<table>
<thead>
<tr>
<th>Title</th>
<th>Spoofing speech detection using temporal convolutional neural network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Tian, Xiaohai; Xiao, Xiong; Chng, Eng Siong; Li, Haizhou</td>
</tr>
<tr>
<td>Date</td>
<td>2016</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/47064">http://hdl.handle.net/10220/47064</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<a href="http://dx.doi.org/10.1109/APSIPA.2016.7820738">http://dx.doi.org/10.1109/APSIPA.2016.7820738</a>].</td>
</tr>
</tbody>
</table>
Spoofing Speech Detection using Temporal Convolutional Neural Network

Xiaohai Tian∗†, Xiong Xiao‡, Eng Siong Chng∗†‡ and Haizhou Li∗§

∗ School of Computer Science and Engineering, Nanyang Technological University (NTU), Singapore
† Joint NTU-UBC Research Center of Excellence in Active Living for the Elderly, NTU, Singapore
‡ Temasek Laboratories, NTU, Singapore
§ Department of Electrical and Computer Engineering, National University of Singapore

Email: {xhtian,xiaoiong,ASESChng}@ntu.edu.sg, eleliha@nus.edu.sg

Abstract—Spoofing speech detection aims to differentiate spoofing speech from natural speech. Frame-based features are usually used in most of previous works. Although multiple frames or dynamic features are used to form a super-vector to represent the temporal information, the time span covered by these features are not sufficient. Most of the systems failed to detect the non-vocoder or unit selection based spoofing attacks. In this work, we propose to use a temporal convolutional neural network (CNN) based classifier for spoofing speech detection. The temporal CNN first convolves the feature trajectories with a set of filters, then extract the maximum responses of these filters within a time window using a max-pooling layer. Due to the use of max-pooling, we can extract useful information from a long temporal span without concatenating a large number of neighbouring frames, as in feedforward deep neural network (DNN). Five types of feature are employed to access the performance of proposed classifier. Experimental results on ASVspoof 2015 corpus show that the temporal CNN based classifier is effective for synthetic speech detection. Specifically, the proposed method brings a significant performance boost for the unit selection based spoofing speech detection.

I. INTRODUCTION

With the development of speech synthesis (SS) and voice conversion (VC) techniques, the state-of-the-art systems are able to generate high quality and natural speech with small amount of speech data from target speaker [1, 2]. On the other hand, this also imposes a significant threat to automatic speaker verification (ASV) systems, as the ASV system can be easily attacked by the spoofed speech generate by these techniques [3, 4]. Hence, spoofing speech detection is highly demanded to protect the ASV system.

The common way for spoofing speech detection is to build some standalone detection systems using different countermeasures. In previous studies, various feature based countermeasures are proposed. To detect the artifacts of phase, a number of phase-based features have been used, such as modified group delay (MGD) [5, 6, 7, 8], cosine-normalized phase [5, 8], relative phase shift (RPS) [9, 10, 11, 12], cochlear filter cepstral coefficients plus instantaneous frequency (CFC-CIF) [13]. To detect the artifacts of magnitude, several magnitude based features are also used, such as Mel-frequency cepstrum coefficient (MFCC) [14, 15], linear frequency cepstral coefficients (LFCC) [16], Subband centroid frequency coefficient (SCFC) [17] and so on. These features, however, are generally low-dimensional to facilitate certain classifiers, such as Gaussian mixture model (GMM) [6, 14, 18]. The dimension reduction process compresses the features based on human perception and may discard the important information for spoofing speech detection. This may degrade the system performance.

In [7], a neural network (NN) based classifier is proposed to handle the high-dimensional features in order to use detailed information for the detection. For the NN based system using high-dimensional features, all the vocoder-based spoofing speech are detected with the equal error rate (EER) of 0%. However, most of the systems mentioned above use frame-based feature, which does not contain enough temporal information to detect the spoofing speech without using vocoder, for example unit selection based spoofing attacks. Due to the frames of unit selection based spoofing attacks are from natural speech and the artifacts occasionally appears in concatenating points. A feature covering long temporal span information, may up to 100 frames, is needed to capture such artifacts for detection. Hence, although multiple frames (51 frames) [7] and dynamic features [17, 19] have been proposed to capture the temporal artifacts, the detection systems still failed to detect the spoofing speech generated by unit selection based techniques.

