Unsupervised Representation Learning Using Convolutional Restricted Boltzmann Machine for Spoof Speech Detection

Hardik B. Sailor, Madhu R. Kamble, Hemant A. Patil

Speech Research Lab, Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT), Gandhinagar-382007, Gujarat, India
{sailor_hardik, madhu_kamble, hemant_patil}@daiict.ac.in

Abstract

Speech Synthesis (SS) and Voice Conversion (VC) presents a genuine risk of attacks for Automatic Speaker Verification (ASV) technology. In this paper, we use our recently proposed unsupervised filterbank learning technique using Convolutional Restricted Boltzmann Machine (ConvRBM) as a front-end feature representation. ConvRBM is trained on training subset of ASV spoof 2015 challenge database. Analyzing the filterbank trained on this dataset shows that ConvRBM learned more low-frequency subband filters compared to training on natural speech database such as TIMIT. The spoofing detection experiments were performed using Gaussian Mixture Models (GMM) as a back-end classifier. ConvRBM-based cepstral coefficients (ConvRBM-CC) perform better than hand crafted Mel Frequency Cepstral Coefficients (MFCC). On the evaluation set, ConvRBM-CC features give an absolute reduction of 4.76 % in Equal Error Rate (EER) compared to MFCC features. Specifically, ConvRBM-CC features significantly perform better in both known attacks (1.93 %) and unknown attacks (5.87 %) compared to MFCC features.

Index Terms: Automatic Speaker Verification, spoofing, countermeasures, ConvRBM, filterbank.

1. Introduction

Automatic Speaker Verification (ASV) or voice biometrics is the task of verifying the claimed identity of a person from his or her voice with the help of machines [1]. However, the practical ASV systems are vulnerable to the biometric attacks. The major forms of the attack known today includes voice conversion (VC) [2], speech synthesis (SS) [3], replay [4], and impersonation [5], which are known to degrade the performance of ASV systems [1]. The general countermeasure approach is one of the solutions to focus on feature representation and statistical pattern recognition techniques. In particular, feature representation forms key task for spoof speech detection (SSD). The aim is to distinguish between genuine and impostor speech by capturing the key discriminative features between two speech signals. This might suggest that the design of spoofing countermeasures should better focus on feature representation, rather than on the advanced or complex classifiers [6, 7].

The details of various approaches used for the SSD task both for the ASVspoof 2015 challenge and post evaluation results are given in [8]. Most of the ASV systems used Fourier transform (FT) magnitude-based and phase-based features from the speech signal. The detailed analysis of various features for ASVspoof 2015 challenge database is presented in [7]. The representation of a speech signal based on human speech perception is of significant interest in developing features for speech processing applications. Classical auditory models were developed to mimic the human auditory system in the 1980s. These auditory models are based on mathematical modeling of auditory processing or psychophysical and physiological experiments. Mel Frequency Cepstral Coefficients (MFCC) [9] are one of the state-of-the-art auditory-based features for spoof detection. The ASVspoof 2015 challenge winner system uses auditory-inspired features Cochlear Filter Cepstral Coefficients-Instantaneous Frequency (CFCCIF) [10,11]. Recently, auditory-inspired Constant-Q Cepstral Coefficients (CQCC) also perform better compared to MFCC features specifically in detecting spoof by unit selection speech synthesis system [12, 13]. Such handcrafted features rely on simplified auditory models [14, 15].

Representation learning has gained a significant interest for feature learning in various signal processing areas including speech processing [16]. For the SSD task, various approaches were proposed using representation learning (i.e., deep learning) techniques. In [17], deep features were learned using deep neural network (DNN) from the Mel filterbank. Deep features were learned using deep learning architectures, namely, DNN and Recurrent Neural Networks (RNN) and applied on various classifiers such as linear discriminant analysis (LDA) [18]. DNN-based bottleneck features were also used with Gaussian Mixture Models (GMM) classifier in [19]. An end-to-end learning from the raw speech signals for the SSD task is also recently proposed [20] where it was evaluated for BTAS2016 challenge database [21]. These studies show that instead of conventional handcrafted features, the features learned using the machine learning techniques perform better for the SSD task. Recently, we proposed a Convolutional Restricted Boltzmann Machine (ConvRBM) for unsupervised filterbank learning directly from the raw speech signals. The review of different methods for unsupervised filterbank learning is given in [22]. ConvRBM filterbank was shown to perform better than MFCC and Mel filterbank features for speech recognition task [22, 23].

In this paper, we propose to exploit our approach of the unsupervised filterbank learning using ConvRBM for the SSD task. The filterbank learned using ConvRBM was used to extract the features from the genuine and spoofed speech signals. Compared to our earlier works [22, 23], here we have used an Adam optimization [24] in ConvRBM training. The experiments on ASV 2015 database shows that ConvRBM-based features perform better than MFCC features.

