Attentive activation function for improving end-to-end spoofing countermeasure systems

Woo Hyun Kang, Jahangir Alam, Abderrahim Fathan

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

Abstract
The main objective of the spoofing countermeasure system is to detect the artifacts within the input speech caused by the speech synthesis or voice conversion process. In order to achieve this, we propose to adopt an attentive activation function, more specifically attention rectified linear unit (AReLU) to the end-to-end spoofing countermeasure system. Since the AReLU employs the attention mechanism to boost the contribution of relevant input features while suppressing the irrelevant ones, introducing AReLU can help the countermeasure system to focus on the features related to the artifacts. The proposed framework was experimented on the logical access (LA) task of ASVSpoof2019 dataset, and outperformed the systems using the standard non-learnable activation functions.

1. Introduction
In the past decade, attributed to the widespread deployment of smart devices, automatic speaker verification (ASV) has become an essential technology for user authentication. However, due to the dramatic improvement in the speech synthesis and voice conversion techniques in recent years, many concerns were raised regarding the spoofing attacks on the ASV systems. In order to countermeasure these spoofing attacks, various researches were conducted to discriminate the synthetic speech samples from the genuine (bona fide) samples.

The main objective for building a reliable spoofing countermeasure system is to detect the artifacts from the synthetic speech spectrum. 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 extracted at 10 ms intervals and designed to detect artifacts in the spoofed speech. Previously, the standard Gaussian Mixture Model (GMM) classifier in combination with frame-level acoustic [10] or deep features [9] was the most widely adopted spoofing detection approach [12,9,10].

But the recent trends in voice anti-spoofing is to employ deep learning architectures in an end-to-end fashion on the top of raw statistical-based spoofing systems (e.g., GMM, i-vector), their results suggest that there is still more room for improvement. In order to effectively capture the artifact relevant to the spoof attacks within the given speech spectrogram, we propose to adopt an attentive activation function to the end-to-end spoofing countermeasure system. More specifically, we exploited the attention rectified linear unit (AReLU) [19], which is known to provide well-focused activation of relevant regions of the feature map. By introducing the AReLU activation in the front-end network, the countermeasure system can focus on the artifacts created by the spoofing process while suppressing the irrelevant features.

To evaluate the performance of the proposed scheme, we conducted a set of experiments using the ASVSpoof 2019 logical access dataset. The experimental results show that the AReLU-based end-to-end system was able to be optimized with more stability than the systems with the standard rectified linear unit (ReLU) activation. Moreover, the proposed system outperformed the conventional methods.

The contributions of this paper are as follows:
• We analyze the training behavior of anti-spoofing countermeasure systems with different activation functions.
• We compare the countermeasure performance of the proposed AReLU-based end-to-end system and the conventional methods.
• We compare the countermeasure performance of the activation ensembled systems which employ AReLU activation and various other ReLU variants.
• From the best of our knowledge, this is the first attempt on using the AReLU for anti-spoofing countermeasure system.

2. End-to-end anti-spoofing system with attentive activation function
2.1. 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
The proposed model also adopts the end-to-end framework for antispoofing, which is composed of 2 networks: an embedding network and a classification network. For the embedding network, we experimented with one TDNN-based and two ResNet-based architectures, which have shown competitive performance in the speaker verification and image classification tasks:

- TDNN: also known as the x-vector architecture, which is composed of 5 TDNN layers. More information on the architecture can be found in [20].
- ResNet-18: an 18 layers deep convolutional network, which is composed of 4 residual blocks.
- SE-ResNet-18: a variant of the ResNet-18, where a squeeze-and-excitation (SE) block [21] is applied at the end of each non-identity branch of residual block to significantly decrease the computational cost of the system.

