Spoofing detection from a feature representation perspective

Citation for published version:

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Proceedings for the 41st IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2016)

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Spoofing detection, which discriminates the spoofed speech from the natural speech, has gained much attention recently. Low-dimensional features that are used in speaker recognition/verification are also used in spoofing detection. Unfortunately, they don’t capture sufficient information required for spoofing detection. In this work, we investigate the use of high-dimensional features for spoofing detection, that maybe more sensitive to the artifacts in the spoofed speech. Six types of high-dimensional feature are employed. For each kind of feature, four different representations are extracted, i.e. the original high-dimensional feature, corresponding low-dimensional feature, the low- and the high-frequency regions of the original high-dimensional feature. Dynamic features are also calculated to assess the effectiveness of the temporal information to detect the artifacts across frames. A neural network-based classifier is adopted to handle the high-dimensional features. Experimental results on the standard ASVspoof 2015 corpus suggest that high-dimensional features and dynamic features are useful for spoofing attack detection. A fusion of them has been shown to achieve 0.0% the equal error rates for nine of ten attack types.

Index Terms— Spoofing attack, spoofing detection, countermeasure, high-dimensional feature, phase

1. INTRODUCTION

Automatic speaker verification (ASV) system aims to verify the claimed identity based on a given speech signal. For many security systems, the robustness of ASV system against the spoofing attacks is a major concern. However, even the state-of-the-art ASV systems are not designed to sustain spoofing attacks, such as impersonation, replay, speech synthesis and voice conversion, as reviewed in [1]. Specifically, attacks realised by speech synthesis [2] and voice conversion [3], which provide easily accessible ways to generate high quality speech of the target speaker, impose a genuine threat to the ASV systems [4]. To address the threat of these two kinds of synthetic spoofing attacks, one way is to improve the robustness of ASV system by combining the detection process and verification process [5]. An alternative way is to build some standalone detection systems using different countermeasures, and this is also the focus of this paper.

Selecting an effective feature to detect spoofing attacks is important. Considering the phase information is usually neglected by many synthetic techniques, phase-based features are typically used for anti-spoofing, such as modified group delay (MGD) [6, 7, 8, 9], cosine-normalized phase [6, 9], relative phase shift (RPS) [10, 11, 12, 13], cochlear filter cepstral coefficients plus instantaneous frequency (CFCCIF) [14]. Modulation-base features have been used in [15] to detect temporal artifacts. Deep neutral networks have been also used in [16] to extract more discriminant feature. A comparison between different features for synthetic spoofing detection can be found in [17]. However, these are generally low dimensional features, as they have been processed after several stages including feature extraction and dimension reduction. This is also to facilitate the classifiers used, such as Gaussian mixture model (GMM) [18, 7, 15], which is not designed to model the features with high dimension. As the synthetic techniques typically exploit the low-dimensional features, much detailed information has been abandoned in the spoofed speech. These detailed information may be comprised in the high-dimensional features extracted directly from the Fourier transform. Hence, detailed information carried in high-dimensional or high-frequency features might be useful for spoofing detection.

In our previous work [8], seven high-dimensional features, including both magnitude- and phase-based features, are used for synthetic spoofing detection. Even though the system achieves good performance in the synthetic speech detection task, which confirms the effectiveness of the high-dimensional features, it is still not clear how to select a robust feature for spoofing detection.

In this work, we investigate spoofing detection from a feature representation perspective with the following hypotheses:

- The high-dimensional feature is more effective than the low-dimensional feature, as the high-dimensional features contain more detailed information of magnitude and phase;
- The high-frequency region is effective for synthetic spoofing detection, as this region is rarely modelled by speech synthesis or voice conversion;
- The dynamic temporal information is important for spoofing detection, even for high-dimensional features;
- Features derived from different sources are complementary and a fusion of these features can improve detection performance.

To verify these hypotheses, we conduct a series of experiments using six features and the same neural network-based classifier. For each feature, we extract high-dimensional, and corresponding low-dimensional features. We also employ the low- and high-frequency regions of the high-dimensional features to assess their effectiveness.

