An Attention-Based Method for Guiding Attribute-Aligned Speech Representation Learning

Yu-Lin Huang¹, Bo-Hao Su¹, Y.-W. Peter Hong¹,², Chi-Chun Lee¹,²

¹Department of Electrical Engineering, National Tsing Hua University, Taiwan
²Institute of Communication Engineering, National Tsing Hua University, Taiwan

huang8592301@gmail.com, borrissu@gapp.nthu.edu.tw, {ywhong,cclee}@ee.nthu.edu.tw

Abstract

The rich personal information contained in speech signal can lead to privacy leakage and unfair prediction for speech based technology. In this work, we propose a feature-scoring variational autoencoder (FS-VAE) to handle these issues by performing attribute alignment for speech representation learning. FS-VAE performs attribute alignment by using attention-based scoring machines guided by two additional penalty terms. After obtaining the attribute-aligned representation, we can then choose and mask the nodes containing specific attribute of interest based on the requirement in the downstream tasks. We evaluate our methods on tasks of PP-SER (identity-free emotion recognition) and PP-SV (emotion-less speaker verification). Our proposed method achieves better utility maintenance and competitive privacy protection compared to the most recent attribute-aligned representation learning method.

Index Terms: speech representation, feature scoring, privacy, fair, attribute alignment

1. Introduction

Speech is the most natural human communication medium that has motivated a thriving effort in the development of speech related technology [1, 2, 3, 4, 5]. The richness of information in human’s speech signal [6] while useful but also concerning. As speech signal contains rich personal information [7], e.g., identity, gender, and emotion, users may unexpectedly disclose these sensitive attributes while utilizing speech based services. On the other hand, unfairness may occur as data-driven approaches naturally inherit biases, e.g., gender bias [8] or racial discrimination [9]. As effort being devoted toward achieving trustworthy AI, devising strategy to obtain a speech representation that mitigates biases and privacy concerns directly at the front-end representation is becoming the prevalent approach.

Recently, many works utilize adversarial strategy to eliminate a pre-defined attribute in the speech representation to deal with these issues [10, 11, 12]. While promising, adversarial learning suffers from inflexibility, i.e., one has to retrain an encoder to obtain a specific attribute-removed representation under each setting of an application. Hence, in a recent work, Huang et al. proposed an attribute-aligned speech representation learning method [13], which aligns the task-specific attributes in a particular order for the speech representation, e.g., emotion related (without speaker identity) dimensions are concentrated in the top half of the hidden nodes where speaker identity (without emotion) locate in the bottom half. By aligning attributes along node dimensions, one can flexibly choose and mask the hidden nodes depending on the application scenarios. Specifically, Huang et al. [13] proposed a layered representation variational autoencoder (LR-VAE) to handle a two-attribute scenario (emotion and speaker identity) and demonstrated competitive privacy-preserving performances with a single encoder (as compared to two for adversarial learning approaches).

However, since LR-VAE depends on manually designed two monotonic dropout functions to align two attributes in the hidden nodes, crafting such functions that extend to three or four or even more attributes can be complicated if not infeasible. In this work, we propose a feature-scoring variational autoencoder (FS-VAE) to achieve attribute alignment. Instead of designing functions to align attributes, we guide the attribute aligned representation learning process by using task-specific attention-based scoring machines along with two additional losses, i.e., attention penalty loss and diversity loss. This approach separates task-specific attributes to distribute distinctively on different latent dimensions. In downstream tasks, one can choose and mask those dimensions needed to maintain a high main-task recognition performance and protect privacy by removing those un-needed dimensions according to the learned attention weights from these scoring machines.

In this work, we present two task definitions: a privacy-preserving speech emotion recognition (PP-SER) that protects identity in SER and a privacy-preserving speaker verification (PP-SV) that protects emotion in SV. We evaluate our method on the MSP-Podcast [14]. Comparing to LR-VAE, the current state-of-the-art attribute-aligned representation learning method, our proposed FS-VAE achieves competitive PP-SER performance (1.86% WFS better, 2.26% EER worse) and improved PP-SV performance (1.08% EER better, 0.30% WFS worse). We also observe that FS-VAE concentrates the task-specific attributes to a fewer number of nodes.