2. Convolutional RBM

Convolutional Restricted Boltzmann Machine (ConvRBM) is an unsupervised probabilistic model with two layers, namely, visible layer and hidden layer [25]. Here, we have used ConvRBM to learn an auditory-like subband filters from the utterance-level raw speech signals [22, 23]. The block diagram
of the arrangement of hidden units is shown in Figure 1. The input \( x \) to ConvRBM is an entire speech signal. The hidden layer consists of \( K \) groups. Weights \( (\mathbf{W}^k) \) are shared between visible and hidden units among all the locations in each group \((k = 1, \ldots, K)\). \( b_k \) and \( c \) are hidden and visible biases that are also shared. For the \( k^{th} \) subband, the input to the hidden layer is given as, \( \mathbf{h}_k = (x * \mathbf{W}^k) + b_k \), where \(*\) is a convolution operation and \( \mathbf{W} \) denote the flipped array [25]. With a noisy rectifier linear units (NReLU), the sampling equations for hidden and visible units \( (x_{recon} \text{ to reconstruct the speech}) \) are given as [22, 23]:

\[
\begin{align*}
\mathbf{h}^k & \sim \max(0, \mathbf{I}_k + N(0, \sigma(I_k))), \\
\mathbf{x}_{recon} & \sim \mathcal{N}(\sum_{k=1}^{K}(\mathbf{h}^k * \mathbf{W}^k) + c, 1),
\end{align*}
\]

where \( N(0, \sigma(I_k)) \) is a Gaussian noise with mean zero and sigmoid of \( \mathbf{I}_k \) as a variance and \( \mathbf{x}_{recon} \) is a reconstructed speech signal (visible units). We have used single-step contrastive divergence (CD-1) to train the model [26]. Parameters are updated using Adam optimization method [24]. It was shown that Adam optimization perform better than stochastic gradient-based methods due to use of first and second order moments of the gradient and bias correction terms [24].

Figure 1: The arrangement of hidden units in \( K \) groups and corresponding weight connections. The filter index-axis is perpendicular to the plane of this paper. Each hidden unit (red dots) in the \( k^{th} \) group is wired such that it results in a valid convolution between the speech signal and weights \( \mathbf{W}^k \). After [22].

![Figure 1](image)

Figure 2: Feature extraction using trained ConvRBM. (a) speech signal, (b) and (c) responses from the convolutional layer and ReLU nonlinearity, respectively, (d) representation after pooling, (e) logarithmic compression. After [22].

After ConvRBM is trained, average pooling is applied to reduce the representation of ConvRBM filter responses in the temporal-domain. Here, pooling in the time-domain is equivalent to short-time averaging in spectral features. For a speech signal of the sampling frequency, \( F_s = 16 \) kHz, pooling is applied using 25 ms window length and 10 ms window shift. Pooling is performed across time and separately for each subband filter. We have experimented with both average and max-pooling and found better results with average pooling. Figure 2 shows the block diagram for feature extraction procedure. During the feature extraction stage, we used the ‘same’ length convolution and deterministic ReLU nonlinearity \( max(0, \mathbf{I}_k) \) as an activation function. The pooling operation reduces the temporal resolution from \( K \times n \) samples to \( K \times F \) frames. Logarithmic nonlinearity compresses the dynamic range of features.

3. Analysis of the ConvRBM filterbank

3.1. Analysis of subband filters

The ConvRBM is trained using the training set of ASVspoof Challenge 2015 database. Figure 3 shows the subband filters learned using ConvRBM trained on entire training set (denoted as ConvRBM-TrainingAll), synthetic speech from the training set (denoted as ConvRBM-TrainingSyn) of ASVspoof 2015 database and TIMIT database (denoted as ConvRBM-TIMIT). We have analyzed the model with \( K = 40 \) subband filters for all the cases. We found the center frequencies (CFs) of subband filters as described in [22]. Filters were arranged according to their increasing order of CFs. Weights of the model called as impulse responses of the subband filters in time-domain shown in Figure 3 (a)-(c) and the corresponding frequency responses are shown in Figure 3 (d)-(f). The time-domain subband filters of ConvRBM-TrainingAll and ConvRBM-TrainingSyn are different than ConvRBM-TIMIT whose subband filters resemble more to the Gammatone impulse responses. However, the filterbanks of ConvRBM-TrainingAll and ConvRBM-TrainingSyn includes more lower frequency subband filters with many of the subband filters are wavelet-like basis functions (see the short duration impulses responses in Figure 3 (a), (b)). We can also see that all the subband filters are localized in the frequency-domain with different CFs except in the synthetic speech case as shown in Figure 3 (e). The training set of ASVspoof 2015 database contains 3750 utterances of the natural speech and 16225 utterances of the synthetic speech. Hence, the ConvRBM subband filters trained on training set (that includes both natural and synthetic speech) adapted more towards representing the synthetic speech signals. From the frequency-domain representation of filters, we can see that it also limits the model to represent higher frequencies, which are difficult to model in the synthetic speech signals, such as, fricative and transient sounds.