To aggregate the frame-level output of the ResNet, an attention pooling layer is incorporated where the weighted first and second order (i.e., standard deviation) moments are pooled together across the temporal dimension [9,11,15,16,18] to obtain an utterance-level representation. The pooled statistics are then fed into a neural classifier, which consists of a fully-connected layer and a 2-dimensional softmax layer, where each softmax node represents the bona fide and spoofing classes, respectively.

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

\[
L_{DOS} = - \frac{1}{N} \sum_{i=1}^{N} \log(1 + e^{k(y_i - \hat{w}_i \hat{\omega}_i) \alpha_i \beta_i})
\] (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 \(\hat{\omega}_i\) are normalizations of \(W_0\) and \(\omega_i\) respectively.

### 2.2. Attention Rectified Linear Unit (AReLU)

AReLU is a variant of the ReLU function, which employs the 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 element-wise sign-based attention (ELSA). Given input \(x_i\), which is the \(i^{th}\) element of feature \(X\), the AReLU is formulated as follows:

\[
\tilde{f}_{AReLU}(x_i) = f_{ReLU}(x_i) + g_{att}(x_i, \alpha, \beta)
\] (2)

\[
= \begin{cases} 
    C(\alpha) x_i & \text{if } x_i < 0 \\
    (1 + \sigma(\beta)) x_i & \text{otherwise} 
\end{cases}
\] (3)

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. Unlike the standard ReLU which has a fixed scaling parameters, since the parameters of AReLU are learned in a data-adaptive fashion, they can effectively learn and emphasize the salient elements (e.g., artifacts caused by the spoofing) for antispoofing countermeasure.

In order to enable the end-to-end antispoofing system to efficiently capture the artifacts within the input spectrogram, we used AReLU as the very first activation of the frame-level network, which is placed right after the first 2D-Conv layer. Moreover, to ensure that the extracted embedding reflects the relevant elements of the frame-level representations, we also used AReLU as the last activation of the frame-level network, which is prior to the pooling layer. In our experiments, we have used shared AReLU parameters for the first and last layers.
Table 2: Summary of ASVspoof2019 logical Access (LA) corpora in terms of training (Train), development (Dev) and evaluation (Eval) partitions and number of recordings.

|                  | #Speakers | #Recordings |
|------------------|-----------|-------------|
|                  | Bona fide | Spoof       |
| Training partition | 20        | 2,580       |
| Development partition | 20       | 2,548       |
| Evaluation partition | 67       | 7,355       |

Figure 2: Training losses of the ReLU-based and AReLU-based end-to-end antispoofing countermeasure systems. The y-axis represents the training loss value, while the x-axis represents the training iterations.

3. Experiments

3.1. Experimental setup

As local frame-level hand-crafted features we use 60-dimensional (including the delta and double delta coefficients) 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 corpus for conducting spoofing detection research on LA attacks. 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. In our experiments, we have used the development subset as validation set. 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.

3.2. Experimental results

3.2.1. Training analysis

In this experiment, we compared the effect of AReLU in terms of training stability when optimizing the end-to-end spoofing countermeasure system. Fig. 2 depicts the training losses of the standard end-to-end system with ReLU activations, and our proposed AReLU-based system. As shown in Fig. 2, the training losses for both systems were able to decrease as the training proceeds. However, it could be observed that while the ReLU-based system experienced occasional fluctuation in the training loss (e.g., around 2,000-th iteration), the AReLU-based system was able to be trained in a relatively much stable manner. This may be attributed to the fact that the attention mechanism of AReLU learns the element-wise residues for the activated (positive) elements with respect to the standard ReLU, which can significantly reduce the gradient vanishing problem.

3.2.2. Attentive activation function for different frame-level networks

In this experiment, we compare the antispoofing countermeasure performance of the TDNN, ResNet-18 and SE-ResNet-18-based end-to-end systems with ReLU and AReLU activations. As shown in Table 3, it could be seen that in all the experimented systems, the use of AReLU was able to outperform the standard ReLU activation in terms of EER and min-tDCF. Especially in the SE-ResNet-18 architecture, the usage of AReLU achieved a relative improvement of 18.38% over the ReLU, in terms of min-tDCF. Since the antispoofing performance is highly dependent on the system’s ability to detect the artifacts within the speech spectrogram, we could safely assume that the AReLU can enable the countermeasure system to focus more on the relevant features.

