IDENTIFYING SOURCE SPEAKERS FOR VOICE CONVERSION BASED SPOOFING ATTACKS ON SPEAKER VERIFICATION SYSTEMS

Danwei Cai¹, Zexin Cai¹, Ming Li¹,²

¹Department of Electrical and Computer Engineering, Duke University, Durham, USA
²Data Science Research Center, Duke Kunshan University, Kunshan, China
ming.li369@duke.edu

ABSTRACT
An automatic speaker verification system aims to verify the speaker identity of a speech signal. However, a voice conversion system could manipulate a person’s speech signal to make it sound like another speaker’s voice and deceive the speaker verification system. Most countermeasures for voice conversion-based spoofing attacks are designed to discriminate bona fide speech from spoofed speech for speaker verification systems. In this paper, we investigate the problem of source speaker identification – inferring the identity of the source speaker given the voice converted speech. To perform source speaker identification, we simply add voice-converted speech data with the label of source speaker identity to the genuine speech dataset during speaker embedding network training. Experimental results show the feasibility of source speaker identification when training and testing with converted speeches from the same voice conversion model(s). In addition, our results demonstrate that having more converted utterances from various voice conversion model for training helps improve the source speaker identification performance on converted utterances from unseen voice conversion models.¹

Index Terms: Speaker verification, voice conversion, spoofing attack, anti-spoofing, source speaker identification

1. INTRODUCTION
An automatic speaker verification system verifies the identity of speakers by analyzing audio signals. Speaker verification is a vital biometric technology in real-world applications, such as call centers for banking systems, smartphones, smart speakers, and other Internet-of-Things devices. As such applications are inherently security-critical, the robustness of speaker verification systems against spoofing attacks is of utmost importance. Even with the recent advance in speaker modeling enabled by deep neural networks (DNN)¹², speaker verification systems are susceptible to malicious spoofing attacks [3].

Between the process of signal acquisition and verification result deliveries, the speaker verification system can be manipulated or attacked in various ways [3]. Among these attacks, imposter spoofing at the microphone or during signal transmission is the most typical one. Recent studies have demonstrated that most speaker verification systems are unprotected from various spoofing attacks, such as impersonations [4], replays [5], speech synthesis [6], voice conversion [7], and adversarial attacks [8]. On the other hand, countermeasures have been developed to defend speaker verification systems from these spoofing attacks [1] [9] [10]. The Automatic Speaker Verification Spoofing And Countermeasures Challenge (ASVspoof) series are being held to support independent assessments of vulnerabilities to spoofing and to assess the performance of countermeasures against spoofing [11] [12].

This study focuses on the spoofing attack of voice conversion on speaker verification systems. Voice conversion involves manipulating a speech signal of the original person (i.e., source speaker) in order to make it sound more like the speaking voice of another person (i.e., target speaker) while preserving the linguistic content [13]. The application of deep learning has enhanced voice conversion technologies in terms of voice naturalness and voice similarity [14] [15]. The improvement, however, raises concerns regarding privacy and authentication. Therefore, preventing the incorrect use of one’s voice with voice conversion technologies becomes more and more important.

Various approaches have been proposed for speaker verification systems to defend against the spoofing attack of voice conversion. These countermeasures are usually designed to discriminate bona fide speech from spoofed speech for speaker verification systems. However, none of these countermeasures provide the ability of source speaker identification – inferring the identity of the source speaker given the voice converted speech. Source speaker identification has potential applications in crime investigation and judicial procedures. For example, source speaker identification can help identify a suspect involved in financial fraud with voice conversion-based impersonation spoofing.

Typically, a voice conversion system consists of two modules – acoustic feature conversion and waveform generation [16]. The feature conversion module changes the spectral feature of the source speaker towards the target speaker by manipulating speaker-related characteristics, such as prosody, pitch, and formants. The waveform generation module reconstructs the time-domain speech signals from the converted spectral feature. Generally speaking, feature conversion algorithms can be categorized into three groups - encoder-decoder models [17], generative adversarial network (GAN)-based models [15] and parallel spectral feature mapping models [18]. These algorithms, however, are far from perfect. The converted speech, to some extent, still retains the voice style of the source speaker. For example, the speaker-related linguistic factors reflected in sentence structure, lexical choice, and idiolect are fixed and can not be altered by a voice conversion system. For the encoder-decoder-based feature conversion, speaker-dependent factors and speaker-independent factors can not be perfectly decoupled by the encoder. The information leak of the source speaker in the speaker-independent factors will be retained during the decoding phase. For the GAN-based feature conversion, the use of the cycle consistency mechanism [19] imposes a strict “time-frequency bin level” constraint during the generation process so that speaker-
irrelevant features are retained [20].