3.2. Filterbank scale analysis

In order to compare the learned filterbank with the standard auditory filterbanks, we have shown a CFs vs. subband filter index plot in Figure 4. We have also shown the frequency scale of ConvRBM-TIMIT that follows the Equivalent Rectangular Bandwidth (ERB) scale. The filterbank learned using ConvRBM-TrainingAll, ConvRBM-TrainingSyn and ConvRBM-TrainingNat (natural speech from the training set) use more number of lower frequency subband filters compared to rest of the filterbanks. The frequency scale of ConvRBM-TrainingNat is slightly different in the frequency range 1-3 kHz compared to ConvRBM-TrainingAll and ConvRBM-TrainingSyn. However, the frequency scales of ConvRBM-TrainingNat and ConvRBM-TIMIT alone are sig-
Figure 3: Examples of subband filters trained on entire training set of ASVspoof 2015 (Panel I), synthetic speech of ASVspoof 2015 (Panel II) and TIMIT (Panel III) databases, respectively: (a)-(c) subband filters in time-domain (i.e., impulse responses), (d)-(f) subband filters in frequency-domain (i.e., frequency responses).

Significantly different after 1 kHz. Since ConvRBM is a statistical model, it better learns the subband filters with more diverse database and encode the statistical properties of the underlying database (such as 462 speakers in TIMIT vs. 25 speakers in the training set of ASVspoof 2015). We also observe that model is biased towards the synthetic speech due to large number of examples compared to natural speech in the training set.

Figure 4: Comparison of the filterbank learned using ConvRBM with auditory filterbanks.

4. Experimental Setup

4.1. ASVspoof 2015 database

The experiments are conducted on the ASVspoof Challenge 2015 database [1]. It consists of speech data without channel or background noise collected from 106 speakers (45 male and 61 female). It is divided into three subsets: training, development and evaluation set. More detailed description of the database is discussed in [27].

4.2. Training of ConvRBM and feature extraction

We have trained ConvRBM on training subset of ASVspoof Challenge 2015 database for the SSD task. Each speech signal after mean-variance normalization was applied to ConvRBM. The filter length is chosen to be $m=128$ samples (i.e., 8 ms) similar to as in [22]. The learning rate was chosen to be 0.0001 and decayed at each epoch according to the learning rate scheduling as suggested in [24]. The moment parameters of Adam optimization chosen to be $\beta_1=0.9$ and $\beta_2=0.999$. We have trained the model with a different number of ConvRBM filters, with average and max-pooling. After the model was trained, the features were extracted from speech signal with details shown in Figure 2. To reduce the dimension and compare the proposed features with MFCC features, the Discrete Cosine Transform (DCT) was applied and only first 13-D were retained. Delta and delta-delta features were also appended resulting in 39-D cepstral features (denoted as ConvRBM-CC).

Table 1: The results of different parameters of ConvRBM-CC features on the development set in % EER

<table>
<thead>
<tr>
<th>Features</th>
<th>No. of filters ($K$)</th>
<th>Pooling</th>
<th>% EER</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFCC</td>
<td>40</td>
<td>-</td>
<td>6.14</td>
</tr>
<tr>
<td>ConvRBM-CC</td>
<td>60</td>
<td>average</td>
<td>3.71</td>
</tr>
<tr>
<td>A:ConvRBM-CC</td>
<td>40</td>
<td>average</td>
<td>3.18</td>
</tr>
<tr>
<td>B:ConvRBM-CC</td>
<td>40</td>
<td>max</td>
<td>2.53</td>
</tr>
<tr>
<td>A+MFCC</td>
<td>40</td>
<td>-</td>
<td>2.80</td>
</tr>
<tr>
<td>B+MFCC</td>
<td>40</td>
<td>-</td>
<td>2.31</td>
</tr>
</tbody>
</table>

4.3. Model training and score-level fusion

We have used Gaussian Mixture Model (GMM) with 128 mixtures for modeling the two classes, in which the classes correspond to the genuine and impostor in ASVspoof 2015 database. The GMMs are trained with the training set of the database. The use of GMM classifier has been shown to perform best in the detection of genuine vs. impostor speech in the ASVspoof 2015 challenge [28]. Final scores are represented in terms of the log-likelihood ratio (LLR).

