ID 1&2, ID 4&5, and ID 8&9), no clear improvement or decrease in performance was observed. This could potentially be attributed to the limited amount of data, which makes the models prone to overfitting and results in unstable performance. Based on the score distribution depicted in Figure 3, the performance on the development set alone might not fully reflect the generalization performance of the models. In addition, performance of the SSL-based models are also not satisfactorily.
Table 1
The performances of various systems with center-based maximum similarity method in the development and evaluation sets. ID 0 indicates that we only adopt 7 known centroids without unknown category.

<table>
<thead>
<tr>
<th>ID</th>
<th>Model</th>
<th>Train data</th>
<th>Feature</th>
<th>Dev Acc</th>
<th>Dev F1</th>
<th>Eval F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ResNet34SimAM-ASP (7 categories)</td>
<td>Train set</td>
<td>Mel</td>
<td>96.536</td>
<td>0.965</td>
<td>0.7150</td>
</tr>
<tr>
<td>1</td>
<td>ResNet34SimAM-ASP</td>
<td>Train set</td>
<td>Mel</td>
<td>96.536</td>
<td>0.965</td>
<td>0.7838</td>
</tr>
<tr>
<td>2</td>
<td>ResNet34SimAM-ASP</td>
<td>Train + Dev</td>
<td>Mel</td>
<td>-</td>
<td>-</td>
<td>0.7880</td>
</tr>
<tr>
<td>3</td>
<td>ResNet34GSP</td>
<td>Train</td>
<td>Mel</td>
<td>94.238</td>
<td>0.942</td>
<td>0.7650</td>
</tr>
<tr>
<td>4</td>
<td>ResNet34SE-ASP</td>
<td>Train</td>
<td>Mel</td>
<td>93.107</td>
<td>0.930</td>
<td>0.7693</td>
</tr>
<tr>
<td>5</td>
<td>ResNet34SE-ASP</td>
<td>Train + Dev</td>
<td>Mel</td>
<td>-</td>
<td>-</td>
<td>0.7398</td>
</tr>
<tr>
<td>6</td>
<td>ResNet34SE-ASP</td>
<td>Train</td>
<td>Spectrum</td>
<td>98.798</td>
<td>0.988</td>
<td>0.6006</td>
</tr>
<tr>
<td>7</td>
<td>ECAPA-ASP</td>
<td>Train</td>
<td>Mel</td>
<td>92.107</td>
<td>0.920</td>
<td>0.6402</td>
</tr>
<tr>
<td>8</td>
<td>LCNN</td>
<td>Train</td>
<td>Mel</td>
<td>96.27</td>
<td>0.9626</td>
<td>0.7628</td>
</tr>
<tr>
<td>9</td>
<td>LCNN</td>
<td>Train + Dev</td>
<td>Mel</td>
<td>-</td>
<td>-</td>
<td>0.7825</td>
</tr>
<tr>
<td>10</td>
<td>AASIST-SAP</td>
<td>Train</td>
<td>Waveform</td>
<td>95</td>
<td>0.9476</td>
<td>0.7422</td>
</tr>
<tr>
<td>11</td>
<td>Wav2vec(fixed)-ECAPA</td>
<td>Train</td>
<td>Waveform</td>
<td>97.75</td>
<td>0.9773</td>
<td>0.7075</td>
</tr>
<tr>
<td>12</td>
<td>Wav2vec(finetune)-ECAPA</td>
<td>Train</td>
<td>Waveform</td>
<td>91.17</td>
<td>0.9122</td>
<td>0.4493</td>
</tr>
<tr>
<td>13</td>
<td>WavLM(fixed)-ECAPA</td>
<td>Train</td>
<td>Waveform</td>
<td>93.04</td>
<td>0.93</td>
<td>0.6401</td>
</tr>
<tr>
<td></td>
<td>fus(0.5 × ID 1 + 0.5 × ID 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.7943</td>
</tr>
<tr>
<td></td>
<td>fus(0.3 × ID 1 + 0.25 × ID 4 + 0.3 × ID 9 + 0.25 × ID 10)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.8312</td>
</tr>
</tbody>
</table>

Figure 5: Inter-class similarity matrix for different system

Considering the utilization of the center-based maximum similarity method, the inter-class similarity matrix is computed for different models, as shown in Figure 5. By combining Table 1 and Figure 5, it is observed that better results are achieved when the inter-class similarity distances are larger. Therefore, the best single model of each system is selected by considering both the inter-class similarity matrix and the results on the development set.

Model fusion is performed at the score level to achieve complementary performance between models. Several optimal models with different modeling approaches are selected. Finally, an F1 score of 0.8312 is achieved on the evaluation set. Finally, by model fusion under the score level, we achieved the 0.8312 F1-score in the evaluation set of ADD2023 Track3.

7. Acknowledgments

This research is funded in part by the National Natural Science Foundation of China (62171207) and MaShang Consumer Finance Co.Ltd. Many thanks for the computational resource provided by the Advanced Computing East China Sub-Center.

References