Since the voice converted speech contains information of both source and target speakers, we can train the speaker model to recognize the converted speech as the source speaker. By setting the converted speech label as the source speaker’s identity, we train the speaker model with converted speech and bona fide speech, encouraging the speaker model to extract source speaker information from the converted speech while maintaining a discriminative speaker embedding space.

From the defender’s perspective, source speaker identification can be classified into white and black box identification. In white-box identifying, the defender can access the structure and parameters of the voice conversion models used by attackers. In black-box source speaker identification, the voice conversion models used by attackers are hidden to the defender. This paper demonstrates that source speaker identification is feasible under the white box identifying protocol: speaker verification systems can be trained to recognize the source speaker of the voice converted speech. Also, training the speaker model with converted speeches from multiple voice conversion models improves the performance of black-box source speaker identification compared to training with converted speeches generated by only one voice conversion model. This result indicates that commonality exists among converted speech from different voice conversion algorithms, and general black-box source speaker identification is possible. To the best of our knowledge, this study is the first to investigate the problem of source speaker identification for voice conversion-based spoofing attacks on speaker verification systems.

2. RELATED WORKS

2.1. Voice conversion

As mentioned before, a voice conversion system consists of two modules – feature conversion and waveform generation [16]. The feature conversion module changes the spectral feature of the source speaker towards the target speaker; and thus takes center stage in most voice conversion studies. Early studies on feature conversion relied on parallel speech data, i.e., the speech signals from source and target speakers share the same linguistic content. Under the statistical modeling framework, both parametric and non-parametric approaches were applied to parallel voice conversion. Examples of parametric approaches include Gaussian mixture model [21], dynamic kernel partial least squares regression [22]; examples of non-parametric approaches include non-negative matrix factorization [23] and phonetic sparse representation [24]. However, parallel speech data is hard to collect and thus limits the application of voice conversion. Therefore, recent studies are focused on non-parallel voice conversion. Erro et al. [25] proposed the INCA alignment algorithm to establish correspondence between non-parallel source and target audios. Other non-parallel feature conversion methods include the phonetic posteriorgrams-based approach [26,27], which uses an automatic speech recognizer to extract speaker-independent phonetic representation. However, phonetic-based features are shown to contain speaker information in speaker verification [28].

On the other hand, the aforementioned approaches mainly focus on one-to-one and many-to-one voice conversion, while many-to-many/an-y-to-any conversion greatly enhances the robustness towards unseen speakers. Various deep frameworks, including GAN [29,30] and auto-encoder structures [31,32,33,34], have been employed to achieve many-to-many voice conversion. Such systems either disentangle speaker information inherently or infer discriminative speaker representation from pre-trained automatic speaker recognition systems. In this case, many-to-many voice conversion models learn the latent speaker space through seen speakers from the training data and generalize well to unseen speakers, allowing the model to clone a target voice with just one utterance from the target speaker.

3. METHODS

Speaker embedding network aims to learn a discriminative embedding space where utterances from the same speaker are clustered together and utterances from the different speakers are separated. Voice conversion models make the attacker’s speech (source speech) sound like the target speaker to deceive the speaker verification system. Therefore, converted speech is more likely to be in the subspace of the target speaker. Source speaker identification, however, aims to learn a speaker embedding space that maps converted speech to the subspace of the source speaker.

Given a source speech dataset \( D_s = \{ s_i \} \) and a target speech dataset \( D_t = \{ t_j \} \), a voice conversion model manipulate the voice of the source speech \( s_i \) to sound like the voice of target speech \( t_j \), producing a converted speech dataset \( D_c = \{ x_{s_i \rightarrow t_j} | s_i \in D_s, t_j \in D_t \} \). The source speech dataset \( D_s \), the target speech dataset \( D_t \), and the converted speech dataset \( D_c \) associated with voice conversion algorithm \( C_k (k = 1, \ldots, K) \) are used together as the training data \( D = D_s \cup D_t \cup D_c \) to train the speaker embedding network. During training, the label of the converted speech \( x_{s_i \rightarrow t_j} \) is set as the speaker identity of the source speech \( s_i \). The speaker embedding network is trained to extract source speaker information from the converted speech while maintaining the discriminative speaker embedding space.

