X-Vector Singular Value Modification and Statistical-Based Decomposition with Ensemble Regression Modeling for Speaker Anonymization System

Candy Olivia Mawalim\textsuperscript{1}, Kasorn Galajit\textsuperscript{1,2}, Jessada Karnjana\textsuperscript{2}, Masashi Unoki\textsuperscript{1}

\textsuperscript{1} Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi, Ishikawa 923–1292 Japan
\textsuperscript{2} NECTEC, National Science and Technology Development Agency, Puthum Thani, Thailand
candyolivia@jaist.ac.jp, kasorn@jaist.ac.jp, unoki@jaist.ac.jp, jessada.karnjana@nectec.or.th

Abstract

Anonymizing speaker individuality is crucial for ensuring voice privacy protection. In this paper, we propose a speaker individuality anonymization system that uses singular value modification and statistical-based decomposition on an x-vector with ensemble regression modeling. An anonymization system requires speaker-to-speaker correspondence (each speaker corresponds to a pseudo-speaker), which may be possible by modifying significant x-vector elements. The significant elements were determined by singular value decomposition and variant analysis. Subsequently, the anonymization process was performed by an ensemble regression model trained using x-vector pools with clustering-based pseudo-targets. The results demonstrated that our proposed anonymization system effectively improves objective verifiability, especially in anonymized trials and anonymized enrollments setting, by preserving similar intelligibility scores with the baseline system introduced in the VoicePrivacy 2020 Challenge.

Index Terms: speaker anonymization, x-vector, singular value modification, statistical-based decomposition, ensemble regression modeling

1. Introduction

As speech is generally preferred over text communication, voice-input features have become widely implemented in recent technology. However, voice recordings can contain personal, sensitive information, which may lead to security and privacy risks when exposed [1]. Such risks are due to advancements in speech synthesis and conversion technology that have enabled increasingly accurate voice cloning even with limited speech samples [2, 3]. Consequently, there have been growing efforts to preserve voice security and privacy, one of the main proposed approaches being speaker anonymization.

Speaker anonymization or de-identification is a method for suppressing or concealing speaker identity in their speech data [4]. According to the VoicePrivacy 2020 Challenge [5], the following four requirements are important for a speaker anonymization system: (i) the speaker identity must be hidden, (ii) the output speech should be natural and intelligible, (iii) the language information should be preserved, and (iv) a speaker-to-speaker correspondence must be followed.

Several methods have been proposed for anonymization systems [1, 4, 6, 7, 8]. Previously, an anonymization system was developed by suppressing speaker identity using a voice transformation system [6, 7]. For instance, a diphone-based syntactic source speech (kaldiphone) is transformed to fit a set of speakers to attack the speaker identification system. It was suggested that this voice transformation could influence the Gaussian mixture model (GMM) based speaker identification system [6]. Subsequently, a voice transformation method to de-identify speech using GMM mapping and harmonic-stochastic models was proposed [8]. De-identification of online speakers was feasible with this method. Next, a technique for concealing speaker identity through voice transformation was developed using the natural speech of a target person instead of a synthetic voice [9]. Another approach was implemented using cepstral frequency warping plus amplitude scaling to transform speech and hide the identity [10].

Fang et al. [4] proposed a method based on a neuro source-filter (NSF) model to separate the speaker identity and the linguistic content from the input speech before resynthesizing the speech data with modification of speaker identity information (x-vector). This method is referred to as the first baseline system in the VoicePrivacy 2020 Challenge [5]. The x-vector was chosen since it could effectively encode speaker identity as a feature in speaker verification system [11]. In the first baseline system, the original x-vector was replaced with the mean x-vector from the farthest x-vector group in the anonymization x-vector pool. On the other hand, our proposed method offers two different approaches for anonymizing speaker identity information (x-vector): (1) modifying its singular value, and (2) decomposition based on the x-vectors’ statistical properties and transforming it with ensemble regression models. We predicted that by modifying the significant elements of x-vectors, the speaker-to-speaker correspondence requirement of anonymization system could be satisfied. Furthermore, we investigated the performance of the synthesis system to improve the quality of anonymized speech.

The rest of this paper is organized as follows. Section 2 describes the proposed anonymization system in detail. Section 3 presents the experimental setup and results of the proposed method. Finally, Section 4 presents the conclusion and future work.

2. Proposed Model

Figure 1 shows our proposed model for a speaker anonymization system. The analysis and synthesis framework from input speech to anonymized system using an x-vector and a neural-source filter (NSF) model were based on the first baseline system in Voice Privacy 2020 Challenge [4, 5, 12]. Four pre-trained models were employed in the baseline system, including an ASR acoustic model [4, 13] for extracting linguistic-related features or bottleneck (BN) features, an x-vector extractor [11] trained by VoxCeleb datasets [14, 15], a speech synthesis acoustic model [4], and an NSF [16] for generating a speech signal with F0, Mel-filterbank, and an anonymized x-vector as input. We modified the baseline model by replacing the F0 extractor with the one provided by another speech analysis toolkit. The experiment by Morise et al. demonstrated that WORLD
where the least similar centroid using a clustering method.

vector. The pseudo target x-vector was determined from the vector pool to obtain the input x-vector and pseudo target x-vector. The decomposition is expressed as:

$$X = U\Sigma V^T,$$  \hspace{1cm} (1)

where U and V are the orthonormal eigenvectors of $XX^T$ and of $X^TX$, respectively, and $\Sigma$ consists of the square roots of the eigenvalues of $X^TX$.