SPOOFING DETECTION FROM A FEATURE REPRESENTATION PERSPECTIVE

Xiaohai Tian\(^1,2\), Zhizheng Wu\(^3\), Xiong Xiao\(^4\), Eng Siong Chng\(^1,2,4\) and Haizhou Li\(^1,5\)

\(^1\)School of Computer Engineering, Nanyang Technological University (NTU), Singapore
\(^2\)Joint NTU-UBC Research Center of Excellence in Active Living for the Elderly, NTU, Singapore
\(^3\)The Center for Speech Technology Research, University of Edinburgh, United Kingdom
\(^4\)Temasek Laboratories, NTU, Singapore
\(^5\)Human Language Technology Department, Institute for InfoComm Research, Singapore

\{xhtian, xiaoxiong, asesching\}@ntu.edu.sg, zhizheng.wu@ed.ac.uk, hli@i2r.a-star.edu.sg

ABSTRACT

Spoofing detection, which discriminates the spoofed speech from the natural speech, has gained much attention recently. Low-dimensional features that are used in speaker recognition/verification are also used in spoofing detection. Unfortunately, they don’t capture sufficient information required for spoofing detection. In this work, we investigate the use of high-dimensional features for spoofing detection, that maybe more sensitive to the artifacts in the spoofed speech. Six types of high-dimensional feature are employed. For each kind of feature, four different representations are extracted, i.e. the original high-dimensional feature, corresponding low-dimensional feature, the low- and the high-frequency regions of the original high-dimensional feature. Dynamic features are also calculated to assess the effectiveness of the temporal information to detect the artifacts across frames. A neural network-based classifier is adopted to handle the high-dimensional features. Experimental results on the standard ASVspoof 2015 corpus suggest that high-dimensional features and dynamic features are useful for spoofing attack detection. A fusion of them has been shown to achieve 0.0% the equal error rates for nine of ten attack types.
2. FEATURE REPRESENTATIONS FOR SPOOFING DETECTION

2.1. Feature extraction

Six types of feature are used in this study. We choose these six types because they show good performance [8]. They include two magnitude-based features, namely log magnitude spectrum (LMS) and residual log magnitude spectrum (RLMS); and four phase-based features, namely instantaneous frequency derivative (IF), baseband phase difference (BPD), group delay (GD) and modified group delay (MGD). All the features are evaluated using short-time Fourier transform (STFT) on the speech signal. The speech is sampled at 16KHz and the STFT analysis window is 25ms with 15ms overlap. The Hamming window and direct current (DC) offset are applied on each analysis frame. The magnitude and phase spectrum, extracted directly from the Fourier transform, are further used to generate different magnitude- and phase-based features, respectively. The FFT is directly from the Fourier transform without dimension reduction, as described in Section 2.1. The dimension of HD feature is 256.

The features are summarized as follows:

- **LMS**: The log magnitude spectrum feature, which contains the formant information, harmonic structure and all the spectral detail of speech signal. To reduce the dynamic range of the magnitude spectrum, the logarithmic is used. In case of LMS both large and small magnitude frequency components are visible.
- **RLMS**: To reduce the impact of formant information and better analyse the harmonic structure and spectral details, the residual log magnitude spectrum feature is used in this work. The inverse linear predictive coding (LPC) filter is employed to estimate the glottal waveform from the speech signal; then the LMS is extracted from the residual waveform.
- **IF**: Instantaneous frequency [19] is the derivative of the phase along time. Therefore, it captures the temporal information of phase. Unlike the original phase spectrum that hardly shows any patterns, there are clear patterns in the IF spectrum, making it possible to be used as a feature.
- **BPD**: Baseband phase difference [20] is a phase feature extracted from baseband STFT, which can also provide a clear pattern to present phase information.
- **GD**: Group delay [21] is a representation of filter phase response, which is defined as the negative derivative of the Fourier transform phase. It is a frame-based feature, used to capture the phase distortion along frequency axis.
- **MGD**: A variation of GD. The modified group delay [21] can obtain a more clear phase pattern than GD. Two factors, and are used for control the dynamic range of the modified group delay, here the same setting as suggested in [8].

2.2. Feature representation

In order to investigate the effectiveness of the high-dimensional features and relative contribution of the low- and the high-frequency region for synthetic spoofing detection, different feature representations are used in this study, summarized as follows:

- **HD**: The original high-dimensional features which extracted directly from the Fourier transform without dimension reduction, as described in Section 2.1. The dimension of HD feature is 256.
- **LD**: The low-dimensional representation of the HD feature. The Mel-frequency scaled filter banks are computed over the corresponding features to generate 23 filter bank coefficients.
- **HD-LF**: The low-frequency range of the HD feature, consisting of the first half of 128 frequency bins.
- **HD-HF**: The high-frequency range of the HD feature, consisting of the second half of 128 frequency bins.