Nowadays, convolutional neural network (CNN) is widely used and shows the potential to in achieving good performance in classification and recognition tasks, such as video classification [20], image classification [21], face recognition [22], speech recognition [23] and so on. Inspired by the success of these works, in this paper, we propose a temporal CNN [24] based classifier for spoofing speech detection. Especially, our focus is on unit selection based spoofing speech detection. There are two major advantages of using temporal CNN based classifier for spoofing speech detection. First, as a NN-based classifier, temporal CNN is capable to deal with the high-dimensional features. Second, the max-pooling layer, which outputs the maximum value within long term span, can capture long term temporal information. This temporal information is especially useful to detect the unit selection based spoofing attacks, which the artifacts only appear in concatenation point with a long time span.
II. SYSTEM ARCHITECTURE

The temporal CNN based detection system, as shown in Figure 1, contains a front-end feature extraction and a back-end classifier. The details of these parts are introduced as follows.

A. Front-end Feature Extraction

Similar to our previous system [7, 19], five types of feature, including log magnitude spectrum (LMS), instantaneous frequency derivative [25] (IF), baseband phase difference [26] (BPD), group delay [27] (GD) and modified group delay [27] (MGD), are extracted.

For each frame, the magnitude and phase spectrum are first obtained by applying short-time Fourier transform (STFT) on the speech signal using analysis window of 25ms with 15ms overlap. The Hamming window and direct current (DC) offset is applied on each analysis frame. Then, the magnitude-based feature, LMS, is derived from magnitude spectrum. IF, BPD, GD and MGD are derived from phase spectrum. In our implementation, the FFT length is chosen to be 512 and the dimension of all the original features are 256. The details of feature extraction can be found in [7, 28].

B. Back-end Classifier

As shown in Figure 2, the temporal CNN based classifier consists of three types of layer: a convolutional layer, a max-pooling layer and a feedforward layer. The convolution layer applies a set of filters that process small regions of the input features along time axis. The max-pooling layer takes the maximum filter responses from a sliding window to form a lower resolution representation of the convolution layer output. Then, the outputs of the max-pooling layer are fed to the feedforward layer for further prediction.

1) Convolutional Layer: In conventional CNN, a convolutional layer consist of a set of filters. During the forward pass, each filter slides across the width and height of the input features and the filter is convolved with a subregion of the input features. Each filter is a weight matrix, and all the input features share the same weights to compose a feature map. Thus, the convolutional layer composes many feature maps generated by different filters. In practice, we random initialize the weight matrix, and the weights are learned via backpropagation.

In temporal CNN, the height of the filter is the same as the dimension of input feature. Thus the filter slides and convolves in one direction. Specifically, for speech application, the filter height is cover the whole frequency axis, and the convolution is only applied along the time axis. Hence, in this sense, the output of convolutional layer are feature trajectories substituted to feature maps, as shown in figure 2.

2) Max-pooling Layer: A max-pooling layer is usually added on top of the convolution layer. It divides the outputs of the convolutional layer into local regions. Each local region will be down-sampled with the maximum value from that region.

For temporal CNN, as the outputs of the convolutional layer are one dimensional feature trajectories, the major function of max-pooling process is capturing the important local structures distributed over time. In our spoofing speech detection task, it is effective to detect the long time span temporal artifacts, such as the unit selection based spoofing attacks.

III. EXPERIMENTS

A. Experimental Setup

1) Database: To assess the performance of the temporal CNN based classifier, the ASVspoof 2015 database [29] is used in this work. Ten types of spoofing attack are included in this database, namely S1 to S10. The database consists of three subsets, including training set, development set and evaluation set. The training and development sets only contain the S1 to S5 spoofing attacks. The evaluation set consists of all the ten types of spoofing attack. Refer to our previous results [7, 28], it is observed that the results on the development set are similar to that of the S1 to S5 on the evaluation set. Hence, only the training set and the evaluation set are used in this work.

2) Detection Systems: To validate our proposals, the previous MLP based system [28] is used as the reference baseline. We describe the detail information as follows.

- **MLP based system**: Each of the features mentioned above with its delta and acceleration coefficients is used as the input vector to train its own classifier. The MLP consists of one hidden layer with 2,048 sigmoid nodes is used to perform frame-wise classification. Given testing utterance, the posterior probabilities of all the frames are estimated and averaged over the test utterance.

