Analyzing Language-Independent Speaker Anonymization Framework under Unseen Conditions

Xiaoxiao Miao¹, Xin Wang¹, Erica Cooper¹, Junichi Yamagishi¹, Natalia Tomashenko²

¹National Institute of Informatics, Japan ²LIA, University of Aix-Marseille, France
xiaoxiaomiao@nii.ac.jp

Abstract

In our previous work, we proposed a language-independent speaker anonymization system based on self-supervised learning models. Although the system can anonymize speech data of any language, the anonymization was imperfect, and the speech content of the anonymized speech was distorted. This limitation is more severe when the input speech is from a domain unseen in the training data. This study analyzed the bottleneck of the anonymization system under unseen conditions. It was found that the domain (e.g., language and channel) mismatch between the training and test data affected the neural waveform vocoder and anonymized speaker vectors, which limited the performance of the whole system. Increasing the training data diversity for the vocoder was found to be helpful to reduce its implicit language and channel dependency. Furthermore, a simple correlation-alignment-based domain adaptation strategy was found to be significantly effective to alleviate the mismatch on the anonymized speaker vectors. Audio samples¹ and source code² are available online.

Index Terms: speaker anonymization, self-supervised learning, CORrelation ALignment, multilingual HiFi-GAN.

1. Introduction

The human voice contains a wealth of personal information, such as the speaker’s identity and emotion. Since personal information can be revealed by advanced speaker or other types of recognition systems, the demand for privacy-preserving technologies is growing. Although there is no legal definition of privacy [1], through the initiative called VoicePrivacy Challenge (VPC) 2020 [2, 3], the research community has defined a speaker anonymization task, the goal of which is to protect the speaker identity information (privacy) while maintaining the speech intelligibility and naturalness (utility).

While other related methods exist [4], a recently proposed deep neural network (DNN)-based [5] method was used as the VPC 2020 primary baseline to disentangle speaker and other information in the speech data and synthesize speech after anonymizing the speaker information. The effectiveness of this speaker anonymization system (SAS) has been confirmed on English test sets. However, it requires large amounts of text transcriptions for English training data to obtain accurate linguistic representations, which makes it impossible to use for an unknown language. While other digital-signal-processing-based methods [6] require little or no training data, they are less effective than the DNN-based methods at protecting the speaker identity [7, 3].

Aiming at an effective speaker anonymization solution that can be applied to the speech of any language, we have proposed a self-supervised learning (SSL)-based language-independent SAS [8]. It uses an SSL-based content encoder to extract general context representations regardless of the language of the input speech. The whole SAS requires no text labels or other language-specific resources, allowing the system to anonymize speech data from any language. This SAS has been applied to Mandarin speech data. Even though the Mandarin language was completely unseen to the SAS, the Mandarin speech samples were anonymized reasonably well. However, it was also observed from an increased character error rate (CER) that the speech contents were distorted after anonymization. While the trade-off between speaker anonymization and speech intelligibility is common to many SASs [3], our goal is to push the limit of the language-independent SAS and improve both privacy and utility metrics in unseen conditions.

This study takes one step towards our goal by experimentally analyzing the performance bottleneck of the SAS. Specifically, it analyzes how the components such as the speech generator (i.e., vocoder) are implicitly dependent on a particular language or channel in the training database of that language. While keeping the target language (i.e., Mandarin) unseen, this study finds it beneficial to increase the language diversity of the training data, for example by adding German, Italian and Spanish speech data. Furthermore, this study investigates the language/channel mismatch brought by the impure speaker identity representation. It is found that the mismatch can be alleviated by transforming the anonymized speaker vector using a simple CORrelation ALignment (CORAL)-based domain adaptation strategy [9]. Transferring the anonymized speaker vector from the source domain (English) to a general domain covering German, Italian and Spanish data achieves better performance. When transforming to a more ideally matched domain with a few samples of Mandarin data, the CORAL provides the best utility with remaining high privacy. These findings are expected to be useful to the community for building a better language-independent SAS that can work under unseen conditions.