2. Methodology

2.1. Dataset description

We evaluate our method on two tasks, PP-SER and PP-SV. For evaluation, an emotional speech dataset with multiple speakers is required. Hence, we utilize the MSP-Podcast corpus [14], one of the largest emotional corpus with many speakers. In total, the MSP-Podcast contains 33262 speaking turns amounting to 56 hours. In this work, in order to compare fairly to the previous work [13], we perform 5-class emotion classification: neutral, angry, sad, happy and disgust. The distribution of the 5 emotion classes are: neutral: 53.05%, angry: 8.81%, sad: 3.95%, happiness: 27.10%, and disgust: 7.09%. We used the standard splits in Release 1.4 that contains 610 speakers in training set, 30 speakers in development set, and 30 speakers in testing set. Note that the speakers in each set are disjoint.

2.2. Feature extraction

We apply wav2vec2.0 [15], a self-supervised speech representation trained by masking the speech input and solving contrastive task, as input feature. Wav2vec2.0 can be seen as an uni-
versal front-end speech embedding and has achieved outstanding results across numerous downstream applications [16, 17]. Specifically, we extract wav2vec2.0 embedding by the released pre-trained model [18], wav2vec2-base, that was trained on the LibriSpeech [19]. Notice that the output of wav2vec2.0 is frame based. We apply average pooling along the time axis to obtain a 768 dimensional feature vector for each utterance.

2.3. Attribute-aligned learning strategy

Attribute-aligned learning strategy aims to learn an encoder which forces task-specific information to condense and distinctively distribute on specific node dimensions. In this work, we propose a feature-scoring variational autoencoder (FS-VAE) to achieve attribute-alignment, including VAE as the representation learning backbone, task-specific feature-attention mechanism, with two designated loss terms, i.e., attention loss and diversity loss.

We apply VAE [20] as backbone for disentangled representation learning, which factorizes the input feature into independent latent dimension. The loss function of VAE is defined as:

$$L_{VAE} = -E_p(x|z) \log p(x|z) + D_{KL}(q(z|x)||p(z))$$  

(1)

Here, $D_{KL}()$ stands for the non-negative Kullback-Leibler divergence, which encourages the distribution of the latent dimension to be close to an isotropic Gaussian.

2.3.1. Feature-scoring attention mechanism

To perform attribute-selection in downstream tasks, we require a mechanism that distributes the task-specific information distinctively, i.e., encouraging each node to be responsible for a single attribute. We employ an attention-based mechanism, i.e., feature-scoring machines (FSM) [21, 22], on the latent vector to capture the attribute-specific information. Define the FS-VAE latent code as $z \in \mathbb{R}^F$ and a scoring vector $s \in \mathbb{R}^F$, where $0 \leq s_i \leq 1$ for $i \in \{0, \ldots, F-1\}$. During FS-VAE training, a weighted feature vector is generated by $z' = s \ast z$, where $\ast$ denotes an element-wise product, and then fed into the classifier for attribute-specific information extraction. During the optimization step, the dimensions of the latent code with higher scores for emotion attribute will be updated more when back-propagating emotion classification loss, (hence, containing more emotion-related information), and vice versa. In this work, two FSMs are trained to capture the emotion-related attribute and identity-related attribute, respectively.

Further, to purify the latent dimensions after attribute alignment, we apply Gradient Reversal Layer (GRL) [23]. We re-direct the reversed gradients to affect those nodes with significant importance to the particular task. During training, we input a masked feature vector $\tilde{z} = m \ast z$ to the discriminator, where the mask vector $m$ is generated by a threshold function $f(s)$:

$$m_i = f(s_i) = \begin{cases} 1, & s_i \geq \theta_t \\ 0, & s_i < \theta_t \end{cases}$$  

(2)

Here, $\theta_t$ represents the threshold value for the designated task $t$. Node-specific adversarial learning forces the latent dimension with critical importance to the designated attribute carry “pure” information.