- **Temporal CNN based system**: The convolutional layer contains 512 filters. Each filter has a size of 256 × 11, which means the filter covers all the 256 frequency bins and contains 11 successive frames. Then 512 feature
trajectories are generated by convolutional layer. The max-pooling layer down-samples the feature trajectories with the maximum values over a overlapped window of 100 frames with 80 frames overlap. The outputs of the max-pooling layer are fed to the feedforward layer with 2,048 sigmoid nodes. Finally, we use the softmax to predict the posterior probability of the input features.

To avoid the influence of the silence patches, a pitch based voice activity detector (VAD) is used to discard scores of silence at the beginning and the ending of the utterance.

3) Evaluation metrics and fusion: The equal error rate (EER), where the false acceptance rate and the miss rejection rate becomes equal, is used to evaluate the system performance.

A system fusion is applied on the feature-based results to benefit the advantages of different features. To avoid the over-fitting problem, the same weight is assigned to all systems. Then the fusion is adopted by averaging the scores of all systems to produce the final score.

In this work, the Bosaris toolkit\textsuperscript{1} is used to compute the EERs of each feature and the fused system.

B. Results and Analysis

1) Evaluation with mismatched data: Table I summarizes the experimental results in terms of evaluation with mismatched types of spoofing attacks. Specifically, we use the training set to train the classifiers and perform the evaluation on the evaluation set.

We first exam the effectiveness of the temporal CNN based system across different types of spoofing attack. For better analysis, we divide the spoofing attacks into two categorise: S1-S9, using vocoders and low-dimensional features used for generation; S10, generated by waveform-based unit selection.

From the preliminary results, some observations are found. First, although S6-S9 are only available during evaluation, the results of the MLP based system are comparable to that of S1-S5. This is due to the vocoders and low-dimensional features used for S6-S9 attacks generation are similar as S1-S5. As expected, similar phenomenons are observed in temporal CNN based system.

Second, in general, for S1-S9 attacks, the MLP based system slightly outperform to the temporal CNN based system. An example of the score distributions of two systems using LMS feature are showed in Figure 3 and Figure 4. This is due to the analysis and synthesis process of vocoder is based on frame. Thus the artificial cues of vocoder-based spoofing attacks will appear in each frames. The max-pooling layer of the temporal CNN based system, however, tends to down-sample the features in a long time span, i.e. 100 frames in our implementation, so some information are discarded. On the contrary, the MLP based system is capable to preserve all the feature details. Hence lead to a better performance on vocoder-based spoofing attacks.

Third, for both the MLP and the temporal CNN based systems, S10 performs worse than S1-S9. However, it is observed that in general the temporal CNN based system is notably outperform the MLP based system. Take LMS feature based

\textsuperscript{1}https://sites.google.com/site/bosaristoolkit/
system as an instance. As shown in Figure 3 and Figure 4, it is observed that compared to the MLP based system, the temporal CNN based system can easily discriminate S10 from natural speech, and reduces the EER of 21.59% (from 35.24% to 13.65%). This indicates that the temporal CNN based classifier can effectively improve the system performance on unit selection based spoofing speech detection, owing to its capability to capture the long term temporal information.

Then, we examine the temporal CNN based system performance using different features. We observe that in the MLP based system the best performance on evaluation set is obtained by the BPD feature achieving an averaged EER of 3.16%. While in the temporal CNN based system, the GD feature performs best with an averaged EER of 1.40%. However, the BPD feature in the temporal CNN based system performs much worse than in MLP based system, especially for S10 detection.

By applying the feature fusion, finally the MLP and the temporal CNN based system obtain the averaged EER of 2.87% and 1.41%, respectively. This implies the temporal CNN based system offer overall better performances than the MLP based system.

2) Evaluation with matched data: To further validate the performance of both MLP and temporal CNN based system, we adopt an experiment with matched types of spoofing attacks of training and evaluation. Hence, we divide the evaluation set into two parts, each types of spoofing attacks and natural speech are equally assigned into these two part. One part is used to train the classifiers and the evaluation is performed on the other part. Table II summarizes the experimental results.

We first analyze the performance of the MLP based system. It is surprisingly to observe that the performance of the MLP based system is significant degraded by including all the ten types of spoofing attacks in classifier training. Even after system fusion using different features, the averaged EER is 3.60%. Figure 5 shows an example of score distribution using LMS feature to train the MLP based system. We observe that the scores of spoofing attacks are overlapped with that of natural speech. It because the MLP based system performs frame-wise with short windows for training and classification. For unit selection based spoofing attack (S10), during the short window the training vectors of S10 are highly similar to natural speech, as each frame of S10 is actually from natural speech. This will inevitably decrease the discrimination power of the classifier and degrade the system performance.