2. SSL-based Language-Independent Speaker Anonymization System

The baseline SSL-based language-independent SAS [8] disentangles speech into the fundamental frequency (F0), speaker identity representation, and content representation. Figure 1 shows the training and anonymization procedure of the baseline system (black and blue arrows path), respectively. There are two steps in the training stage:

1) Original F0, speaker identity, and context feature extraction from the original speech recordings. The YAAP algorithm [10] is used to extract F0. The emphasized channel attention, propagation and aggregation in a time delay neural network (ECAPA-TDNN) speaker encoder trained on the VoxCeleb-1 & 2 [11, 12] datasets is used to extract 192-dimensional speaker

¹https://xiaoxiaomiao39.github.io/IS2022-SAS/
²https://github.com/xiaoxiaomiao39/SSL-SAS
identity vectors. To extract finer-grained context representations, the HuBERT-based soft content encoder [13] downsamples the input speech into a sequence of 768-dimensional continuous representations, which is reduced to 200 dimensions through linear projection. Note that this HuBERT-based soft content encoder took the CNN encoder and the sixth transformer layer from the input of a HuBERT base model [14] pre-trained on LibriSpeech \footnote{https://github.com/pytorch/fairseq/tree/main/examples/hubert} as the backbone. It was fine-tuned on the LibriTTS-train-clean-100 [15] dataset, and the training criterion is detailed in [8].

2) Speech synthesis. The frame-wise content features, F0, and utterance-level source speaker vector are passed to the HiFi-GAN neural vocoder [16] after the operation of upsampling and concatenation to synthesize speech. The HiFi-GAN model was trained on LibriTTS-train-clean-100 [15], denoted as monolingual HiFi-GAN.

An extra step called Speaker vector anonymization is included in the anonymization stage [2, 3]. Given a source speaker vector, cosine distance is used to find the 200 farthest speaker vectors from an external speaker vector pool (LibriTTS train-other-500). From these 200 vectors, 100 vectors are randomly selected and their average is used as the anonymized speaker vector [17]. Then, the content features, F0 and anonymized speaker vector instead of the source speaker vector are used to generate the anonymized speech.

3. Analysis of Performance Bottleneck

Although the above SAS performed reasonably well on the unseen Mandarin data, the anonymization performance was below the theoretical optimum. Furthermore, the contents of the anonymized speech were distorted by the SAS. It was shown that the CER of the anonymized speech reached 18.92%, which was much higher than the CER of 10.36% on the original data. Also, when the output speech was produced without actually anonymizing the speaker vector (i.e., resynthesis), its CER was still 14.81%. However, resynthesized speech from an ideal SAS should obtain a similar CER to the original speech.

The above results motivated us to analyze the performance bottleneck of our SAS under unseen circumstances. Here we examine the components in the system one by one and present techniques to alleviate the bottlenecks. Although we only consider Mandarin speech as the unseen test data, the analyses are expected to apply to other unseen languages as well.

3.1. Robustness of HiFi-GAN

The CER gap between the original (10.36%) and resynthesized speech data (14.81%) suggests that the speech contents in the resynthesized speech may have been distorted. A similar finding has been reported on the language-dependent VPC baseline [18]. Since the system extracted features and re-synthesized the speech waveform without anonymizing the speaker representations, the increased CER is only caused by the content feature extractor and vocoder.

We hypothesize that the HiFi-GAN vocoder is one bottleneck\footnote{We also investigated a multilingual-trained SSL-based soft content encoder but no improvements were observed.}. It is known that to build a neural vocoder that generalizes well to unseen speakers in unseen languages, the training dataset has to cover diverse speakers and languages [19]. However, the HiFi-GAN in our SAS was trained using a subset from LibriTTS with many speakers, but only English-speaking ones. To verify the hypothesis, we used a multilingual database [20] to train the HiFi-GAN and compared its performance with the HiFi-GAN trained on the monolingual LibriTTS data in the experiments. This comparison is illustrated in Figure 1(a). Note that the multilingual database does not contain Mandarin data, and its details are explained in Section 4.2.

3.2. Language and Channel Mismatch on Speaker Vectors

Comparing the CERs in the resynthesized (14.81%) and anonymized (18.92%) cases, the increased CER is likely due to the anonymized speaker vector since it is the only difference between the resynthesized and anonymized data. Many studies have shown that speaker vectors contain speaker-unrelated information from the source domain, e.g., channel conditions and lexical contents [21, 22]. Because the anonymized vector is composed from the pool of English speaker vectors (i.e., those from LibriTTS train-other-500 [15]), it may carry irrelevant information pertinent to the English database. Therefore, directly using the anonymized vector on Mandarin data may introduce language, channel, or other types of domain mismatch.