2.3.2. Additional losses

The sensitive attributes, i.e., emotion and identity, can be correlated, the distribution of the scoring vectors from two vanilla FSMs are highly overlapping. Therefore, we design additional constraints to ensure each node is distinctively responsible for a single attribute. We integrate two different losses, attention penalty loss and diversity loss, to guide the attention weights for attribute-alignment. Attention penalty loss is a regularization term that encourages dissimilarity of score vectors between different tasks to prevent redundancy [24]. We define a score matrix $S \in \mathbb{R}^{T \times F}$, where each row of the matrix is a 12-normalized score vector $\hat{s}_t$ corresponding to an attribute $t \in T$. Note that $T$ is the attribute set with $|T|$ attributes, where $|T| = 2$ in this work. Attention penalty loss is defined as:

$$L_{att_t} = \| (SS^T - I) \|_F$$  

(3)

Here $\| \cdot \|_F$ stands for the Frobenius norm of a matrix and $I \in \mathbb{R}^{T \times T}$ is an identity matrix. The element $s_{ij}$ in $SS^T$ is the cosine similarity between $\hat{s}_i$ and $\hat{s}_j$. As the diagonal elements are always equal to 1, we subtract an identity matrix to exclude the diagonal elements in loss calculation. Since non-diagonal elements contribute positive values to the penalty term when the scores are non-orthogonal, through minimization, it encourages dissimilarity between attribute-specific FSM scores.

Diversity loss is another loss used to enhance the intra-class compactness and inter-class separability in the representation space. In this work, we utilize the additive-margin softmax (AM-Softmax) [25], where the classes are the attributes in our case. AM-Softmax imports angular margin into softmax, which forces the model to learn between-class large-margin representations. The diversity loss is derived as:

$$L_{div} = \frac{1}{N|T|} \sum_{t=1}^{N} \sum_{t'=1}^{T} \log \frac{e^{s_t^* W_{ij}^t s_{t'} - m}}{\sum_{j=1, j \neq t}^{T} e^{s_t^* W_{ij}^t s_{t'} - m}}$$  

(4)

where $N$ is the number of samples, $s_t^*$ is the weighted feature vector related to attribute $t$, and $W$ is the last fully connected layer of the model.
Table 1: Privacy-preserving performance presented in WFS (%) and EER (%) for SER and SV respectively, where PP stands for privacy-preserving. Superscript * shows p-value < 0.05, comparing to the proposed method (FS-VAE) in the last row.

<table>
<thead>
<tr>
<th>Method</th>
<th>Origin WFS</th>
<th>PP-SER WFS</th>
<th>PP-SV WFS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wav2vec2.0</td>
<td>56.73</td>
<td>55.81*</td>
<td>55.08*</td>
</tr>
<tr>
<td>A-VAE</td>
<td>-</td>
<td>53.22*</td>
<td>38.44*</td>
</tr>
<tr>
<td>D-VAE</td>
<td>53.89</td>
<td>52.35*</td>
<td>37.85*</td>
</tr>
<tr>
<td>LR-VAE[13]</td>
<td>54.20</td>
<td>53.25*</td>
<td>36.22*</td>
</tr>
<tr>
<td>W-VAE</td>
<td>-</td>
<td>52.46*</td>
<td>40.72*</td>
</tr>
<tr>
<td>FS-VAE</td>
<td>54.33</td>
<td>55.11</td>
<td>36.52</td>
</tr>
</tbody>
</table>

Note that the y-axis of SER curves are WFS, and EER for SV. For LR-VAE, we mask in bottom-up order in PP-SER, and top-down order in PP-SV. For FS-VAE, we mask from the dimension with higher scores.

1 and table 2, where the superscript * indicates a statistically significant difference (p < 0.05).