The effectiveness of temporal information for synthetic spoofing detection has been shown in many works [22, 17]. In [8], we use 51 frames and achieved good performance. Such a high-dimensional feature, however, will increase the difficulty of classifier training. Hence, the dynamic features, including delta and acceleration coefficients, of all the representations noted above are extracted in this study to capture the temporal information, namely HD-D, LD-D, HD-LF-D, HD-HF-D.

2.3. Fusion

Considering the complementarity between different features, a score level fusion is applied. Previous studies [8, 17] shown that single type of feature is usually effective for certain types of artifact, while may not be sensitive to other types of artifact. For example, the main propose the LMS and RLMS features are to capture the artifacts of magnitude, while the IF, BPD, GD and MGD are expected to detect the distortion of phase. Hence, the system fusion is employed to leverage and synergy the merits of different features. To avoid over-fitting to development data, the scores of all systems are simply averaged to produce the final score.

3. EXPERIMENTS

3.1. Experimental setup

The ASVspoof 2015 database [23] is used to assess the performance of different features for synthetic spoofing detection. This database consists of three subsets, including training set, development set and evaluation set. There are totally 10 types of spoofing attack, namely S1 to S10. The training and development sets only contain the spoofing attacks generated by the first five methods (S1-S5); while the evaluation set consists of the spoofing attacks generated by both five known methods (S1-S5) and five unknown methods (S6-S10). Noted that, vocoders and low-dimensional features are used in all the first nine methods (S1-S9)\(^1\); while waveform-based unit selection is used to generate S10. More details about the database can be found in [23].

Since we focus on feature representations, all the spoofing detectors employed the same neural network (NN) based classifier, as it is capable to model high-dimensional features. The NN consists of one hidden layer with 2,048 sigmoid nodes and 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.

The equal error rate (EER) is used to evaluate the system performance. The EER is obtained by selecting an operating point which gives the equal miss rate and false alarm rate. In practice, the EERs of each feature for different spoofing attacks are computed using the Bosaris toolkit\(^2\). For feature-based systems, we only report the results on the evaluation set; while, for each speech synthesis/voice conversion methods of the development set (S1-S5) and the evaluation set (S1-S10), the averaged EERs of the fused systems are reported.

\(^1\)Our system achieved the best performance on S1-S9 in the ASVspoof 2015 challenge.

\(^2\)https://sites.google.com/site/bosaristoolkit/
3.2. Results

From our preliminary results, we observe that the results on the development set are similar to that of the S1 to S5 on the evaluation set. Hence, we only report the results on the evaluation set, and the feature-based results are presented in Table 1. Here, we separate the results into three parts, the results of known attacks (S1-S5), the results of unknown attacks using vocoders and low-dimensional features (S6-S9) and the results for unknown attacks generated by waveform (S10).

We first examine the effectiveness of the high-dimensional features. As expected, the high-dimensional (HD) features always outperform its corresponding low-dimensional (LD) representation. Similar phenomena were observed when dynamic features are included, in particular the HD-D achieves lower error rates than the LD-D. This is due to the low-dimensional feature is not capable in capturing as much detailed information as the high dimensional feature. It also implies that the detailed magnitude and phase information of speech signal contain more artificial cues for synthetic spoofing detection.

We then compare the performance of the low- and the high-frequency regions of the high-dimensional features. The results show that the HD-HF feature always outperforms the corresponding HD-LF feature. This suggests that the high-frequency region of synthetic voice contains more artifacts than the low-frequency counterpart. Low dimensional features, such as Mel-frequency scaled filter banks, have high resolution at low frequency and low resolution at high frequency. They take human perception sensitivity with respect to frequencies into consideration, and therefore are best for speech/speaker recognition. However, they are not designed to be sensitive to the artifacts in synthetic speech signals. Some interesting observations are found by using dynamic features: 1) For magnitude-based features, LMS and RLMS, the high-frequency part (HD-HF-D) outperforms its low-frequency counterpart (HD-LF-D). Especially, for the LMS feature, the HD-HF-D feature (EER of 0.03%) obtain a very close detection accuracy to the HD-D feature (EER of 0.0%). Second, all the fused systems fail to detect S10 generating by unit selection algorithm, sporadic spoofing attacks in evaluation set (S1-S9) are detected with EERs of 0.0%. Second, all the fused systems fail to detect S10 generating by unit selection algorithm, which outperform the HD-D representation achieves good performance on this set (EER of 0.02%). This implies the effectiveness of phase information. The LMS feature with the HD-D representation performs best with an EER of 0.01%.

