Towards End-to-End Synthetic Speech Detection

Guang Hua, Member, IEEE, Andrew Beng Jin Teoh, Senior Member, IEEE, and Haijian Zhang, Member, IEEE

Abstract—The constant Q transform (CQT) has been shown to be one of the most effective speech signal pre-transforms to facilitate synthetic speech detection, followed by either hand-crafted (subband) constant Q cepstral coefficient (CQCC) feature extraction and a back-end binary classifier, or a deep neural network (DNN) directly for further feature extraction and classification. Despite the rich literature on such a pipeline, we show in this paper that the pre-transform and hand-crafted features could simply be replaced by end-to-end DNNs. Specifically, we experimentally verify that by only using standard components, a lightweight neural network could outperform the state-of-the-art methods for the ASVspoof2019 challenge. The proposed model is termed Time-domain Synthetic Speech Detection Net (TSSDNet), having ResNet- or Inception-style structures. We further demonstrate that the proposed models also have attractive generalization capability. Trained on ASVspoof2019, they could achieve promising detection performance when tested on disjoint ASVspoof2015, significantly better than the existing cross-dataset results. This paper reveals the great potential of end-to-end DNNs for synthetic speech detection, without hand-crafted features.

Index Terms—Synthetic speech detection, speech forensics, ASVspoof2019, ASVspoof2015, cross-dataset testing, end-to-end.

I. INTRODUCTION

The success of deep learning technology has shifted the paradigm of speech synthesis from the classic hidden Markov model based framework [1] to neural speech synthesis. Equipped with powerful deep neural network (DNN) architectures e.g., [2], and fueled by massive training data, today’s text-to-speech (TTS) systems could synthesize high quality speech that is hard to be distinguished from human voices. Despite the multitude of benefits, these advances have also improved the quality of voice spoofing attacks, including voice conversion [3], impersonation [4], cloning [5], etc., posing new challenges to synthetic speech detection.

For nearly a decade, the combination of a front-end feature extractor and a back-end binary classifier is the de facto framework for synthetic speech detection. Within this framework, an overwhelming majority of the existing works have focused on the development of hand-crafted front-end features, including fundamental frequency, power spectrum, octave spectrum, linear frequency cepstral coefficient (LFCC), mel-frequency cepstral coefficient (MFCC), cepstral mean and variance (CMVN), cochlear filter cepstral coefficient (CFCC), filter bank based cepstral coefficient, linear prediction cepstral coefficient (LPCC), modified group delay (MGD), relative phase shift (RPS), constant Q cepstral coefficient (CQCC), and many of their variations and combinations [6]–[15]. Usually, one or a few of these features are used to train a Gaussian mixture model (GMM) or a support vector machine (SVM) for classification. Taking the advantage of DNNs in classification tasks, multilayer perceptron (MLP) and convolutional neural network (CNN) based classifiers have been used to replace the conventional back-end classifiers [15]–[22]. On the other side, DNN structures have also been used at the front-end to facilitate feature extraction [22]–[25], followed by conventional classifiers. DNNs can also work across the front- and back-end, with pre-transformed features as input [26]–[30].

Among hand-crafted features, CQCC has been found to be the best choice, which is also the baseline feature in the ASVspoof2019 challenge [31]. Recently, Yang et al. developed a set of subband CQCC features for better detection performance [19]. Subsequently, Das et al. [21] further fused 8 hand-crafted features, followed by an MLP classifier. For deep learning based approach, Lavrentyeva et al. [29] proposed the use of FFT, LFCC, and CMVN, followed by a CNN for classification, while using CQT as model input, Li et al. [30] incorporated the so called Res2Net structure and squeeze-and-excitation (SE) block. With score level fusion, Lavrentyeva et al. [29] and Li et al. [30] have achieved the state-of-the-art performance on ASVspoof2019 dataset.

Based on the above overview, the existing mainstream workflow for synthetic speech detection is summarized in the brown blocks of Fig. 1. It can be seen that a time-frequency transform (e.g., CQT) of the speech waveform before hand-crafted feature extraction (e.g., CQCC), or before feeding the data into a DNN, has become an implicit standard routine in the existing works. However, since DNNs are best known for their excellent capability of feature extraction, there naturally arises a question of whether it is necessary to apply these pre-transforms. In fact, these transforms usually discard some information about the observed speech signal. For example, the CQT feature, more precisely the log power spectrum of the CQT [30], does not have the phase information of the signal.
To further generate the CQCC, even more information will be discarded [19]. From hand-crafted feature engineering point of view, a good feature captures discriminative information between classes and is also compact in size, but the same principle may not apply to the DNN regime.