The decision of test speech being genuine or impostor and the score-level fusion of features are done as in [10].
5. Experimental Results

5.1. Results on Development Dataset

The results on the development set for the individual performance of 39-D (static+$\Delta$+$\Delta\Delta$) MFCC and ConvRBM-CC with different parameters (number of subband filters $K$ and pooling techniques) are shown in Table 1. It is observed that ConvRBM-CC features (3.71-2.53 % EER) gave relatively better performance compared to MFCC features (6.14 % EER). However, increasing number of subband filters (i.e., $K=60$) does not improve the performance of classification compared to smaller number of subband filters (i.e., $K=40$). Lowest % EER is achieved using max pooling and 40 number of subband filters. We have used 40 subband filters for rest of the experiments. The score-level fusion of ConvRBM-CC ($K=40$, average and max pooling) with MFCC further reduces % EER. This shows that ConvRBM-CC features contain complementary information that was not evident from MFCC features alone. The DET curves of MFCC and ConvRBM-CC with different parameters are shown in Figure 5.

![Figure 5: The DET curve for performance of ConvRBM-CC (60, 40 filters with max and average pooling) and MFCC features on the development set.](image)

5.2. Results on Evaluation Dataset

Table 2 shows the performance of ConvRBM-CC features for each of the different spoofing attacks grouped into known and unknown attacks with their average EERs for known and unknown spoofing attacks. It is observed that ConvRBM-CC features perform better than MFCC features on the evaluation set in all the spoofing attacks. ConvRBM-CC with the max-pooling perform better then average-pooling for known attacks (S1-S5). However, in the case of unknown attacks specifically S10 (unit selection speech synthesis), the average-pooling perform better (22.64 %) than the max-pooling (33.20 % EER). Due to dominance of S10 % EER, the average pooling gave lowest EER of 5.87 % in unknown attacks compared to the max-pooling (7.69 %) and MFCC (13.76 %). Compared to the development set, ConvRBM-CC with the average-pooling perform better than the max-pooling on the evaluation set with lowest EER 3.90 % on an average. To observe whether any complementary information is being captured in the average and max-pooling of ConvRBM-CC, score-level fusion is performed. It resulted in the reduction of % EER in few cases and increased % EER including S10. We have also performed the score-level fusion of MFCC and ConvRBM-CC with the average-pooling. Here, the fusion reduce the % EER for all the attacks except S2, S6 and S10 (with significantly high % EER). Hence, the individual ConvRBM-CC with average pooling performed well in the SSD task. A comparison of the proposed feature representation with the literature (state-of-the-art and feature learning methods) is shown in Table 3. Compared to the supervised features obtained using DNN with LDA/GMM classifiers [18], [19], our unsupervised filterbank learned using ConvRBM perform better in S10 class and similar % EER on an average in unknown attacks. It also perform better than supervised Spectro/CNN [29] in S10 and resulted in similar % EER for unknown attacks and on an average. Given the success of a RNN, we would also like to use it as a back-end instead of GMM. CQCC features gave the lowest results achieved on the ASVspoof 2015 databases.

![Table 2: Results on evaluation dataset for each spoofing attack in terms of % EER](image)

<table>
<thead>
<tr>
<th>Feature Set</th>
<th>Known Attacks</th>
<th>Unknown Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFCC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S1</td>
<td>S2</td>
</tr>
<tr>
<td>A:ConvRBM-CC(avg)</td>
<td>0.00</td>
<td>5.68</td>
</tr>
<tr>
<td>B:ConvRBM-CC(max)</td>
<td>0.00</td>
<td>3.61</td>
</tr>
<tr>
<td>A+B</td>
<td>0.35</td>
<td>3.70</td>
</tr>
<tr>
<td>MFCC+A</td>
<td>0.00</td>
<td>4.13</td>
</tr>
</tbody>
</table>

6. Summary and Conclusions

In this study, we propose to use the unsupervised filterbank learning using ConvRBM for the SSD task. The filterbank learned on training set shows that the frequency scale is different than the one learned using natural signals. It is observed that due to more number of synthetic speech in the training set, ConvRBM filterbank is more biased to the synthetic speech signals. The experimental results on the development and evaluation set shows that ConvRBM-CC features with the average-pooling perform better than the MFCC features. Our future works includes detailed analysis of natural and spoof speech regarding the nature of subband filters and frequency scale. We would also like use our Unsupervised Deep Auditory Model (UDAM) [30] along with TEO [31] for the SSD task.
7. References