Then we analyze the performance of the temporal CNN based system. For S6-S9 attacks, even all these spoofing types attack are observed during training, the performance of temporal CNN based system almost consistent with previous results. This is due to S6-S9 attacks are vocoded speech which is similar as S1-S5. They may not provide additional useful

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Feature</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
<th>S5</th>
<th>S6</th>
<th>S7</th>
<th>S8</th>
<th>S9</th>
<th>S10</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLP</td>
<td>LMS</td>
<td>0.02</td>
<td>0.02</td>
<td>0.01</td>
<td>0.01</td>
<td>0.02</td>
<td>0.01</td>
<td>0.01</td>
<td>0.00</td>
<td>0.01</td>
<td>35.24</td>
<td>3.53</td>
</tr>
<tr>
<td></td>
<td>IF</td>
<td>1.30</td>
<td>1.30</td>
<td>1.30</td>
<td>1.30</td>
<td>1.34</td>
<td>1.32</td>
<td>1.30</td>
<td>1.30</td>
<td>1.30</td>
<td>25.56</td>
<td>3.73</td>
</tr>
<tr>
<td></td>
<td>BPD</td>
<td>0.06</td>
<td>0.05</td>
<td>0.00</td>
<td>0.00</td>
<td>0.41</td>
<td>0.23</td>
<td>0.05</td>
<td>0.04</td>
<td>0.03</td>
<td>30.67</td>
<td>3.16</td>
</tr>
<tr>
<td></td>
<td>GD</td>
<td>0.02</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
<td>0.20</td>
<td>0.09</td>
<td>0.00</td>
<td>0.01</td>
<td>0.00</td>
<td>33.90</td>
<td>3.42</td>
</tr>
<tr>
<td></td>
<td>MGD</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.02</td>
<td>0.06</td>
<td>0.03</td>
<td>0.00</td>
<td>0.00</td>
<td>38.54</td>
<td>3.87</td>
</tr>
<tr>
<td></td>
<td>Fusion</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>28.72</td>
<td>2.87</td>
</tr>
<tr>
<td>Temporal CNN</td>
<td>LMS</td>
<td>1.55</td>
<td>0.92</td>
<td>0.32</td>
<td>0.36</td>
<td>1.06</td>
<td>0.95</td>
<td>1.62</td>
<td>4.02</td>
<td>0.89</td>
<td>13.65</td>
<td>2.53</td>
</tr>
<tr>
<td></td>
<td>IF</td>
<td>0.28</td>
<td>0.29</td>
<td>0.07</td>
<td>0.06</td>
<td>0.58</td>
<td>0.47</td>
<td>0.20</td>
<td>0.29</td>
<td>0.09</td>
<td>20.08</td>
<td>2.24</td>
</tr>
<tr>
<td></td>
<td>BPD</td>
<td>0.66</td>
<td>0.91</td>
<td>0.13</td>
<td>0.16</td>
<td>1.54</td>
<td>1.25</td>
<td>0.75</td>
<td>0.65</td>
<td>0.39</td>
<td>38.19</td>
<td>4.46</td>
</tr>
<tr>
<td></td>
<td>GD</td>
<td>0.16</td>
<td>0.12</td>
<td>0.13</td>
<td>0.12</td>
<td>0.27</td>
<td>0.37</td>
<td>0.10</td>
<td>0.10</td>
<td>0.08</td>
<td>12.50</td>
<td>1.40</td>
</tr>
<tr>
<td></td>
<td>MGD</td>
<td>0.29</td>
<td>0.25</td>
<td>0.13</td>
<td>0.13</td>
<td>0.58</td>
<td>0.45</td>
<td>0.24</td>
<td>0.17</td>
<td>0.10</td>
<td>27.20</td>
<td>2.95</td>
</tr>
<tr>
<td></td>
<td>Fusion</td>
<td>0.10</td>
<td>0.08</td>
<td>0.01</td>
<td>0.03</td>
<td>0.13</td>
<td>0.10</td>
<td>0.06</td>
<td>0.06</td>
<td>0.04</td>
<td>13.51</td>
<td>1.41</td>
</tr>
</tbody>
</table>
The experiments results show that,

- compare to the MLP based classifier, the temporal CNN based classifier can effectively boost the performance of unit selection based spoofing attack detection;
- when including the S10 in training, the performance of the temporal CNN based system for unit selection based spoofing attack is improved significantly.

