CONVNEXT BASED NEURAL NETWORK FOR AUDIO ANTI-SPOOFING

Qiaowei Ma, Jinghui Zhong, Yitao Yang, Weiheng Liu, Ying Gao and Wing W.Y. Ng

South China University of Technology
jinghuizhong@scut.edu.cn

ABSTRACT

With the rapid development of speech conversion and speech synthesis algorithms, automatic speaker verification (ASV) systems are vulnerable to spoofing attacks. In recent years, researchers had proposed a number of anti-spoofing methods based on hand-crafted features. However, using hand-crafted features rather than raw waveform will lose implicit information for anti-spoofing. Inspired by the promising performance of ConvNeXt in image classification tasks, we revise the ConvNeXt network architecture and propose a lightweight end-to-end anti-spoofing model. By integrating with the channel attention block and using the focal loss function, the proposed model can focus on the most informative sub-bands of speech representations and the difficult samples that are hard to classify. Experiments show that our proposed system could achieve an equal error rate of 0.64% and min-tDCF of 0.0187 for the ASVSpoof 2019 LA evaluation dataset, which outperforms the state-of-the-art systems.

Index Terms— automatic speaker verification, anti-spoofing, end-to-end.

1. INTRODUCTION

Automatic speaker verification (ASV) systems use the speaker’s voiceprint information to identify specific person, and have been widely used in many real life applications. However, with the rapid development of the text to speech (TTS) [1] and voice conversion (VC) [2] algorithms, the ASV systems are vulnerable to the spoof attacks.

In order to promote the research on spoof attack detection, the bi-annual anti-spoofing challenge was first held in 2015 [3]. Since then, many spoof attack detection methods had been proposed. And these works mostly focus on feature engineering and network architecture designing. For the feature engineering, hand-crafted features such as phase information [4], octave spectra information [5], Constant Q Cepstral Coefficients (CQCC) [6], CQT-based modified group delay feature [7] and genuinized feature that transformed from the given log power spectrum (LPS) [8] were proposed to enhance the effectiveness of the anti-spoofing system. For the network architecture design, the residual network and its variant [7, 9] were used to detect the spoof attacks, Wu et al. [8] use a light convolutional neural network (LCNN) against spoofing attacks. Recently Li et al. [10] use a Res2Net architecture for replay and synthetic speech detection. Res2Net is a multiple-feature scale network architecture. It split the features maps within one block into multiple channel groups and designs a residual-like connection across different channel groups, which could increase the possible receptive fields and enhance the anti-spoofing capacity of the model. Although the above residual network architecture or its variant achieves competitive performance for spoof attack detection, these single systems still lack generalizability to unseen spoofing attacks. Ensemble systems that use different hand-crafted features would improve the anti-spoofing performance, but it will increase the model’s complexity.

Extracting hand-crafted features would lose some useful information for detecting spoof attacks, for example, the log power spectrum of the CQT feature, does not have the phase information of the signal. Therefore, some researchers proposed the anti-spoofing model that directly uses the raw waveform as the network’s input to capture the spoof cues of the spoof audio [11, 12, 13]. The results of these end-to-end systems are better than many anti-spoofing systems that use hand-crafted features.

Recently, Liu et al. modernized a standard ConvNet (ResNet [14]) towards the design of a hierarchical vision transformer and proposed a pure ConvNet model called ConvNeXt. [15]. ConvNeXt had achieved great success in some vision tasks. Its classification performance demonstrated ConvNeXt’s powerful feature extraction capability. Inspired by the success of the residual network and its variant used for spoof attack detection and the promising performance of the end-to-end spoof attack detection, we design an end-to-end anti-spoofing neural network by revising ConvNeXt’s network architecture. The major contributions of this paper are as follows:

- We proposed a new fully end-to-end anti-spoofing neural network (named CNBNN) by revising ConvNeXt’s network architecture, which achieved outstanding performance and outperform state-of-the-art systems.
- We revise the efficient channel attention (ECA) module from [16] and integrate it into the proposed model.
Such a channel attention module could make the model focus on the most informative sub-bands of speech representations to improve the detection performance of the system.

- The proposed best single system could achieved an equal error rate (EER) of 0.64% and min-tDCF of 0.0187 on the evaluation dataset of ASVSpoof 2019 LA dataset, which demonstrate the model’s capacity for anti-spoofing.