For the unknown attacks (S10), the performance degrades dramatically. This is due to the fact that all the features used in our systems aim for detecting the artifacts of either magnitude or phase. However, S10 attacks are generated by unit selection algorithm, which use original waveforms directly. Hence, the artifacts only appear in the transition positions, which increase the difficulty for detection.

3.3. Fusion results

The results of fused systems on both development and evaluation sets are presented in Table 2. From the results, we have following observations. First, comparing to the systems using single feature, the EERs of the fused system are reduced significantly on both development and evaluation sets. Particularly, for the fused system of HD-D, all the spoofing attacks in development set and most of spoofing attacks in evaluation set (S1-S9) are detected with EERs of 0.0%. Second, all the fused systems fail to detect S10 generating by waveform concatenation. We know that in unit selection most of the speech samples are actually natural speech. The artifacts only exist between the units. Third, again, the results confirm the effectiveness of high-dimensional features, high-frequency information and dynamic features for spoofing attacks detection. Finally, we confirm that all the results are consistent with [8]. Specifically, for the development set and (S1-S9) of evaluation set, our system outperforms the previous system. The best results is achieved by the fusion system of HD-D with the EER of 2.78%

4. DISCUSSIONS

4.1. Magnitude vs phase features

From the perspective of voice conversion and speech synthesis, artifacts are introduced in both magnitude and phase domains. For mag-
In general, low-dimensional features, used in most speech synthesis and voice conversion approaches, model the low-frequency of speech information more accurately than its high-frequency counterpart. Additionally, due to the smoothing effect of modelling, the spectral details can be further lost. Hence, with magnitude-based representations, it is possible to detect such discontinuities in the waveform concatenating points. We will investigate techniques to detect such discontinuities for spoofing detection in the future work.

4.3. High-frequency vs low-frequency features

In general, low-dimensional features, used in most speech synthesis and voice conversion approaches, model the low-frequency of speech information more accurately than its high-frequency counterpart. Additionally, due to the smoothing effect of modelling, the spectral details can be further lost. Hence, with magnitude-based representations, artifacts are easier to find in the high-frequency region. Our results, in Section 3, confirm the effectiveness of the high-frequency features. Similar conclusion can also be found in [17].

The situation is a bit different in phase-based features. As not modelled in speech synthesis or in voice conversion, the phase features do not contain the smoothing effects of modelling and the issues concerning low-dimensional features. However, the phase generated by vocoder is still different from that of natural speech. Different to the results of magnitude-based features, with the phase-based features implemented with dynamic features, the low-frequency (HD-LF) outperforms the high-frequency (HD-HF). But, the performance of high-dimensional features (HD) is much better than either the low-frequency or the high-frequency. This suggests that both the low- and the high-frequency of phase-based features contribute to the synthetic spoofing detection.

4.4. Difficulty in detecting unit selection-based attacks

Similar to all the other systems submitted to the ASVspoof 2015 challenge [23], our system doesn’t perform as expected in S10, which is an unit-selection based attack. The unit-selection based attack is produced by concatenating the time-domain waveform directly without any vocoding and feature extraction techniques, which doesn’t carry much artifacts from the perspective of feature representations.

According to the human perception study [27], human listeners can easily detect the unit-selection attack, as human ear can detect the artifacts of the discontinuity at the waveform concatenating points. We will investigate techniques to detect such discontinuities for spoofing detecting in the future work.

5. CONCLUSIONS

In this paper, we investigate the high-dimensional features and the high-frequency information to discriminate synthetic spoofing attacks and natural speech. The experiments results show that,

• the high-dimensional features outperform its low-dimensional representations;
• the high-frequency and the low-frequency information are complementary in discriminating synthetic spoofing attacks and natural speech;
• the dynamic features are useful for synthetic spoofing attacks detection;
• fusion of different systems improve the detection performance.

Additionally, by applying the score level system fusion, all the spoofing attacks using vocoders and low-dimensional features are successfully detected. While poor performance is observed for unit selection-based spoofing attacks. Therefore, in future, we will investigate more robust feature to detect such kind of spoofing attacks.

Acknowledgment This research is supported by the National Research Foundation, Prime Ministers Office, Singapore under its IDM Futures Funding Initiative and administered by the Interactive and Digital Media Programme Office. This work is also supported by the DSO funded project MAISON DSOCL14045, Singapore.
6. REFERENCES