4. EXPERIMENTS

4.1. Dataset

We use LibriSpeech [35] as the source speech dataset and VoxCeleb [36,37] as the target speech dataset. We split LibriSpeech into a training subset containing 282,610 utterances from 2400 speakers and a testing subset containing 9,757 utterances from 84 speakers. In VoxCeleb, training data is VoxCeleb 2 development set including 1,092,009 utterances from 5,994 speakers. Testing data is VoxCeleb 1 testing set containing 4,874 utterances from 40 speakers. Training and testing data are not overlapped in both source and target datasets.

To generate voice-converted speech, we randomly sample three source speech from LibriSpeech for one target speech in VoxCeleb. In other words, each target speech is impersonated by three different attackers. To save storage and training time, we only select one-tenth (\( \frac{1}{10} \)) of VoxCeleb training data as target speech to generate converted speech for all VC systems. The total number of converted speech for a VC method is 327,600 (109,200×3).

4.2. Voice conversion models

We use four any-to-any voice conversion algorithms, i.e., AutoVC [31], AGAIN-VC [32], S2VC [38], SigVC [39], to generate voice converted speech in the experiments. We use the official implementation and pre-trained voice conversion model of AutoVC [31], AGAIN-VC [32] and S2VC [38] to generate converted speech. For S2VC, the self-
supervised representation used in our experiments is contrastive predictive coding (CPC) [40]. Also, instead of using the WaveRNN vocoder provided in the official implementation, we train a HiFiGAN vocoder [41] with VCTK dataset [42] for faster wave generation. For SigVC, we use the in-house implementation. Details of SigVC model can be found in [39]. All the VC systems are used to generate voice converted speech for both training and testing data.

4.3. Speaker embedding network training

We apply data augmentation to both genuine data (source and target speech) and voice-converted speech. Additive background noise or convolutional reverberation noise is applied to the time-domain waveform. MUSAN dataset [43] RIRS dataset [44] are used for data augmentation.

During DNN training, audio waveforms in a data batch are randomly cropped between 2 to 4 seconds. Logarithmical Mel-spectrogram with 80 frequency bins is extracted as the acoustic feature. Mel-spectrograms are computed over Hamming windows of 20ms shifted by 10ms.

We use residual convolutional network (ResNet) as the speaker encoder [45]. The ResNet’s output feature maps are aggregated with a global statistics pooling layer which calculates means and standard deviations for each feature map. A fully connected layer is employed afterward to extract the 128-dimensional speaker embedding. The speaker embedding network architecture is the same as in [46]. Rectified linear unit (ReLU) activation and batch normalization are applied to each convolutional layer in ResNet. Network parameters are updated using Adam optimizer [47] with an initial learning rate of 0.001 along with cosine decay learning rate schedule.

We train eight speaker verification systems with different setups of training data as summarized in Table 1.

- System NoVC: trained without any converted speeches
- System VC1-⋆: system trained with converted speeches generated by only one voice conversion model indicated by ⋆.
- System VC2: trained with converted speeches generated by two voice conversion models of AutoVC and AGAIN-VC
- System VC3: trained with converted speeches generated by three voice conversion models of AutoVC, AGAIN-VC, and S2VC
- System VC4: trained with converted speeches generated by all voice conversion models

| Model      | Vox | Libri | AutoVC | AGAIN-VC | S2VC | SigVC |
|------------|-----|-------|--------|----------|------|-------|
| NoVC       | √   |       |        |          |      |       |
| VC1-Auto   | √   | √     |        |          |      |       |
| VC1-AGAIN  | √   | √     |        |          |      | √     |
| VC1-S2     | √   | √     |        |          |      | √     |
| VC1-Sig    | √   | √     |        |          |      | √     |
| VC2        | √   | √     |        |          |      | √     |
| VC3        | √   | √     |        |          |      | √     |
| VC4        |      | √     |        |          |      | √     |

4.4. Source speaker identification results

Given a pair of genuine speech, a speaker verification system verifies whether they are from the same speaker. Given a pair of voice converted speech, source speaker identification system verifies whether they are from the same source speaker (imposter). Figure 1 shows the difference between speaker verification tasks and source speaker identification tasks.

For the genuine VoxCeleb 1 test set, speaker verification results are reported on the original trial list of Voxceleb 1 with 37,720 trials. The number of true trials and false trials are the same.

For the converted speech test sets with source speaker identification tasks, a positive result is produced when the system successfully verifies the source speaker (imposter) of the converted speech. The source speaker identification trail is based on the test trial from Voxceleb 1. Voice conversion is applied to convert three different source speakers into a same target voice in enrollment and test speech. Since each target speech is impersonated by three different source speech, the total number of verification trial are 339,480 (37,720 × 3 × 3). The number of true trials and false trials are 4,164 and 335,316 respectively.