In our approach, we interpreted $U$ as the utterance-to-concept similarity matrix, and $V$ as the x-vector-to-concept similarity matrix. $\Sigma$ represents the strength of each concept involved. By reducing the dimension of $\Sigma$, we expect to obtain more general constituent elements of the x-vector. Thus, x-vector anonymization is conducted by controlling $\Sigma$ with a threshold parameter (singular value threshold). Figure 3 shows the anonymization of an x-vector singular value.

**X-vector Reconstruction.** Lastly, the anonymized x-vector of a speaker’s utterance was obtained from the anonymized x-vector matrix reconstructed from $U$, $V$, and the modified $\Sigma$.

### 2.2. Statistical-Based Regression Modelling

Figure 4 shows the second approach of our anonymization system, which comprises the following four steps:

**X-vector Variant-based Decomposition.** First, the variant of intraspeaker x-vectors in x-vector pool 1 was analyzed to observe the distribution of the x-vector of a speaker in different utterances. The standard deviation of the intraspeaker x-vectors were calculated with a given threshold to decompose the x-vector into two parts, i.e., high-variant x-vector ($y_h$) and low-variant x-vector ($y_l$). This decomposition is based on our hypothesis that the low-variant x-vector is a stable part of the x-vector that contains the uniqueness of the speaker identity; therefore, it is an important cue for one-to-one mapping from the original to anonymized speech.

**Anonymization Pool Construction.** After the x-vector was decomposed into high and low-variant parts, we built clustering models to create pseudo-target x-vectors. The clustering model was trained using x-vector pool 2. The clustering model produced several centroids which are assigned as the candidates of the pseudo-target x-vectors. The pseudo-target x-vector was determined by the centroid least similar to the pseudo-input x-vector. The pseudo-target x-vectors were fit into a regression model in two consecutive processes, and then pairs of pseudo input-target x-vectors were fit into the regression model. In other words, we defined the x-vectors pairs as our anonymization pool.

**Ensemble Learning for Regression Modeling.** Two ensemble regression models were constructed by fitting the anonymization pool x-vectors. A non-linear regression model was trained for the high-variant x-vector, and a linear regression model was trained for the low-variant x-vector. We predicted that by transforming the low-variant x-vector linearly, the uniqueness of each speaker’s x-vector could be preserved. In other words, we fit a linear function ($z_i^* = Ax_i + B$) for transforming the original low-variant x-vector ($z_i$) to the anonymized
3. Experiments

3.1. Datasets

All datasets utilized in the experiments were based on the VoicePrivacy 2020 Challenge [12]. Table 1 shows the training data used as our x-vector pools. In the variant analysis, we randomly selected subsets of LibriTTS train-other-500 and train-clean-100 [21] with 30 utterances from each speaker (with 30 total speakers per dataset). The full set of x-vectors extracted from train-other-500 was then utilized in the singular value (SV) pool and pool-2. In x-vector pool-2, we also utilized the full set of train-clean-100. We fit our regression models with 95% of the total data and the remaining 5% was used to evaluate our models by $R^2$ score and root-mean squared error (RMSE). The development and test sets of LibriSpeech (Libri) [22] and VCTK [23] were utilized to evaluate speaker verifiability (ASVeval) and intelligibility (ASReval).

Table 2: Comparison of F0 extractors in terms of intelligibility assessment

<table>
<thead>
<tr>
<th>Subset</th>
<th>Data</th>
<th>Yaapt</th>
<th>DIO</th>
<th>Harvest</th>
<th>RAPT</th>
<th>SWIPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Libri (dev)</td>
<td>ori</td>
<td>3.83</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
</tr>
<tr>
<td></td>
<td>resyn</td>
<td>6.5</td>
<td>6.7</td>
<td>6.52</td>
<td>6.59</td>
<td>6.41</td>
</tr>
</tbody>
</table>

3.2. Experimental Setup

The main part of our experiment was conducted using the Kaldi toolkit [24]. WORLD and Speech Processing Toolkit (SPTK) were used to extract F0. We investigated four different F0 estimation algorithms, i.e., DIO and Harvest from WORLD, and RAPT and SWIPE from SPTK. In addition, we used Scikit-learn [25] to construct the machine learning model for our anonymization system.