3.1. Baseline methods

Wav2vec2.0: Apply original wav2vec2.0 embedding for SER and SV model training. Extract the pre-final layer of SER (SV) model for PP-SER (PP-SV) task.


D-VAE: Apply disentangled representation learning, which divides the latent vector into attribute-specific regions. Mask the particular region to achieve privacy protection.

LR-VAE: Proposed method in [13], the most recent SOTA attribute-aligned speech representation learning method.

W-VAE: Apply the weighted latent vector for downstream tasks without attribute-selection (a model variant of FS-VAE).

3.2. Result and analysis

3.2.1. Privacy-preserving performance

Our goal is to protect a particular sensitive attribute while maintaining the main task utility. Comparing to other baselines, our proposed FS-VAE achieves the best performances (PP-SER: 55.11% WFS, 32.48% EER; PP-SV: 16.34% EER, 36.52% WFS) with improved utility and competitive privacy protection. There are a couple observations to note. The first row in table 1 shows that wav2vec2.0 embedding achieves promising results on both tasks of SER and SV, which demonstrates its capability as an informative universal front-end. More interestingly, when we extract the pre-final layer of the SER and SV models to examine the PP-SER and PP-SV results. The results show that the embedding, even when training for a particular attribute recognition, still contain significant information about other sensitive attributes leading the issue of privacy leakage.

Firstly, we compare the performances to the adversarial representation learning, a prevalent method used for privacy protection. The result is shown in the A-VAE row (table 1). For PP-SER, although FS-VAE achieves a little worse identity protection (an increase of 2.92% EER), it better maintains the SER performance (an increase of 1.89% WFS). On the other hand, for PP-SV, FS-VAE outperforms the A-VAE on both SV performance (a drop of 4.36% EER) and emotion protection (an increase of 1.92% WFS). Note that A-VAE requires scenario-
specific encoders, i.e., retraining an encoder for different protection settings, while FS-VAE requires just a single encoder.

Secondly, we compare our proposed FS-VAE with the SOTA attribute-aligned representation learning method, LR-VAE (the LR-VAE row in table 1). For PP-SER, FS-VAE achieves a competitive result. Although FS-VAE performs slightly worse on identity protection (an increase of 2.26% EER), it results in a better emotion recognition performance (an increase of 1.86% WFS). On the other hand, for PP-SV, FS-VAE shows obvious improved results of better utility maintenance (a drop of 1.08% EER) and slightly worse privacy protection results (a drop of 0.30% WFS). FS-VAE has competitive PP-SER results and improved PP-SV performance when compared to LR-VAE. Note that, FS-VAE is more flexible than LR-VAE in the sense that it can be extended to multiple attribute settings by simply adding additional rows in attention penalty loss and more classes in diversity loss.

Lastly, we compare FS-VAE to disentangled representation learning (D-VAE) and weighted vector without attribute selection (W-VAE). The result is shown in the D-VAE and W-VAE row of table 1 respectively. When comparing to the D-VAE, we observe that FS-VAE achieves better utility maintenance (an increase of 2.76% WFS, a drop of 1.90% EER better) and privacy protection (a drop of 1.27% EER, an increase of 2.23% WFS) for both PP-SER and PP-SV. When comparing to the W-VAE, W-VAE achieves comparable privacy protection as our method though FS-VAE obtains better utility maintenance (an increase of 2.65% WFS, a drop of 1.36% EER). These results highlight the importance of attribute alignment and node masking.

3.2.2. Analysis of attribute-alignment strategy
We conduct a masking experiment to study the effectiveness of feature scoring machine (FSM) for attribute alignment. The usage of the two loss functions guides the attribute-alignment and concentrates the task-specific attributes on particular nodes. We compare the results to the layered dropout strategy [13]. The experiment procedure is as follow: first, we encode input features into latent vectors with 128 dimensions, and sort the dimension by the value of score vector; next, we divide the sorted dimension into 16 groups. During masking, for each step, we mask an additional group of nodes with highest scores; then, the masked latent vectors are applied to two tasks: emotion recognition and speaker verification. For example, in the 1st step, 8 latent dimension with highest scores are masked, while the remaining 120 dimension are applied to both SER and SV models. For LR-VAE, we conduct the same analysis but mask the latent vector from one end to the other end, i.e., the emotion-related end or the identity-related end [13].

