The VoicePrivacy 2020 Challenge

Post-evaluation analysis

Presenter: Natalia Tomashenko

Natalia Tomashenko 1
Brij M.L. Srivastava 2
Xin Wang 3
Emmanuel Vincent 2
Andreas Nautsch 4
Junichi Yamagishi 3,5
Nicholas Evans 4
Jose Patino 4
Jean-François Bonastre 1
Paul-Gauthier Noé 1
Massimiliano Todisco 4
Mohamed Maouche 2
Benjamin O’Brien 6
Anais Chanclu 1

1 LIA – University of Avignon – France
2 Inria – France
3 NII – Tokyo – Japan
4 Audio Security and Privacy Group, EURECOM – France
5 University of Edinburgh – UK
6 Aix-Marseille University – France
Laboratoire Parole et Langage (LPL) – France

4th November 2020
Investigate the anonymized data collection:

• Training more advanced attack models
• Downstream tasks, i.e. ASR training
Introduction: aim

Investigate the anonymized data collection:

- Training more advanced attack models
- Downstream tasks, i.e. ASR training

Objective evaluation:
automatic speaker verification (ASV\textsubscript{eval})

Objective evaluation:
automatic speech recognition (ASR\textsubscript{eval})
Objective evaluation: automatic speaker verification ($\text{ASV}_{\text{eval}}$)

Test trials

• 1
  original

• 2
  Anonymization
  anonymized
  Pseudo-speaker

• 3
  Anonymization
  anonymized
  Pseudo-speaker 1

Enrollment

$\text{ASV}_{\text{eval}}$

Privacy metrics
$\text{EER}, \text{C}_{\text{ltr}}, \text{C}_{\text{itr}}$

Anonymization
anonymized
Pseudo-speaker 2
Objective evaluation: automatic speaker verification (ASV_{eval})

Trained on anonymized data
Objective evaluation: automatic speech recognition (ASR\textsubscript{eval})

Test trials

- 1
  - original
  - ASR\textsubscript{eval}

- 2
  - Anonymization
  - anonymized
  - ASR\textsubscript{eval}

Utility metrics
- WER
- WER
Objective evaluation: automatic speech recognition ($\text{ASR}_{\text{eval}}$)

Test trials

- 1. Original
- 2. Anonymization

Utility metrics
- WER

Trained on anonymized data

VoicePrivacy
Post-evaluation analysis

Using anonymized speech data to train $\text{ASV}_{\text{eval}}$

More advanced attack model

Training $\text{ASV}_{\text{eval}}^{\text{anon}}$ on anonymized data rather than original data leads to significant EER reduction for all systems in the case when the enrollment and trial data are anonymized.
Post-evaluation analysis

Using anonymized speech data to train $\text{ASR}_{\text{eval}}$

Efficient ASR training
Training $\text{ASR}_{\text{eval}}^{\text{anon}}$ on anonymized data significantly decreases WER
Post-evaluation analysis

Using anonymized speech data to train $\text{ASR}_{\text{eval}}$
Voice similarity matrices: LibriSpeech-test-male

Using **original** speech data to train $\text{ASV}_{\text{eval}}$

Using **anonymized** speech data to train $\text{ASV}_{\text{eval}}^{\text{anon}}$

[Noe 2020]
Voice similarity matrices: LibriSpeech-test-male

Using **original** speech data to train ASV\textsubscript{eval}

Using **anonymized** speech data to train ASV\textsubscript{eval}\textsuperscript{anon}
Voice similarity matrices: VCTK-test-male

Using **original** speech data to train $\text{ASV}_{\text{eval}}$

Using **anonymized** speech data to train $\text{ASV}^{\text{anon}}_{\text{eval}}$
Conclusions

• A strong attack model can be developed when an attacker has access to anonymized speech data

• Anonymized data can be successfully used in training ASR systems
References **VoicePrivacy challenge**

- VoicePrivacy site: [https://www.voiceprivacychallenge.org/](https://www.voiceprivacychallenge.org/)

- [Tomashenko 2020] Introducing the VoicePrivacy initiative. Natalia Tomashenko, Brij Mohan Lal Srivastava, Xin Wang, Emmanuel Vincent, Andreas Nautsch, Junichi Yamagishi, Nicholas Evans, Jose Patino, Jean-François Bonastre, Paul-Gauthier Noé, Massimiliano Todisco

**Alternative anonymization metrics:**

- [Nautsch 2020] The Privacy ZEBRA: Zero Evidence Biometric Recognition Assessment. Andreas Nautsch, Jose Patino, Natalia Tomashenko, Junichi Yamagishi, Paul-Gauthier Noe, Jean-Francois Bonastre, Massimiliano Todisco, Nicholas Evans
References: participants’ papers

- **A:** [Mawalim 2020] X-Vector Singular Value Modification and Statistical-Based Decomposition with Ensemble Regression Modeling for Speaker Anonymization System. Candy Olivia Mawalim, Kasorn Galajit, Jessada Karnjana, Masashi Unoki
- **I:** [Dubagunta 2020] Adjustable Deterministic Pseudonymisation of Speech: Idiap-NKI’s submission to VoicePrivacy 2020 Challenge. S. Pavankumar Dubagunta, Rob J.J.H. van Son and Mathew Magimai-Doss
- **K:** [Han 2020] System Description for Voice Privacy Challenge. Yaowei Han, Sheng Li, Yang Cao, Masatoshi Yoshikawa
Other results
EER for ASR\textsubscript{eval} trained on orig. and anon. data: LibriSpeech
EER for $\text{ASR}_{\text{eval}}$ trained on orig. and anon. data: VCTK dev
EER for ASR$_{\text{eval}}$ trained on orig. and anon. data: VCTK test
Thank you!