To generate the anonymization x-vector pool, we employed a Gaussian mixture model as our clustering model. We investigated the variation in the number of clusters and the measured x-vector similarity (cosine distance or probabilistic linear discriminant analysis (PLDA)) to build the anonymization pool as the input for the regression model. Consequently, we built gender-dependent regression models that mapped the high-variant and low-variant parts (as in second approach) of the x-vector. The RandomForest algorithm was used as the regression models for the high-variant x-vector. RandomForest uses ensemble learning and can produce a highly accurate model and control over-fitting even when the amount of data is large [25]. In our experiment, we tuned the RandomForest regressor parameters, i.e., the number of estimators ($n_{	ext{est}}$) and maximum depths ($\text{max depth}$).

Our final model used $n_{\text{est}} = 10$ and the default $\text{max depth}$ from scikit-learn since it performed optimally in our evaluation (in predicting 5% of the training data). For the low-variant x-vector, we investigated several pairs of constants $A$ and $B$ for each gender obtained from the parameter variation used while constructing the anonymization pool.

3.3. Results

We evaluated each component of our proposed model by conducting an ablation test. Table 2 shows the evaluation of the resynthesis process using NSF with several F0 estimators (Kaldi (Yaapt), WORLD (DIO and Harvest), and SPTK (RAPT and SWIPE)). The intelligibility assessment (ASReval) was con-
Table 3: Ablation test on proposed model in terms of objective speaker verifiability. The anonymization system was built using a RandomForest regressor which trained by anonymization pool with GMM clustering with 200 centroids and PLDA scoring. For anonymization model 1, the singular value threshold was between 10% to 20%. The F0 was extracted by the SWIPE algorithm in SPTK. Since the results of model 2 were more optimal than model 1, only the combination of F0 modification with model 1 is reported in this table. Gen stands for gender (F: female and M: male).

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Gen</th>
<th>Anonymization</th>
<th>Anon. Model 1</th>
<th>Anon. Model 2</th>
<th>F0 + Anon. Model 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>F0 (Resynthesis)</td>
<td>F ori an</td>
<td>42.95</td>
<td>8.87</td>
<td>147.21</td>
<td>50.99</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>0.80</td>
<td>1.13</td>
<td>14.25</td>
<td>14.25</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>21.81</td>
<td>0.04</td>
<td>147.31</td>
<td>55.90</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>0.04</td>
<td>14.28</td>
<td>1.24</td>
<td>1.24</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>24.84</td>
<td>0.72</td>
<td>115.02</td>
<td>56.37</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>20.44</td>
<td>0.00</td>
<td>8.54</td>
<td>28.88</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>0.04</td>
<td>14.28</td>
<td>1.24</td>
<td>1.24</td>
</tr>
<tr>
<td>F0 (Resynthesis)</td>
<td>F ori an</td>
<td>7.66</td>
<td>0.18</td>
<td>26.30</td>
<td>7.66</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>0.69</td>
<td>118.50</td>
<td>2.07</td>
<td>2.07</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>21.81</td>
<td>0.04</td>
<td>147.31</td>
<td>55.90</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>0.04</td>
<td>14.28</td>
<td>1.24</td>
<td>1.24</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>24.84</td>
<td>0.72</td>
<td>115.02</td>
<td>56.37</td>
</tr>
<tr>
<td></td>
<td>M anon an</td>
<td>20.44</td>
<td>0.00</td>
<td>8.54</td>
<td>28.88</td>
</tr>
</tbody>
</table>

Table 4: Speaker intelligibility attained by the pretrained ASReval model.

<table>
<thead>
<tr>
<th>Subset</th>
<th>Data</th>
<th>WER (%)</th>
<th>F0</th>
<th>Anon.</th>
<th>Anon.</th>
<th>F0+Anon.</th>
<th>F0+Anon.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCTK (dev)</td>
<td>ori</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
</tr>
<tr>
<td></td>
<td>anon</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
</tr>
<tr>
<td>VCTK (test)</td>
<td>ori</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
</tr>
<tr>
<td></td>
<td>anon</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
<td>3.82</td>
</tr>
</tbody>
</table>

We proposed two x-vector anonymization approaches: singular value modification and statistical-based decomposition with regression models. The main concept was that one-to-one mapping from input speech to anonymized speech could be obtained by modifying the significant elements of the x-vector. The evaluation results demonstrated that our proposed anonymization system was effective in increasing the anonymization rate (ASReval) compared with resynthesis only. We intend to increase the amount of training data and study state-of-the-art regression models for anonymizing x-vector to improve our system. We will also investigate how to construct an analysis-synthesis system that better suits the anonymization process.

4. Conclusion and Future Work

We proposed two x-vector anonymization approaches: singular value modification and statistical-based decomposition with regression models. The main concept was that one-to-one mapping from input speech to anonymized speech could be obtained by modifying the significant elements of the x-vector. The evaluation results demonstrated that our proposed anonymization system was effective in increasing the anonymization rate (ASReval) compared with resynthesis only. We intend to increase the amount of training data and study state-of-the-art regression models for anonymizing x-vector to improve our system. We will also investigate how to construct an analysis-synthesis system that better suits the anonymization process.

5. Acknowledgements

This work was supported by a Grant-in-Aid for Scientific Research (B) (No. 17H01761) and JSPS KAKENHI Grant (No. 20H20580).
6. References