We observe the identity-protection emotion recognition task in figure 2, the upper PP-SER row. Comparing the emotion recognition curves (WFS), both LR-VAE and FS-VAE maintain high SER performance as the masking progress moves on, while FS-VAE maintains SER performance better at the 15th step, with only one group left (8 dimension). On the other hand, we can see that the speaker verification curve (EER) of FS-VAE has a rapid increase at the beginning (2nd and 3rd step) of the experiment. It shows that the few top-scored identity-related nodes contains a high portion of speaker identity information with little emotion-related information.

Further, we study the emotion-protection speaker verification task in figure 2, the lower PP-SV row. For the EER curves, the downward trend of FS-VAE is smoother than LR-VAE (utility maintenance). We also observe that LR-VAE experiences an early significant performance drop (12th and 13th step), while

### Table 2: Ablation study results. Privacy-preserving performance presented in WFS (%) and EER (%) for SER and SV respectively. Note that * means to include the corresponding component, while – means to exclude the component. Superscript * shows p-value < 0.05, comparing to proposed method.

<table>
<thead>
<tr>
<th>Components</th>
<th>PP-SER</th>
<th>PP-SV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Att-Loss</td>
<td>WFS</td>
<td>EER</td>
</tr>
<tr>
<td>Div-Loss</td>
<td>−</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>−</td>
<td>52.33*</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>55.11</td>
</tr>
</tbody>
</table>

FS-VAE has a more gentle downward slope. For WFS curves (privacy protection), we see a rapid performance drop at the first few steps (2nd step) of the experiment indicating that by masking just a few nodes, the emotion-related information in the remaining representation has also effectively been deleted.

3.2.3. Ablation study
We perform ablation study to investigate the effectiveness of the two loss terms, attention penalty and diversity loss. We re-train the FS-VAE with different combinations of these two loss, and apply the latent code for two privacy-preserving scenarios, PP-SER and PP-SV. The results are shown in table 2.

Firstly, we study the baseline case, i.e., training without the two penalty terms. The poor utility maintenance (40.01% WFS, 37.06% EER) shows that without explicit constraints, the two attributes are highly overlapping on similar set of nodes resulting in poor performances. Next, we study the case when applying attention penalty loss only, which is designed to make the attribute-specific scores distinct. The improved utility maintenance (14.14% WFS better, 20.56% EER better) demonstrates that the inclusion of attention penalty loss is key in the alignment. On the other hand, we study the case of applying diversity loss, which enhances the inter-task separability and intra-class compactness in the weighted vectors. The result shows that using diversity loss only loosely encourage the task-specific attributes to distribute on different dimensions, but the constraint is not strong enough as compared to attention penalty loss. Lastly, we observe the case when applying both loss functions where it achieves the best privacy-preserving performance (PP-SER: 55.11% WFS, 32.48% EER; PP-SV: 16.34% EER, 36.52% WFS); the diversity loss, while not enough by itself, can act as an auxiliary term that improve the overall performances.

4. Conclusions
In this work, we propose an attention-based attribute aligned representation learning strategy to achieve flexible speech representation for privacy protection. Comparing to previous methods, it better maintains the utility and achieves competitive performance on PP-SER and improves performance on PP-SV. We also show that the two losses separates task-specific attributes and guides the alignment learning process without explicitly defining dropout functions. These losses enable scoring machines to measure the attribute-specific importance of each dimension and naturally provides a flexible mechanism to select and protect target sensitive attributes. In the future, since our proposed method is extendable to operate in multiple attributes setting, we will immediately evaluate on a proper database with multiple attributes. Moreover, we will generalize our approach from using an aggregated feature vector to time series modeling, and further explore multimodality, such as speech and language, for learning speech representation.
5. References