To verify this hypothesis, we use a simple but effective unsupervised domain adaption technique called CORAL [9]. The goal of CORAL is to find a transfer matrix $A$ that can align the feature distributions of the source domain and target domain by minimizing their covariances. Suppose source-domain English speaker vectors $D_s = \{n_i\}, n_i \in \mathbb{R}^{192}$, and the target speaker vectors $D_T = \{m_i\}, m_i \in \mathbb{R}^{192}$, here $n_i$ and $m_i$ are the 192-dimensional vectors extracted from the last projection layer of the ECAPA-TDN. After the feature normalization,

Figure 1: Diagram of language-independent SAS. Blue and red arrows indicate components investigated in this study.
tion where the speaker vectors $D_S$ and $D_T$ are normalized to have zero mean and unit standard deviation in each dimension, the relationship of source- and target-domain statistics is that mean $\mu_S = \mu_T = 0$ and covariance matrices $C_S \neq C_T$. The transfer matrix $A$ can be obtained via:

$$\text{CORAL}(D_S, D_T) = \min_A \| A^T C_S A - C_T \|^2_F$$

where $\| \cdot \|^2_F$ represents the matrix Frobenius norm. The detailed procedure to compute the optimal $A^\star$ can be found in [9, 23]. Then, the anonymized English speaker vectors transformed by $A^\star$ are used as the new anonymized speaker vectors.

We consider two cases of CORAL transformations based on the data availability:

**General CORAL transformation**: we assume that Mandarin data are unavailable, and the target-domain speaker vectors are collected from the German, Italian, and Spanish speech data; 

**Mandarin CORAL transformation**: we assume that a few (no more than 100) Mandarin samples that are completely disjoint (unseen-unheard speakers) with the test set are available as the target-domain speaker vectors.

In the first case, where the domain of the test data to be anonymized remains unseen to the SAS, CORAL using the target speaker vectors from multiple languages and channels is expected to alleviate the mismatch between the English vector pool and the vector to be anonymized. The second case is an oracle scenario where the mismatch caused by the impure speaker vectors can be reduced to a greater extent when they are transferred to the matched domain.

Figure 2 plots the t-SNE visualization of speaker vectors before and after the two cases of CORAL transformations. These speaker vectors are sampled from the different datasets listed at the bottom of Table 1. It is observed that the original distributions of speaker vectors from the different domains are widely spread due to the language and channel mismatch. The distribution between English and general domains has more overlap than between the English and Mandarin domains. Despite the different degrees of overlap, CORAL transformations push the speaker vectors from different domains to move closer.

### 4.2. Databases

In addition to the standard databases to build the SAS (Section 2), this study used external data listed in Table 1 for the SAS training and CORAL transformation. The multilingual dataset for HiFi-GAN consists of LibriTTS-train-clean-100 and subsets that contains German, Italian, and Spanish data sampled from the Multilingual LibriSpeech corpus [20]. Around 78 hours of clean data were selected for each language. The selection criteria is that the duration of each recording is larger than 10s, and that the signal-to-noise ratio is equal to 100, which is estimated using the WADA SNR algorithm [24].

The Mandarin test trials and enrollment data were sampled from the test set of Mandarin speech corpus AISHELL-3 [25]. Specifically, 4,179 trials from 44 speakers were randomly sampled as the test trials, and additional 2 utterances of the same speaker were sampled for enrollment. They composed 10,120 enrollment-test pairs for the ASV evaluation, which is denoted as AISHELL-3-test-veri. The target-domain vectors for the oracle Mandarin CORAL were extracted from the left data of AISHELL-3 test set, denoted AISHELL-3-test-left in Table 1. Note that there is no speaker or utterance overlap between AISHELL-3-test-left and AISHELL-3-test-veri. The target-domain vectors for the general CORAL were randomly selected from the German, Italian, and Spanish subsets. The source-domain vectors for both types of CORAL were randomly selected from the LibriTTS-train-clean-100. Similar to [8], the $ASV_{eval}$ model was an ECAPA-TDNN trained on the Mandarin CN-Celeb-1 & 2 [26, 27] datasets. The $ASR_{eval}$ model was an open-source ASR Transformer [28] trained on the Mandarin AISHELL-1 ASR dataset [29].
4.3. Results and analysis

Our experiments compared the SAS performance on the Mandarin test data by varying the two factors illustrated in Figure 1(b): using monolingual or multilingual data to train the HiFi-GAN vocoder, and whether CORAL was applied on the anonymized speaker vector. The EERs from different setups are plotted in Figure 3. The CERs are plotted in Figure 4. Note that, when CORAL was used, we also analyzed the impact of using different amounts of data to estimate the CORAL transformation matrix. The label “w/CORAL-100” in the figures indicates using \( N \) randomly-chosen speaker vectors from the source and target domain respectively. All the results for CORAL transformation are computed over 5 runs of speaker vector selection.