3.2.3. 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 formulation for LeakyReLU, ELU and PReLU are as follows:

\[
\text{LeakyReLU}(x) = \begin{cases} 
  x & \text{if } x > 0 \\
  \gamma x & \text{otherwise}
\end{cases}
\]
Figure 3: The DET curves of the SE-ResNet-18-based systems with different activation functions on the ASVSpoof2019 Logical Access Evaluation set.

Table 4: The experimental results of the SE-ResNet-18-based end-to-end systems with different activation functions on the ASVSpoof2019 Logical Access Evaluation set.

| Activation     | EER [%] | min-tDCF |
|----------------|---------|----------|
| LFCC-GMM       | 9.5700  | 0.2366   |
| CQCC-GMM       | 8.0900  | 0.2116   |
| ReLU           | 3.0589  | 0.0718   |
| LeakyReLU      | 2.7999  | 0.0696   |
| ELU            | 4.7026  | 0.0980   |
| PReLU          | 2.6515  | 0.0663   |
| AReLU          | 2.3770  | 0.0586   |

Table 5: The experimental results of the score-level average fusion between systems with different activation functions on the ASVSpoof2019 Logical Access Evaluation set.

| Fusion Method  | EER [%] | min-tDCF |
|----------------|---------|----------|
| AReLU          | 2.3770  | 0.0586   |
| AReLU+ReLU     | 2.3647  | 0.0586   |
| AReLU+LeakyReLU| 2.3794  | 0.0620   |
| AReLU+RReLU    | 2.6815  | 0.0644   |
| AReLU+ELU      | 2.8675  | 0.0707   |
| AReLU+PReLU    | 2.4486  | 0.0641   |

\[ f_{\text{ELU}}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ r(e^{\gamma x_i} - 1) & \text{otherwise} \end{cases} \quad (5) \]

\[ f_{\text{PReLU}}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ \xi_i x_i & \text{otherwise} \end{cases} \quad (6) \]

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

\[ f_{\text{RReLU}}(x_i) = \begin{cases} x_i & \text{if } x_i > 0 \\ a_i x_i & \text{otherwise} \end{cases} \quad (7) \]

where \( a_i \) is randomly sampled from \( \text{unif}(l, u) \) while training, and \( l \) and \( u \) is fixed parameters. When testing, the \( a_i \) is set to the mean of \( \text{unif}(l, u) \), which is \( \frac{l + u}{2} \). The initial value for \( \xi_i \) and \( \gamma, r, l, u \) were set to 0.25, 0.2, 1.0, 0.125, 0.333, respectively in our experiments. The experimented activation functions are depicted in Figure 4, where the visualization was done based on the initial parameters.

Another interesting point to notice from the results is that the learnable activation functions (i.e., PReLU, AReLU) were generally 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 similarly 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 spoofing process, as it can emphasize the positive elements via learnable scaling parameter \( \beta \).

3.2.4. Score-level fusion of end-to-end systems with different activation

In this experiment, we fuse the antispoofer scores produced by the AReLU-based end-to-end system and systems with other
activation functions. For the score-level fusion, we have experimented average fusion, where the average of the output scores of different systems is computed. From Table 6 it could be seen that fusing the scores of the AReLU system with other ReLU variants (i.e., LeakyReLU, RReLU, ELU, PReLU) was not so beneficial. Since the experimented ReLU variants commonly focuses on allowing negative values during the non-linear transformation process, it is likely that these activation functions encode similar information to each other. Therefore fusing the AReLU system with the other ReLU variants may result in redundant information on the artifacts, thus failing to improve the performance.