In this paper, we show that the pre-transforms, as well as the hand-crafted features, are in fact not a must for DNN based synthetic speech detection. Despite the rich hand-crafted features, we experimentally verify that via the use of standard DNN structures, an end-to-end light-weight neural network with mere speech waveform could achieve even better results. Our proposal is motivated by recent works analyzing raw-waveform based DNNs [32] and the attempt of applying end-to-end DNNs to related speech processing tasks, e.g., speech separation [33]. The proposed model is thus termed as Time-domain Synthetic Speech Detection Net (TSSDNet). We note that the first work on end-to-end synthetic speech detection was probably carried out by Muckenhirn et al. [34], in which a basic feedforward sequential CNN was used. It was tested on older datasets, not achieving the state-of-the-art results. In our design of the TSSDNet, two types of advanced CNN structures are considered, including ResNet-style skip connection with $1 \times 1$ kernels [35] and Inception-style parallel convolutions [36], respectively. We demonstrate that via proper training, the proposed networks outperform the state-of-the-art hand-crafted feature based detectors as well as DNN based ones on the challenging ASVspoof2019 dataset [31]. To analyze practical merits of the proposed methods, we further perform a cross-dataset evaluation between ASVspoof2019 and ASVspoof2015 [37], demonstrating their promising generalization capability.

II. THE PROPOSED MODELS

In many deep learning tasks such as object recognition or semantic understanding, it has been found that generally the deeper the network, the better the performance [35], [36], [38]. However, in synthetic speech detection, the critical feature is the artifact left behind data forgery, which may not contain any semantic information. Since deeper features are more towards higher level semantic information, which may not be suitable to represent the subtle forgery artifacts, we hypothesize that the network for synthetic speech detection should be relatively shallower. Grabbing the essence of the popular ResNet [35] and Inception network [36], the proposed end-to-end TSSD-Nets are designed as follows.

A. Model Structure

The proposed Res-TSSDNet and Inc-TSSDNet are depicted in Fig. 2 (a) and (b), respectively, which share the same first layer, 3 final fully-connected linear layers, and global max pooling before the linear layers. The ResNet-style and Inception-style blocks are repeated for $M$ times, respectively, and batch normalization (BN) is applied in both networks. $C_R$ and $C_I$ denote the number of channels in the corresponding modules, which may vary across layers. Noticeably, to increase the receptive field and control model complexity, dilated convolutions [39] with dilation $d$ are incorporated in the Inc-TSSDNet, which is different from the original Inception network [36]. All the convolution layers apply “SAME” padding with stride = 1, while for the pooling layers the stride equals to the corresponding kernel size.

B. Training Strategy

1) Data Preparation: Normally, the training data contain raw speech recordings with varied durations. To align the training data, we adopt the treatment in [30]. In [30], the training examples are truncated or repeated until the duration is 6.4 seconds to generate the CQCC feature, while here we keep every example with 6 seconds, with the default 16 kHz sample rate. These 6-second examples are then directly fed into the networks for end-to-end training. Since all convolution layers have “SAME” padding, the length of feature vector ($9.6 \times 10^4$ at input) is reduced solely by the pooling layers.
Note that hand-crafted feature based method, e.g., CQCC [19], is insensitive to the length of recording since all time slices contribute to classifier training. Batch size is set to 32.

2) Weighted Cross-Entropy Loss: Considering the fact that in general data-driven media content forgery detection tasks, the number of genuine examples is usually much less than the number of fake ones, we apply weighted cross-entropy (WCE) loss during the training phase to cope with data imbalance. Let \( \{ x_i, y_i \} \) compose the labeled training set, where \( \forall i, y_i \in \{0, 1\} \), then the WCE loss is given by

\[
WCE(z, y_i) = -w_{y_i} \log(z_{y_i}),
\]

where \( z = [z_0, z_1] \) contains the softmax probabilities of the 2 classes, and \( w_{y_i} \) is the inverse ratio of label \( y_i \) in the training set. For all the training processes, we use the Adam [40] optimizer and default settings. Exponential learning rate decay with a multiplicative factor of 0.95 is adopted. The model yielding the lowest equal error rate (EER) on development set within 100 epochs is selected for evaluation.