Monolingual vs. Multilingual HiFi-GAN: In the Resynthesizer setup, the SAS using monolingual training data for HiFi-GAN achieved a CER of 13.63\%, which is lower than 14.81\% when using monolingual data. Meanwhile, the EERs in both cases are equal to 9.13\%. When anonymization was conducted, the SASs using monolingual HiFi-GAN achieved lower CERs than their counterparts using monolingual HiFi-GAN in most of the setups except when no CORAL was used (w/o CORAL, 19.02\% > 18.92\%). Specifically, when the Mandarin CORAL was used, the multilingual HiFi-GAN outperformed the monolingual case in terms of CER, no matter how much data was used to estimate the CORAL matrix.

These results indicate that the multilingual data is helpful to obtain a robust HiFi-GAN to preserve the speech contents better. The improvement is expected to be larger when the domain mismatch on the anonymized speaker vectors is reduced using CORAL. The EERs were roughly similar no matter which HiFi-GAN was used. Therefore, the benefit of using the multilingual HiFi-GAN is mainly on the better preservation of the speech contents, rather than better protection of the speaker identity.

CORAL: Compared to “w/o CORAL”, all the EERs on the Ignorant condition of “w/CORAL-4\(N\)” were successfully increased regardless of the choice of HiFi-GAN training data, CORAL types, and amount of data for CORAL matrix estimation. Similarly, the CERs were significantly decreased after applying CORAL. These results suggest that the mismatch from the anonymized speaker vectors severely affected the SAS, and CORAL is effective to reduce various types of mismatches (e.g., language and channel) between different datasets/domains.

For the different configurations for CORAL, we first observed that the oracle Mandarin CORAL performed better on CERs than the general CORAL. However, their differences on EERs are not obvious. This indicates that the SAS performance on speech content preservation is more sensitive to the mismatch of anonymized vectors than the CORAL configurations. For speaker identity protection, using the general CORAL is sufficient. Interestingly, unlike DNN-based methods, using larger \( N \) to estimate the CORAL matrix did not constantly improve the results. Using 20 samples (w/CORAL-20) generally performed well in terms of EER and CER. The reason is that users and attackers randomly choose speaker vectors from the target domain individually to approximate CORAL transformation matrices. These matrices can be very different if the number of the speaker vectors \( N \) is relatively small, which increases the randomness of the new anonymized speaker vectors used by the users and attackers. Therefore, speaker identity information can be protected better.

Considering that the users may prefer to choose smaller \( N \) to protect their privacy, while an attacker may be interested to use larger \( N \) to find a more precise CORAL transform matrix on the Lazy-informed condition, we then set \( N = 10 \) for users and \( N = 100 \) for attackers to compute the CORAL matrix independently, denoted CORAL-10-100. The results from Table 2 show that the EERs of CORAL-10-100 are lower than those of CORAL-10 for both general and Mandarin cases in an acceptable level. Furthermore, “General CORAL-100-10” still performs better than “w/o CORAL”.

5. Conclusions

This paper analyzed the previously proposed SSL-based SAS under unseen conditions. Two hypotheses, which are that the performance bottleneck exists in the HiFi-GAN and in anonymized speaker vectors, were presented and experimentally verified. The results indicate that increasing the language diversity for the HiFi-GAN benefits the preservation of speech contents. The mismatch on the anonymized speaker vectors severely affect the SAS. The SAS using multilingual HiFi-GAN and CORAL strategy easily outperforms the previous SAS using monolingual HiFi-GAN on both privacy and utility.

Acknowledgements This study is supported by JST CREST Grants (JPMJCR18A6 and JPMJCR20D3), MEXT KAKENHI Grants (21K17775, 21H04906, 21K11951, 18H04112), and the VoicePersonal project (ANR-18-JSTS-0001).
6. References