On the other hand, fusing the standard ReLU with the AReLU-based system showed improvement. This may be attributed to the fact that unlike the AReLU, or any other ReLU variants, the ReLU forces the network to focus only on the positive values, which may lead the system to learn complementary information to the AReLU-based architecture.

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

In this experiment, we applied activation ensembles [29] to the end-to-end system in order to exploit the potential complementarity of the AReLU and other activation functions. Instead of using a single type of activation function, the activation ensemble scheme uses multiple activation functions and pool their outputs via summation:

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

where $f_j$ is an activation and $J$ is the number of unique activation functions used. Analogous to the single activation systems, the ensemble system was trained in an end-to-end fashion, taking the LFCC features as input. Table 7 shows the performance of the activation ensembled systems. As depicted in the results, the ReLU-based system could benefit greatly in terms of detecting unseen attacks by using AReLU in conjunction with activation ensemble, which 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, where the batch normalization layer was dropped in light of the observation made in [26]. Furthermore, it could be seen from Table 7 that the performance differs depending on the combination of activations used for ensemble in ASVspoof2021 settings as well [29].

4. Conclusion

In this paper, we proposed the usage of attentive activation function for the end-to-end anti-spoofing countermeasure system. More specifically, we explored with the idea of introducing the attention rectified linear unit (AReLU) activation to the ResNet-based end-to-end system. As the AReLU is known to be capable of providing well-focused activation of relevant features, the use of AReLU can enable the anti-spoofing system to focus on the artifacts created by the spoof process while suppressing the irrelevant features.

In order to evaluate the proposed AReLU-based end-to-end framework, we have conducted several experiments on the ASVspoof2019 Challenge logical access dataset. Our results showed that using the AReLU can greatly improve the anti-spoofing countermeasure performance over the other activation functions (i.e., ReLU, LeakyReLU, randomized ReLU, exponential LU, parametric ReLU). Moreover, from our experiments, it could be observed that the end-to-end systems with AReLU and other ReLU variants can learn complementary information regarding the anti-spoofing task. Hence further performance enhancement was observed when ensembling the AReLU-based system with different variants of ReLU activations.

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, such as employing the weighted activation ensemble scheme. 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.

5. Acknowledgment

The authors wish to acknowledge funding from the Natural Sciences and Engineering Research Council of Canada (NSERC) through grant RGPIN-2019-05381. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the NSERC.
6. References

[1] Massimiliano Todisco et al., “Constant q cepstral coefficients: A spoofing countermeasure for automatic speaker verification,” *Computer Speech & Language*, vol. 45, pp. 516–535, 2017.

[2] Md Sahidullah et al., “A comparison of features for synthetic speech detection,” in *Proc. Interspeech*, 2015, pp. 2087–2091.

[3] Jahangir Alam and Patrick Kenny, “Spoofing detection employing infinite impulse response—constant q transform-based feature representations,” in *Proc. EUSIPCO*, 2017, pp. 101–105.

[4] Xiaohai Tian et al., “Spoofing detection from a feature representation perspective,” in *Proc. ICASSP*, 2016, pp. 2119–2123.

[5] Tanvina B Patel and Hemant A Patil, “Combining evidences from mel cepstral, cochlear filter cepstral and instantaneous frequency features for detection of natural vs. spoofed speech,” in *Proc. Interspeech*, 2015.

[6] Tanvina B Patel and Hemant A Patil, “Effectiveness of fundamental frequency (f0) and strength of excitation (soe) for spoofed speech detection,” in *Proc. ICASSP*, 2016, pp. 5105–5109.

[7] Xiong Xiao et al., “Spoofing speech detection using high dimensional magnitude and phase features: The ntu approach for asvspoof 2015 challenge,” in *Proc. Interspeech*, 2015.

[8] Md Jahangir Alam et al., “Spoofing detection on the asvspoof2015 challenge corpus employing deep neural networks,” in *Proc. Odyssey*, 2016, pp. 270–276.