3) Mixup Regularization: For practical forensic merits, the trained model is expected to generalize to unseen attacks, and the ASVspoof datasets have been specially designed for this purpose. In this paper, we consider the mixup regularization [41] as a booster to further improve the generalization capability. Specifically, it uses a set of mixed examples and labels, instead of the original set, to train the network, i.e.,

\[
\tilde{x}_i = \lambda x_j + (1 - \lambda)x_j, \quad \tilde{y}_i = \lambda y_j + (1 - \lambda)y_j,
\]

where \( \{ x_i, y_i \} \) and \( \{ x_j, y_j \} \) are two randomly selected training pairs, \( \lambda \sim \text{Beta}(\alpha, \alpha) \), and \( \alpha \in (0, \infty) \) is a hyperparameter. The implementation of the mixup regularization could be carried out via the following equivalent loss function,

\[
CE_{\text{mixup}}(\tilde{z}, \tilde{y}_i, y_j) = \lambda CE(\tilde{z}, y_i) + (1 - \lambda)CE(\tilde{z}, y_j),
\]

where \( \tilde{z} \) contains the softmax probabilities from mixed examples, and \( CE(\cdot, \cdot) \) is the standard cross-entropy (CE) loss, equivalent to setting \( w_0 = w_1 = 1 \) in (1).

III. RESULTS

We first present the main results obtained by the proposed networks in comparison with the benchmark and the state-of-the-art solutions on the latest ASVspoof2019 dataset. We then perform ablation study, followed by cross-dataset evaluation on the ASVspoof2015 dataset. All the results are generated using a single GeForce GTX 1080 or 1080Ti GPU. PyTorch implementations of the proposed TSSDNetworks are available at: https://github.com/ghuahui/end-to-end-synthetic-speech-detection.

A. Main Results

The comparison of the results in terms of EER obtained on the logical access (LA) development and evaluation sets of the ASVspoof2019 challenge is presented in Table I, where the 2D-Res-TSSDNet is the 2D version of the Res-TSSDNet, having the same architecture except that all the convolution and pooling \( (2 \times 2) \) layers use 2D kernels instead.

We make the following remarks from the main results. i) The works of [19] and [21] represent the best results of sophisticated hand-crafted feature engineering plus an MLP as the back-end classifier. ii) The majority of recent works belong to the type of pre-transform (or light feature engineering) plus DNNs to further perform feature extraction and classification. iii) All the works incorporating DNNs rely on the feature and model fusion for performance improvement, and in [29] and [30], the fused results have achieved EERs below 2%. iv) The 2D-Res-TSSDNet result is obtained with experimental settings identical to [30] without fusion, and it can be seen that when working with 2D pre-transform input, the use of advanced DNN components, i.e., Res2Net and SE, becomes very necessary. v) Most importantly, the proposed Res-TSSDNet is a single end-to-end network (no fusion, no feature engineering), containing less than a half of trainable weights than the one in [30] and only about one-tenth than in [29], but it achieves the overall lowest evaluation EER by a clear margin. vi) Lastly, the Inc-TSSDNet is extremely light, having only 0.09M parameters, but it could still achieve an EER lower than those from [27]–[29] heavy models.

B. Ablation Study

We first perform ablation study by varying the depth or width of the networks, and the results are summarized in Table II. For the Res-TSSDNet, the column “1 × 1” indicates whether the “skip connection” in Fig. 2 (a) is used. It can be seen that going either shallower or deeper will result in the raise...
of EER, while with the use of ResNet skip connection, the network could achieve 1.05% EER reduction over the one without using it. Similarly for the Inc-TSSDNet, the sweet spot also lies in the moderate depth or width.

We further perform intra-model sensitivity analysis using the two proposed end-to-end models in Table I. Fixing all hyperparameters, the two models are trained from scratch using ASVspoof2019 training set for over 30 times, and the dev and eval EERs are summarized in Fig. 3. It can be seen that the EERs of both models are bounded within certain ranges (except one outlier eval EER > 4% for the Res-TSSDNet). The Inc-TSSDNet yields tighter dev EERs over the Res-TSSDNet, but eval EERs of the former are clearly higher. We can see from Fig. 3 and Table II that the intra-model differences may be as significant as the differences from model configurations. Relatively lighter models are hence recommended for their better trade-offs between accuracy and efficiency.

In addition, we have also discovered that i) changing all the activations from ReLU to leaky or parametric ReLU does not lead to a clear performance difference; ii) The first layer with a $1 \times 7$ convolution kernel, adopted from ResNet setting, is slightly better than using a $1 \times 3$ kernel; iii) Global max pooling is found to be more effective than global average pooling before the linear layers for both networks, but for the 2D-Res-TSSDNet, we stick to global average pooling; iv) The EERs of using standard CE are slightly higher than those using the WCE; v) Duration of training example also matters. Experimental results using 5-second truncation yielded a slight performance degradation, but when 2-second truncation is applied, the EER on evaluation set increased drastically.

C. Cross-Dataset Testing

We now perform the cross-dataset experiments. Since the ASVspoof2015 training set contains relatively old speech synthesis methods, we focus on using networks trained on the training set of more advanced ASVspoof2019 to test on the dev and eval sets of ASVspoof2015. The intra- and inter-dataset EERs are presented in Table III. It can be seen that the GMMs learned from LFCC and CQCC features in ASVspoof2019 are generally inconsistent with the data in ASVspoof2015. For the best Res-TSSDNet on ASVspoof2019, it could not generalize to ASVspoof2015 either, whose EERs indicate almost indistinguishable softmax probability distributions for real and fake classes. However, by incorporating mixup regularization and increasing the level of mixup level $\alpha$, we observe that the Res-TSSDNet can significantly reduce the cross-dataset EERs to less than 2%, while slightly sacrificing the performance on the original dataset. Further, all the Inc-TSSDNet variants have very attractive generalization capability even for the lightest model. The $M = 5$, 8-branch version yields the best cross-dataset performance with 1.96% eval EER. This is a significant score compared to the existing cross-dataset results as reported in [43]–[45]. Noticeably in [45], also trained on ASVspoof2019 training set and tested on ASVspoof2015, the use of the CQT based features could only achieve EERs greater than 20% (see Table 2 in [45]). For completeness, the detection error trade-off (DET) curves on ASVspoof2015 evaluation set using a few methods in Table III are provided in Fig. 4.

IV. Conclusion

We have shown that a light-weight end-to-end neural network, significantly different from the existing front- and back-end pipeline, could achieve to date the best synthetic speech detection results. It reduces the ASVspoof2019 eval EER by a clear margin compared to much heavier networks fed by pre-transform inputs, sophisticated hand-crafted features plus MLP classifiers, or the fusion of many systems of such kinds. We have further shown via cross-dataset testing that the proposed networks could also generalize to unseen dataset. In the ongoing ASVspoof2021 challenge, a new speech deepfake (DF) detection task is introduced specially for synthetic deepfake speech detection, and end-to-end methods are being given more attention, e.g., the RawNet2 [46] is used as a baseline.

**Table III**

| Method | ASVspoof2019 Eval | ASVspoof2015 Dev | ASVspoof2015 Eval |
|--------|------------------|-----------------|------------------|
| Baseline LFCC+GMM [42] | 9.57 | 19.82 | 15.91 |
| Baseline CQCC+GMM [42] | 8.09 | 47.72 | 39.90 |
| Mixup, $\alpha = 0.1$, Res-TSSDNet | 1.64 | 39.12 | 42.52 |
| Mixup, $\alpha = 0.5$, Res-TSSDNet | 2.07 | 5.48 | 5.46 |
| Mixup, $\alpha = 1.0$, Res-TSSDNet | 2.29 | 3.50 | 5.75 |
| $M = 3$, 4-branch, Inc-TSSDNet | 10.39 | 5.31 | 5.24 |
| $M = 4$, 4-branch, Inc-TSSDNet | 4.04 | 2.78 | 3.29 |
| $M = 4$, 8-branch, Inc-TSSDNet | 3.75 | 1.84 | 2.16 |
| $M = 5$, 8-branch, Inc-TSSDNet | 4.20 | 1.31 | 1.96 |

**Fig. 3.** Intra-model performance on ASVspoof2019.

**Fig. 4.** DET curves of cross-dataset testing on ASVspoof2015 eval set.