However, there is a degradation of the temporal CNN based system for vocoder based spoofing attacks detection. This will become a research point of our following work. Moreover, as inconsistent performance is observed using BPD feature in two systems, in future, we will investigate the robustness of features for spoofing speech detection.

**IV. CONCLUSIONS**

In this paper, we investigate the used of the temporal CNN based classifier to discriminate synthetic spoofing attacks and natural speech. The experiments results show that,

- compare to the MLP based classifier, the temporal CNN based classifier can effectively boost the performance of unit selection based spoofing attack detection;
- when including the S10 in training, the performance of the temporal CNN based system for unit selection based spoofing attack is improved significantly.

However, there is a degradation of the temporal CNN based system for vocoder based spoofing attacks detection. This will become a research point of our following work. Moreover, as inconsistent performance is observed using BPD feature in two systems, in future, we will investigate the robustness of features for spoofing speech detection.

**ACKNOWLEDGMENT**

This research is supported by the National Research Foundation, Prime Ministers Office, Singapore under its IDM Futures Funding Initiative. This work is also supported by the DSO funded project MAISON DSOCL14045, Singapore.

**REFERENCES**


**TABLE II**

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Feature</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
<th>S5</th>
<th>S6</th>
<th>S7</th>
<th>S8</th>
<th>S9</th>
<th>S10</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLP</td>
<td>LMS</td>
<td>0.86</td>
<td>1.17</td>
<td>1.39</td>
<td>1.44</td>
<td>2.16</td>
<td>1.45</td>
<td>0.92</td>
<td>0.12</td>
<td>0.91</td>
<td>36.99</td>
<td>4.74</td>
</tr>
<tr>
<td></td>
<td>IF</td>
<td>0.64</td>
<td>0.94</td>
<td>0.12</td>
<td>0.12</td>
<td>3.49</td>
<td>3.27</td>
<td>0.30</td>
<td>0.12</td>
<td>0.20</td>
<td>33.24</td>
<td>4.24</td>
</tr>
<tr>
<td></td>
<td>BPD</td>
<td>0.40</td>
<td>0.75</td>
<td>0.05</td>
<td>0.06</td>
<td>2.95</td>
<td>1.75</td>
<td>0.37</td>
<td>0.18</td>
<td>0.25</td>
<td>34.78</td>
<td>4.15</td>
</tr>
<tr>
<td></td>
<td>MGD</td>
<td>0.96</td>
<td>1.82</td>
<td>1.00</td>
<td>1.22</td>
<td>6.79</td>
<td>6.99</td>
<td>1.99</td>
<td>0.27</td>
<td>0.63</td>
<td>42.46</td>
<td>6.44</td>
</tr>
<tr>
<td>Fusion</td>
<td>LMS</td>
<td>0.08</td>
<td>0.12</td>
<td>0.04</td>
<td>0.04</td>
<td>0.31</td>
<td>0.36</td>
<td>0.07</td>
<td>0.02</td>
<td>0.03</td>
<td>34.89</td>
<td>3.60</td>
</tr>
<tr>
<td></td>
<td>IF</td>
<td>0.33</td>
<td>0.36</td>
<td>0.15</td>
<td>0.10</td>
<td>0.96</td>
<td>0.85</td>
<td>0.19</td>
<td>0.40</td>
<td>0.13</td>
<td>8.42</td>
<td>1.19</td>
</tr>
<tr>
<td></td>
<td>BPD</td>
<td>2.05</td>
<td>5.25</td>
<td>3.23</td>
<td>3.42</td>
<td>7.75</td>
<td>9.00</td>
<td>2.89</td>
<td>1.66</td>
<td>2.40</td>
<td>36.20</td>
<td>7.43</td>
</tr>
<tr>
<td></td>
<td>MGD</td>
<td>0.16</td>
<td>0.27</td>
<td>0.15</td>
<td>0.13</td>
<td>0.52</td>
<td>0.40</td>
<td>0.22</td>
<td>0.30</td>
<td>0.39</td>
<td>6.07</td>
<td>0.90</td>
</tr>
<tr>
<td>Fusion</td>
<td>LMS</td>
<td>0.07</td>
<td>0.06</td>
<td>0.06</td>
<td>0.04</td>
<td>0.13</td>
<td>0.11</td>
<td>0.04</td>
<td>0.09</td>
<td>0.05</td>
<td>3.45</td>
<td>0.41</td>
</tr>
</tbody>
</table>