[9] J. Monteiro and J. Alam, “Development of voice spoofing detection systems for 2019 edition of automatic speaker verification and countermeasures challenge,” in *Proc. ASRU*, 2019, pp. 1003–1010.

[10] Hemlata Tak et al., “Spoofing Attack Detection Using the Non-Linear Fusion of Sub-Band Classifiers,” in *Proc. Interspeech*, 2020, pp. 1106–1110.

[11] You Zhang et al., “One-class learning towards synthetic voice spoofing detection,” *IEEE Signal Processing Letters*, vol. 28, pp. 937–941, 2021.

[12] P. RahulT et al., “Audio spoofing verification using deep convolutional neural networks by transfer learning,” *ArXiv*, vol. abs/2008.03464, 2020.

[13] Galina Lavrentyeva et al., “STC Antispoofing Systems for the ASVspoof2019 Challenge,” in *Proc. Interspeech*, 2019, pp. 1033–1037.

[14] Zhenzong Wu et al., “Light Convolutional Neural Network with Feature Genuinization for Detection of Synthetic Speech Attacks,” in *Proc. Interspeech*, 2019, pp. 1101–1105.

[15] Tianxiang Chen et al., “Generalization of Audio Deepfake Detection,” in *Proc. Odyssey*, 2020, pp. 132–137.

[16] Joao Monteiro et al., “A multi-condition training strategy for countermeasures against spoofing attacks to speaker recognizers,” in *Proc. Odyssey*, 2020, pp. 296–303.

[17] Hemlata Tak et al., “End-to-end anti-spoofing with rawnet2,” in *Proc. ICASSP*, IEEE, Ed., Ontario, 2021.

[18] Joao Monteiro et al., “Generalized end-to-end detection of spoofing attacks to automatic speaker recognizers,” *Computer Speech & Language*, p. 101096, 2020.

[19] Dengsheng Chen and Kai Xu, “Arelu: Attention-based rectified linear unit,” *arXiv preprint arXiv:2006.13858*, 2020.

[20] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, and S. Khudanpur, “X-vectors: Robust dnn embeddings for speaker recognition,” in *Proc. ICASSP*. IEEE, 2018.

[21] Jie Hu, Li Shen, and Gang Sun, “Squeeze-and-excitation networks,” in *Proc. CVPR*, 2018, pp. 7132–7141.

[22] ASVspoof consortium, *ASVspoof 2019:Automatic Speaker Verification Spoofing and Countermeasures Challenge Evaluation Plan*, 2019 (accessed May 13, 2020).

[23] Tomi Kinnunen et al., “t-dcf: a detection cost function for the tandem assessment of spoofing countermeasures and automatic speaker verification,” *arXiv preprint arXiv:1804.09618*, 2018.

[24] A.L. Maas et al., “Rectifier nonlinearities improve neural network acoustic models,” in *Proc. ICML*, 2013.

[25] Bing Xu et al., “Empirical evaluation of rectified activations in convolutional network,” *arXiv preprint arXiv:1505.00853*, 2015.

[26] Djork-Arné Clevert et al., “Fast and accurate deep network learning by exponential linear units (elus),” in *Proc. ICLR*, 2016.

[27] Kaiming He et al., “Delving deep into rectifiers: Surpassing human-level performance on imagenet classification,” *arXiv preprint arXiv:1502.01852*, 2015.

[28] Junichi Yamagishi, Xin Wang, Massimiliano Todisco, Md Sahidullah, Jose Patino, Andreas Nautsch, Xuechen Liu, Kong Aik Lee, Tomi Kinnunen, Nicholas Evans, and Héctor Delgado, “Asvspoof 2021: accelerating progress in spoofed and deepfake speech detection,” 2021.

[29] Diego Klabjan and Mark Harmon, “Activation ensembles for deep neural networks,” in *Proc. Big Data*, 2019, pp. 206–214.