The rest of this paper is organized as follows: Section 2 illustrates the proposed methods. Experiment setup, results and analysis are discussed in Section 3 and 4, respectively. We conclude this work in Section 5.

2. PROPOSED METHODS

This section will first present a general framework of our proposed system and then introduce the model’s res2net style block and Modified ECA layer in detail. Finally, we will introduce the focal loss used in our model.

2.1. ConvNeXt based neural network architecture

As illustrated in figure 1(a), we adapt the ConvNeXt network architecture from [15]. We revise the network to make it suitable for the input raw waveform, thus we can train the neural network end-to-end. Compared with the original network architecture, we remove the Stochastic Depth [17], which we find does not improve the performance of the anti-spoofing system. For the normalization method, we replace layer normalization with batch normalization and achieve better performance for anti-spoofing. We assume that the network should be relatively shallower because a deeper network extract deeper features which towards higher level semantic information, but it may not suitable to represent the subtle forgery artifacts from the spoof attacks. So we change the different compute stage ratios 3:3:9:3 to 1:2:3:1 to make the network shallower. We use a max pooling layer with a large kernel size of 9 to downsample the feature map instead of just using the convolution layer except the stem layer. And we set the channel of each compute stage to be (16,32,64,128). For the activation function, we replace GELU with SELU, which achieved better performance for anti-spoofing. We revise the ResNet style Block in the network according to the Res2Net block and then design a res2net style block, thus such design could make the model have a multi-scale receptive field and then achieve better performance for detecting the spoof artifact. And we integrate a channel attention module that modified from the ECA layer with it to enhance the model’s robustness and generalization capacity.

2.2. Res2Net style block

As illustrated in figure 1(b), the Res2Net style block use a reverted bottleneck. It means that the hidden dimension of the MLP block is four times wider than the input dimension. To be specific, the input feature maps were first through a res2net style convolutional layer, it splits the input feature maps by the channel dimension into 4 subsets, denoted by $X_i$, where $i \in \{1,2,3,4\}$. Except for $X_1$, each $X_i$ is processed by a $1 \times 3$ convolutional filter $K_i$. Starting from $i = 2$, $X_i$ is added with the output of $K_{i-1}$ before being fed into $K_i$. This process can be formulated as Eq. 1:

$$Y_i = \begin{cases} X_i, & i = 1 \\ K_i(X_i + Y_{i-1}), & 2 \leq i \leq 4 \end{cases}$$

In the last of the res2net style block, two linear layers is used to enlarge and fuse information between each channel. The block that integrated with the channel attention module (MECA) is illustrated in figure 1(c).

2.3. Modified ECA layer

To further enhance the robustness and generalizability of the model, we use a channel attention module that revises from the original ECA layer to make it suitable for the input raw waveform. ECA layer is a channel attention module that revises from the SE Block [18], it is assumed that dimensionality reduction that used in SE block is unnecessary to capture the dependencies between each channel. So in ECA layer, it avoids dimensionality reduction and captures cross-channel interaction in an efficient way.

Fig. 2. Diagram of the modified efficient channel attention (MECA) module. Given the aggregated features obtained by global average pooling (GAP), Modified ECA generates channel weights by performing a fast 1D convolution of size $k$, where $k$ is adaptively determined via a mapping of channel dimension $C$.

As illustrated in figure 2 given a feature map $x \in \mathbb{R}^{C \times N}$, where $C$ represents the numbers of the channel and $N$ represents the numbers of the sampling points of the input raw
Fig. 1. ConvNeXt based neural network. (a) an overall architecture of the proposed model. (b) the detail of the Res2net style Block. (c) Res2net style Block integrated with a channel attention module (Modified ECA layer)

waveform. A channel-wise global average pooling (GAP) without dimensionality reduction is used to gain the representation of each channel \( y \), and then a fast 1D convolution of size \( k \) is used to capture local cross-channel interaction. This process can be represented by Eq. 2:

\[
y = \sigma(\text{Conv1d}_k(x)) \tag{2}
\]

where \( k \) represents how many neighbors participate in attention prediction of one channel. And in this work, we use the method that used in [16] to adaptively select the kernel size, which is proportional to channel dimension. The way to compute \( k \) is represented by Eq. 3:

\[
k = \psi(C) = \left\lfloor \log_2(C) \right\rfloor + b \gamma_{\text{odd}}, \tag{3}
\]

where \( \lfloor t \rfloor_{\text{odd}} \) indicates the nearest odd number of \( t \). \( \gamma \) and \( b \) are the function parameters and are set to 2 and 1 respectively.

When we compute the weight of each channel \( y \), we use \( y \) to reweight the original feature map. Such a channel attention module could make the model learn to emphasize important features and suppress useless features. Thus the model could focus on the most informative sub-bands of speech representations and have a better performance for spoof attack detection.

2.4. Focal loss

Since there exist different kinds of spoof attacks in the training set and different kinds of attacks have different degrees of difficulty for the model to classify. Also, there exists an
imbalanced class distribution on the ASVSpoof 2019 dataset, the number of the bonafide speech is much less than the spoof speech. So in this case, We use focal loss [19] to make the model focus more on the hard-to-classify samples in spoof attacks and also deal with the data imbalanced during the training phase. During training, the samples that are hard to classify would be given more loss, and the samples that are easy to classify would be given less loss. The focal loss could be formulated by Eq. [4]

\[ y = -\alpha_t (1 - p_t)\gamma \log(p_t). \] (4)

In the above, \( \alpha_t \) is loss weight that assign to the ground-truth class. \((1 - p_t)\gamma \) is a modulating factor, with tunable focusing parameter \( \gamma \geq 0 \). And \( p_t \) is the model’s estimated probability for the ground-truth class. For notational convenience, \( p_t \) is defined as follows:

\[ p_t = \begin{cases} p_t & \text{if } y = 0 \\ 1 - p_t & \text{otherwise} \end{cases} \] (5)

in the above \( y \in \{0, 1\} \) specifies the ground-truth class. And \( p \) is the model’s estimated probability for genuine class. During training, when the \( p_t \) is small and an example is misclassified, the modulating factor is near 1 and the loss is nearly unaffected. But As \( p_t \to 1 \), the factor goes to 0 and the loss for well-classified examples is down-weighted. As \( \gamma \) increases, the effect of the modulating factor is likewise increased.

3. EXPERIMENT SETUP

In this section, we first present the dataset and evaluation metrics that we used in the experiment. Then, we introduce the details of system implementation.

3.1. Dataset and evaluation metrics

We use the logical access corpus of ASVspoof2019 Challenge [20] to evaluate the performance of our proposed system. As illustrated in table [1] the LA dataset is partitioned into three parts for training, development and evaluation, and each part includes genuine speech and spoofing attacks that generated from different kinds of text to speech (TTS) and voice conversion (VC) algorithms. There exist the same 6 attacks (A01-A06) in the training and development set and 13 attacks (A07-A19) in the evaluation set. It is noted that the evaluation set includes only two known attacks (A16, A19) and other spoofing attacks are unknown (A07-A15, A17, A18). We use the equal error rate (EER) and the tandem detection cost function (t-DCF) as the primary metrics to evaluate the proposed anti-spoofing system. The t-DCF takes both the ASV system and spoofing countermeasure errors into consideration. For the ASV system, the lower the t-DCF, the better the system performance. All results reported in this paper are the best of three runs with different random seeds.

| Table 1. Summary of the ASVspoof 2019 LA dataset |
|-----------------------------------------------|
| bonafide | Spoofer |
| # utterance | # utterance | # attacks |
| Training | 2580 | 22800 | A01-A06 |
| Development | 2548 | 22296 | A01-A06 |
| Evaluation | 7355 | 63882 | A07-A19 |

3.2. Details of system implementation

In this study, We do not extract the hand-crafted features from the raw waveform. We directly use the raw waveform as the input of the proposed network to train the model end-to-end. Since the speech data of ASVspoof 2019 is recorded with varying durations, we have to align the speech data, all examples should be truncated or repeated until the duration is the same. And in the experiments, we keep all the speech data of LA dataset with 6 seconds.