We report the genuine speaker verification results and the source speaker identification results on table 2. The first column of the table shows the results of the speaker verification on VoxCeleb 1. We observe a performance drop of speaker verification on genuine data (VoxCeleb 1 test set) when the speaker embedding network is trained to perform source speaker identification.

From table 2, speaker embedding network trained with only genuine data (System NoVC) can barely identify source speaker...
from a pair of converted speech. Under white box testing protocol, speaker verification can be trained to recognize the source speaker in converted speech. When training and testing with generated speeches from the same voice conversion model, system VC1-Auto, VC1-AGAIN, VC1-S2, VC1-Sig obtain EERs of 15.8%, 7.47%, 6.5%, 24.2% respectively for source speaker verification task. It is not surprising to see a relative high EER on SigVC converted speech as SigVC system deliberately erases the speaker information from source speakers. When training with multiple VC methods, the speaker embedding network performs source speaker identification fairly well. For the model with all VC methods (system VC4), source speaker verification EERs for converted speech with AutoVC, AGAIN-VC, S2VC, and SigVC are 15.1%, 8.5%, 6.6%, 25.0% respectively.

Table 2 also highlights the source speaker identification results when the testing converted speech is from an unseen VC model not used during training. Compared to system NoVC which is trained with only genuine data, we observe performance gains on some unseen converted speech data for system VC1-Auto, VC1-AGAIN, VC1-S2, and VC1-Sig. We can also see that system VC2 trained with AutoVC and AGAIN-VC converted speech obtains an EER of 28.0% when performing source speaker identification on unseen S2VC converted speech data, which is 38%, 28%, and 10% relative performance gain compared to system NoVC, VC1-AGAIN, and VC1-Auto on unseen S2VC data, respectively. Although this blackbox testing is far from satisfactory, it does indicate that commonality exists among converted speech from different voice conversion algorithms, and general black-box source speaker identification maybe possible with more data and advanced algorithm.

5. CONCLUSION

This study investigates the problem of source speakers identifying for voice conversion-based spoofing attacks on speaker verification systems. We train the speaker model with converted speech (labeled as the identity of source speaker) as well as genuine speech, encouraging the speaker model to extract source speaker information from the converted speech while maintaining the discriminative speaker embedding space. We demonstrate that source speaker identification is feasible when training and testing with converted speeches from the same voice conversion model. Also, when testing on converted speeches from an unseen voice conversion model, we observe that the performance of source speaker identification improves as more voice conversion models are used to generate converted speech during training. This result indicates that commonality exists among converted speech from different voice conversion algorithms, and general black-box source speaker identification is possible. Further works will investigate more voice conversion models with different model architectures and try to build a general source speaker identification system in a general black-box protocol.

6. REFERENCES

[1] W. Cai, J. Chen, and M. Li, “Exploring the Encoding Layer and Loss Function in End-to-End Speaker and Language Recognition System,” in Speaker Odyssey, 2018, pp. 74–81.
[2] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, and S. Khudanpur, “x-vectors: Robust DNN Embeddings for Speaker Recognition,” in ICASSP, 2018, pp. 5329–5333.
[3] Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, and H. Li, “Spoofing and Countermeasures for Speaker Verification: A Survey,” Speech Communication, vol. 66, pp. 130–153, 2015.
[4] R. Gonzalez Hautamaki, T. Kinnunen, V. Hautamaki, and A.-M. Laukkanen, “Automatic Versus Human Speaker Verification: The Case of Voice Mimicry,” Speech Communication, vol. 72, pp. 13–31, 2015.
[5] J. Villalba and E. Lleida, “Detecting Replay Attacks from Far-Field Recordings on Speaker Verification Systems,” in European Workshop on Biometrics and ID Management, 2011, pp. 274–285.
[6] P. L. De Leon, M. Pucher, J. Yamagishi, I. Hernaez, and I. Saratxaga, “Evaluation of Speaker Verification Security and Detection of HMM-Based Synthetic Speech,” IEEE Transactions on Audio, Speech, and Language Processing, vol. 20, no. 8, pp. 2280–2290, 2012.
[7] F. Alegre, A. Amehraye, and N. Evans, “Spoofing Countermeasures to Protect Automatic Speaker Verification from Voice Conversion,” in ICASSP, 2013, pp. 3068–3072.
[8] F. Kreuk, