Investigation on activation functions for robust end-to-end spoofing attack detection system

Woo Hyun Kang∗, Jahangir Alam†, Abderrahim Fathan

Computer Research Institute of Montreal (CRIM)
woohyun.kang,jahangir.alam,abderrahim.fathan@crim.ca

1. Introduction

The main objective for building a reliable spoofing countermeasure system is to detect the artifacts from the given speech, which may have been caused by the generation process of the spoof attacks. To achieve this, many attempts were made to exploit the techniques which have shown stable performance in the speaker recognition task. In the case of logical access (LA) spoofing detection task the most effective countermeasures are the frame-level acoustic features typically extracted at 10 ms intervals and designed to detect artifacts in the spoofed speech. Classically, the standard Gaussian Mixture Model (GMM) classifier in combination with frame-level acoustic [1–7] or deep features [8] was the most widely adopted spoofing detection approach [1,2,9–10]. But the recent trend in voice anti-spoofing is to employ deep learning architectures in an end-to-end manner on the top of raw signal or hand-crafted acoustic features to discriminate between bonafide and spoof speech signals [9,11–18]. In [11], one class softmax loss with ResNet18 architecture was proposed and outperformed the classical GMM-based methods. In order to further improve the generalization of anti-spoofing systems to unseen test data, several variants of softmax loss were also adopted [11,15]. Although the conventional end-to-end systems were able to outperform the GMM-based spoof detection systems, they follow the same configuration with the ones used in image classification, which may not be an optimal choice for spoof detection task.

In recent years, as the selection of an activation function can affect the ability of the neural network to extract relevant information from the input data, various variants of the conventional rectified linear unit (ReLU) functions were proposed. Especially in [19], a trainable attention-based activation was introduced to efficiently focus on the relevant regions of the feature map. In light of this, in this paper, we investigate the effect of various activation functions on the performance of the end-to-end spoof detection system. Moreover, in order to exploit the complementary information propagated through different activation functions, we propose to employ the activation ensemble technique to the end-to-end system.

To evaluate the performance of the proposed scheme, we conducted a set of experiments using the ASVspoof 2019 dataset. The experimental results show that the end-to-end spoof detection can greatly benefit from the usage of multiple activation functions and activation ensembling, outperforming the conventional methods.

The contributions of this paper are as follows:

• We analyze the performance behaviour of anti-spoofing countermeasure systems with different activation functions.
• We compare the countermeasure performance of the proposed activation ensembled system and the conventional methods.

The rest of this paper is organized as follows: The detailed description of end-to-end spoof detection system and conventional activation functions are described in Section 2 and Section 3, respectively. Section 4 describes the activation ensemble technique. The detailed setting for the experimentation and the results are presented in Section 5, and Section 6 concludes the paper.

2. End-to-end anti-spoofing system

Most deep learning based spoofing detection systems employ deep neural architectures, such as residual network (ResNet), on top of hand-crafted/learned features for capturing more discriminative local descriptors which are then aggregated to generate final fixed dimensional utterance-level embeddings. The embeddings are then fed into a classifier which discriminates whether the input audio is a spoof attack or genuine. Conventionally, a two-stage approach was popularly adopted, where the classifier (e.g., support vector machine (SVM)) and the embedding extraction network are trained separately. Recently, in order to mutually optimize the decision hyperplane and the embedding feature space, various end-to-end approaches [9,11–18] were proposed in the past few years, where the neural classifier is trained jointly with the embedding extraction network.

The proposed model also adopts the end-to-end framework for anti-spoofing, which is composed of 2 networks: an embedding network and a classification network. For the embedding network, we experimented with the squeeze-and-excitation

These authors contributed equally to this work

Abstract

The main objective of the spoofing attack detection system is to detect the artifacts caused by the spoof generation process (i.e., speech synthesis or voice conversion) given a speech sample. Since the selection of an activation function can affect the ability of the end-to-end spoof detection to focus on the relevant regions of the feature map, we investigate the effects of different activation functions in the anti-spoofing countermeasure task. From our results, it could be found that different activation functions enable the end-to-end system to learn complementary information for spoof detection. In order to exploit the complementarity between various activation functions, we propose to adopt the activation ensemble technique within the end-to-end system, where the outputs of different activation functions are pooled together. The proposed framework was experimented on the logical access (LA) task ASVspoof2019 dataset and outperformed the systems using a single activation function.

Woo Hyun Kang∗, Jahangir Alam†, Abderrahim Fathan

Computer Research Institute of Montreal (CRIM)
woohyun.kang,jahangir.alam,abderrahim.fathan@crim.ca

∗These authors contributed equally to this work

16 September 2021, Online

2021 Edition of the Automatic Speaker Verification and Spoofing Countermeasures Challenge
For the past several years, the ReLU activation function was widely used in various neural network systems in speaker verification and end-to-end spoof detection. The ReLU function is defined as follows:

\[ f_{ReLU}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ 0 & \text{otherwise} \end{cases} \]

(2)

where \( x_i \) is the input feature. The main reason behind the popularity of the ReLU activation is that ReLU can overcome the vanishing gradient problem and enables the model to train faster. Although the introduction of the ReLU activation has shown impressive performance in various tasks, due to its inability to handle negative inputs, it was occasionally reported that the ReLU can limit the system’s ability to learn.

In order to solve the limitations of ReLU, various variants were proposed, such as the LeakyReLU, exponential LU (ELU) and randomized ReLU (RReLU). The formulation for LeakyReLU, ELU and RReLU are as follows:

\[ f_{LeakyReLU}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ \gamma x_i & \text{otherwise} \end{cases} \]

(3)

\[ f_{ELU}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ r(e^{x_i} - 1) & \text{otherwise} \end{cases} \]

(4)

where \( \gamma \) and \( r \) are fixed parameters. The RReLU is defined similarly to the LeakyReLU as follows:

\[ f_{RReLU}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ a_i x_i & \text{otherwise} \end{cases} \]

(5)

where \( a_i \) is randomly sampled from \( unif(l, u) \) while training, and \( l \) and \( u \) are fixed parameters. When testing, the \( a_i \) is set to the mean of \( unif(l, u) \), which is \( \frac{l+u}{2} \). As described in equation 3, 4, 5, the ReLU variants commonly focus on taking the negative inputs into consideration by giving a slope to the negative region.

3. Conventional activation functions

3.1. Non-trainable activation functions

The end-to-end antispoofing countermeasure system is depicted in Fig. 1.

The end-to-end system is trained via one-class softmax objective, which can be formulated as [11]:

\[ L_{OCS} = -\frac{1}{N} \sum_{i=1}^{N} \log(1 + e^{k(m_{y_i} - W_0 \omega_i) (-1)^{y_i}}) \]

(1)

where \( k \) is the scale factor, \( \omega_i \in R^D \) and \( y_i \in \{0, 1\} \) are the D-dimensional embedding vector and label of the \( i \)-th sample respectively. \( N \) is the mini-batch size and \( m_{y_i} \) defines the compactness margin for class label \( y_i \). The larger is the margin, the more compact the embeddings will be. \( W_0 \) is the weight vector of our target class embeddings. Both \( W_0 \) and \( \omega_i \) are normalizations of \( W_0 \) and \( \omega_i \) respectively.
3.2. Trainable activation functions

In order to allow the activation functions to operate in a data-adaptive manner, several learnable activation functions were proposed. One of them is the parametric ReLU (PReLU), which operates in a similar fashion to the LeakyReLU, but uses a trainable parameter for the negative slope:

\[
f_{\text{PReLU}}(x_i) = \begin{cases} 
    x_i & \text{if } x_i > 0 \\
    \xi x_i & \text{otherwise,}
\end{cases}
\]

where \(\xi\) is a learnable parameter.

The attention ReLU (AreLU) goes one step further than the other ReLU variants, by employing a trainable attention mechanism to boost the contribution of relevant input features while suppressing the irrelevant ones [19]. More specifically, the AreLU is a combination of the standard ReLU and the elementwise sign-based attention (ELSA). Given input \(x_i\), which is the \(i^{th}\) element of feature \(X\), the AreLU is formulated as follows:

\[
f_{\text{AreLU}}(x_i) = f_{\text{ReLU}}(x_i) + g_{\text{att}}(x_i, \alpha, \beta)
\]

where \(\alpha\) and \(\beta\) are learnable scaling parameters, \(C\) is the clamping operation which restricts the value to \([0.01, 0.99]\), and \(\sigma\) is the sigmoid function. While the \(\beta\) parameter amplifies the positive elements, the \(\alpha\) parameter suppresses the negative elements.

4. Activation ensemble framework

As described in equations 2–8, each activation operates and focuses on different aspects of the feature map. Therefore, in order to exploit the complementary information propagated through the different activations, we propose to apply activation ensemble [21] to the end-to-end system. Instead of using a single type of activation function, the activation ensemble scheme uses multiple activation functions and pools their outputs via summation:

\[
f_{\text{ens}}(x_i) = \sum_{j=1}^{J} f_j(x_i),
\]

where \(f_j\) is an activation and \(J\) is the number of unique activation functions used. The general framework of the activation ensemble framework is depicted in Figure 2.

Table 2: Summary of ASVspoof2019 logical Access (LA) corpora in terms of training (Train), development (Dev) and evaluation (Eval) partitions and number of recordings.

<table>
<thead>
<tr>
<th></th>
<th>#Speakers</th>
<th>#Recordings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bona</td>
<td>Fide</td>
</tr>
<tr>
<td>Training partition</td>
<td>20</td>
<td>2.580</td>
</tr>
<tr>
<td>Development partition</td>
<td>20</td>
<td>2.548</td>
</tr>
<tr>
<td>Evaluation partition</td>
<td>67</td>
<td>7.355</td>
</tr>
</tbody>
</table>

Table 3: Initial values for the parameters of the activation functions.

<table>
<thead>
<tr>
<th>(\xi) (PReLU)</th>
<th>(\gamma) (LeakyReLU)</th>
<th>(r) (ELU)</th>
<th>(l) (RReLU)</th>
<th>(u) (RReLU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.25</td>
<td>0.2</td>
<td>1.0</td>
<td>0.125</td>
<td>0.333</td>
</tr>
</tbody>
</table>

5. Experiments

5.1. Experimental setup

As local frame-level frame hand-crafted features, we use 60-dimensional linear frequency cepstral coefficients (LFCC) extracted using 25ms analysis window over a frame shift of 10ms. No data augmentation was performed in our experiments.

For training and evaluating the experimented systems, the ASVspoof 2019 challenge dataset was used, which provides a common framework with a standard corpora for conducting spoofing detection research on LA attacks. The LA dataset includes bonafide and spoof speech signals generated using various state-of-the-art voice conversion and speech synthesis algorithms. A summary of the LA corpora in terms of training (Train), development (Dev) and evaluation (Eval) partitions and number of recordings is presented in Table 2. The development and evaluation subsets constitute the seen and unseen test sets in terms of spoofing attacks. For more details about the corpora, the interested readers are referred to [22]. For training all the experimented systems, balanced mini-batches of size 64 samples were used. The ADAM optimizer was used with initial learning rate of 0.0003 and exponential learning rate decay with rate of 0.5 was applied [11, 18].

For comparing the performance of different systems, the official evaluation metrics of ASVspoof2019 challenge, equal error rate (EER) and minimum tandem detection cost function (min-tDCF) [23], were used. The lower the values of EER and min-tDCF, the better performance is attained. The ASV scores provided by the challenge organizer were used for computing min-tDCF.

5.2. Experimental results

5.2.1. Comparison between different ReLU variants

In this experiment, we compare the performance of end-to-end systems with different activation functions. More specifically, we compare 6 types of ReLU-based activation functions: ReLU, LeakyReLU [24], Randomized LeakyReLU (RReLU) [25], exponential linear unit (ELU) [26], parametric ReLU (PReLU) [27], and AreLU. The initial values for the parameters of each activation function is described in Table 3.
Table 4: The experimental results of the SE-ResNet-18-based end-to-end systems with different activation functions on the ASVSpoof2019 Logical Access Development and Evaluation sets.

<table>
<thead>
<tr>
<th></th>
<th>Dev EER [%]</th>
<th>Eval EER [%]</th>
<th>min-tDCF</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReLU</td>
<td>0.1082</td>
<td>3.0589</td>
<td>0.0718</td>
</tr>
<tr>
<td>LeakyReLU</td>
<td>0.2363</td>
<td>2.7999</td>
<td>0.0696</td>
</tr>
<tr>
<td>RReLU</td>
<td>0.2697</td>
<td>3.2104</td>
<td>0.0790</td>
</tr>
<tr>
<td>ELU</td>
<td>0.2366</td>
<td>4.7026</td>
<td>0.0980</td>
</tr>
<tr>
<td>PReLU</td>
<td>0.1480</td>
<td>2.6515</td>
<td>0.0663</td>
</tr>
<tr>
<td>AReLU</td>
<td>0.2433</td>
<td>2.3770</td>
<td>0.0586</td>
</tr>
</tbody>
</table>

Table 5: The experimental result of the single activation and the activation ensembled systems on the ASVSpoof2019 Logical Access Development and Evaluation sets.

<table>
<thead>
<tr>
<th></th>
<th>Dev EER [%]</th>
<th>Eval EER [%]</th>
<th>min-tDCF</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReLU+AReLU+PReLU+LeakyReLU+ELU</td>
<td>0.3538</td>
<td>2.5700</td>
<td>0.0658</td>
</tr>
<tr>
<td>AReLU+LeakyReLU</td>
<td>0.1968</td>
<td>2.3410</td>
<td>0.0630</td>
</tr>
<tr>
<td>ReLU+PReLU</td>
<td>0.1968</td>
<td>2.3625</td>
<td>0.0565</td>
</tr>
<tr>
<td>ReLU+LeakyReLU+ELU</td>
<td>0.1968</td>
<td>2.2464</td>
<td>0.0550</td>
</tr>
<tr>
<td>ReLU+AReLU+PReLU+LeakyReLU+ELU</td>
<td>0.3538</td>
<td>2.1410</td>
<td>0.0575</td>
</tr>
</tbody>
</table>

Figure 3: The DET curves of the SE-ResNet-18-based systems with different activation functions on the ASVSpoof2019 Logical Access Evaluation set.

Another interesting point to notice from the results is that the learnable activation functions (i.e., PReLU, AReLU) were able to perform better than the fixed activations (i.e., ReLU, LeakyReLU, RReLU, ELU). This may be attributed to the fact that the learnable activation functions are more capable of suppressing the nuisance features as their scaling parameters are optimized in a data-adaptive fashion.

Among the learnable activations (i.e., PReLU, AReLU), the AReLU achieved the best performance, which outperformed the PReLU with a relative improvement of 11.61% in terms of min-tDCF. Although the PReLU suppresses the negative elements in a similar manner to the AReLU, it does not attempt to amplify the relevant features. Therefore the AReLU may be more suited to focus on the artifacts caused by the generation process of the spoof attacks (e.g., speech synthesis, voice conversion), as it can emphasize the positive elements via learnable scaling parameter $\beta$.

The DET curves of the experimented systems are depicted in Fig. 3.

5.2.2. Activation ensemble for end-to-end spoofing countermeasure system

Analogous to the single activation systems, the ensemble system was trained in an end-to-end fashion, taking the LFCC features as input. Table 5 shows the performance of the activation ensembled systems with different combinations of activation functions. As depicted in the results, although the performance on the development set was slightly degraded compared to the standard ReLU activation, the ReLU-based system could benefit greatly in terms of detecting unseen attacks by using learnable activation functions (e.g., AReLU, PReLU) in conjunction via activation ensemble. Especially using the ReLU and AReLU together achieved a relative improvement of 22.67% in terms of EER over the ReLU-based system on the evaluation set. Similarly, the performance of the AReLU-based system could be improved by ensembling various non-learnable activation functions (e.g., LeakyReLU, ELU). Especially when using the AReLU and ELU achieved a relative improvement of 6.14% in terms of min-tDCF over the AReLU-based system. The best performance in terms of EER was observed by ensembling the ReLU, AReLU, PReLU, LeakyReLU and ELU.

6. Conclusion

In this paper, we investigate the effects of different activation functions employed in an end-to-end spoof detection system. More specifically, we experimented with several variants of the conventional rectified linear unit (ReLU) activation function on the ASVSpoof2019 Challenge logical access dataset, and analyzed their performance to capture the artifacts created by the spoof generation process.

Our results showed that using learnable activation functions, such as parametric ReLU (PReLU) or attention ReLU (ARelu) can greatly improve the anti-spoofing countermeasure performance over the non-learnable activation functions (i.e., ReLU, LeakyReLU, randomized ReLU, exponential LU). Moreover, in order to fully consider the complementary information learned by each activation, we have proposed an end-to-end system with multiple activation functions via activation ensemble. From our results, we could see that ensembling multiple different activation functions, including the learnable and non-learnable ones, can greatly improve the performance in terms of spoof detection.

In our future study, we will be expanding the AReLU activation function to be more suited for finding the artifacts within the given speech spectrum. Moreover, we will be exploring a more effective way to exploit the complementary information learned via different activation functions. Furthermore, we will be evaluating the end-to-end systems with attentive activation function on other spoofing attack types, such as the physical
access spoofing attack.

7. Acknowledgment
We wish to acknowledge funding from the Natural Sciences and Engineering Research Council of Canada (NSERC) through grant RGPIN-2019-05381 and Ministry of Economy and Innovation (MEI) of the Government of Quebec for the continued support.

8. References