We train each model with 50 epochs for LA dataset. The batch size is set to 32. The model with the lowest EER on the development set is chosen to be evaluated. We select AdamW [21] as the optimizer with an initial learning rate of 0.001, \( \beta_1 \) and \( \beta_2 \) are set to 0.9 and 0.999 respectively. Exponential learning rate decay with a multiplicative factor of 0.97 is adopted. We used focal loss as the model’s loss function, and the loss weight \( \alpha_t \) is decided by the ratio of the spoof and genuine speech in the training dataset. We set \( \gamma \) to 2 in the focal loss. Finally, the anti-spoofing system’s output is directly adopted as the countermeasure (CM) score.

4. RESULTS AND ANALYSIS

In this section, we first present the ablation study for the proposed method and then a comparison of our result to the state-of-the-art systems is presented.

4.1. Ablation study

To further demonstrate the merit of the proposed channel attention module (MECA), we perform ablation experiments for a such module. As shown in Table 3, without the channel attention module, the proposed model could achieve an equal error rate (EER) of 2.39% and min-tDCF of 0.0615 in the ASVspoof 2019 LA evaluation dataset. Integrated with the channel attention module, the equal error rate and the min-tDCF could reduce to 0.64% and 0.0187 respectively, which demonstrate the effectiveness of the proposed channel attention module (MECA). And all these results are much better than the ASVspoof 2019 LA baselines.

As illustrated in Figure [3], we visualize embeddings from the proposed system evaluated on ASVspoof 2019 LA evaluation dataset by applying t-SNE [23]. We can see that embeddings of the proposed model that use channel attention...
Table 2. Breakdown EER (%) performance of all 13 attacks that exists in the ASVspoof 2019 LA evaluation set, pooled min t-DCF(P1), and pooled EER (%), P2. Two state-of-the-art methods and the proposed model are reported. All reported performances are the best of three runs with different random seeds. The best performance for each column is marked in boldface.

| System       | A07 | A08 | A09 | A10 | A11 | A12 | A13 | A14 | A15 | A16 | A17 | A18 | A19 | P1   | P2 (%) |
|--------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|--------|
| Wang et al. [13] | 0.91 | 0.29 | 0.02 | 1.39 | 0.31 | 1.30 | 0.08 | 0.18 | 0.61 | 0.31 | 2.11 | 2.25 | 0.97 | 0.0289 | 0.99  |
| Jung et al. [12]  | 0.80 | 0.44 | 0.00 | 1.06 | 0.31 | 0.91 | 0.10 | 0.14 | 0.65 | 0.72 | 1.52 | 3.40 | 0.62 | 0.0275 | 0.83  |
| Ours                | 0.15 | 0.15 | 0.02 | 0.41 | 0.10 | 0.06 | 0.02 | 0.35 | 0.41 | 0.30 | 2.19 | 0.27 | 0.42 | 0.0187 | 0.64  |

Table 3. Results for the ablation study of the channel attention module (MECA) in the proposed model and the comparison with ASVSpoof 2019 baseline on the ASVspoof 2019 dataset in terms of min t-DCF and pooled EER.

| System       | Development Set | Evaluation Set | min-tDCF | EER(%) | min-tDCF | EER(%) |
|--------------|-----------------|----------------|----------|--------|----------|--------|
| CQCC-GMM [22] |                 |                | 0.0123   | 0.43   | 0.2366   | 9.57   |
| LFCC-GMM [22] |                 |                | 0.0663   | 2.71   | 0.2116   | 8.09   |
| CNBNN        |                 |                | 0.0115   | 0.42   | 0.0615   | 2.39   |
| CNBNN (MECA) |                 |                | 0.0037   | 0.16   | 0.0187   | 0.64   |

module are more discriminative and form a well-constructed manifold in embedding space than the system that without the channel attention module. This result shows that the proposed system that using the channel attention module have a better capacity for feature extraction so as to detect the spoof attacks more effectively.

Fig. 3. Visualization of t-SNE embeddings from proposed systems in ablation study evaluated on the ASVspoof 2019 LA evaluation dataset. Each color represents whether the speech is genuine (bonafide) or spoofed.

4.2. Comparison with state-of-the-art systems

As illustrated in Table 4, we compare our proposed best single system with competing single state-of-the-art systems. These results show that our proposed model could outperform many systems by a large margin. And compare with other single systems, the model that we used for anti-spoofing is still lightweight, it has only 339K parameters in the neural network.

We also perform the comparison with other state-of-the-art systems for the 13 attacks in the evaluation dataset. As illustrated in Table 2, our proposed best single system could outperform the state-of-the-art AASIST system on 9 attacks (A07, A08, A10-A13, A15, A18 and A19), especially, the absolute EER reduction on A18 attack is 3.13%, which is reduce by a large margin.

5. CONCLUSIONS

This work proposes a new end-to-end anti-spoofing system. We revise the ConvNeXt network architecture and then integrate a channel attention module that is modified from the original ECA layer with it to further enhance the model’s anti-spoofing performance. When using the focal loss, the proposed best single system could achieve state-of-the-art performance on LA scenarios. In the future, we will apply the proposed system to other speech tasks.

6. REFERENCES

[1] Ryan Prenger, Rafael Valle, and Bryan Catanzaro, “Waveglow: A flow-based generative network for speech synthesis,” in ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2019, pp. 3617–3621.
Kou Tanaka, Hiroko Kameoka, Takuhiro Kaneko, and Nobukatsu Hoso, “Atts2-vc: Sequence-to-sequence voice conversion with attention and context preservation mechanisms,” in ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2019, pp. 6805–6809.

Zhizheng Wu, Tomi Kinnunen, Nicholas Evans, Junichi Yamagishi, Cemal Hanlıçi, Md Sahidullah, and Aleksandar Sizov, “Asvspoof 2015: the first automatic speaker verification spoofing and countermeasures challenge,” in Sixteenth annual conference of the international speech communication association, 2015.

Jon Sanchez, Ibbon Saratxaga, Inna Hernaez, Eva Navas, Daniel Erro, and Tuomo Raitio, “Toward a universal synthetic speech spoofing detection using phase information,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 810–820, 2015.

Jichen Yang, Rohan Kumar Das, and Nina Zhou, “Extraction of octave spectra information for spoofing attack detection,” IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 27, no. 12, pp. 2373–2384, 2019.

Massimiliano Todisco, Héctor Delgado, and Nicholas Evans, “Constant q cepstral coefficients: A spoofing countermeasure for automatic speaker verification,” Computer Speech & Language, vol. 45, pp. 516–535, 2017.

Xingliang Cheng, Mingxing Xu, and Thomas Fang Zheng, “Replay detection using cqt-based modified group delay feature and resnet newt network in asvspoof 2019,” in 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC). IEEE, 2019, pp. 540–545.

Zhenzong Wu, Rohan Kumar Das, Jichen Yang, and Haizhou Li, “Light Convolutional Neural Network with Feature Genuinization for Detection of Synthetic Speech Attacks,” in Proc. Interspeech 2020, 2020, pp. 1101–1105.

Mostafa Alzantot, Ziqi Wang, and Mani B. Srivastava, “Deep Residual Neural Networks for Audio Spoofing Detection,” in Proc. Interspeech 2019, 2019, pp. 1078–1082.

Xu Li, Na Li, Chao Weng, Xunying Liu, Dan Su, Dong Yu, and Helen Meng, “Replay and synthetic speech detection with res2net architecture,” in ICASSP 2021-2021 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, 2021, pp. 6354–6358.

Guang Hua, Andrew Beng Jin Teoh, and Haijian Zhang, “Towards end-to-end synthetic speech detection,” IEEE Signal Processing Letters, vol. 28, pp. 1265–1269, 2021.

Jee-woon Jung, Hee-soo Heo, Hemlata Tak, Hye-jin Shim, and Nicholas Evans, “Asist: Audio anti-spoofing using integrated spectro-temporal graph attention networks,” in ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022, pp. 6367–6371.

John H.L. Hansen and ZHENYU WANG, “Audio Anti-spoofing Using Simple Attention Module and Joint Optimization Based on Additive Angular Margin Loss and Meta-learning,” in Proc. Interspeech 2022, 2022, pp. 376–380.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770–778.

Zhuo Liu, Hanzi Mao, Chao-Yuan Wu, Christoph Feichtenhofer, Trevor Darrell, and Saining Xie, “A convnet for the 2020s,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 11976–11986.

Qilong Wang, Banggu Wu, Pengfei Zhu, Peihua Li, Wangmeng Zuo, and Qinghua Hu, “Eca-net: Efficient channel attention for deep convolutional neural networks,” in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 11531–11539.

Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger, “Densely connected convolutional networks,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 4700–4708.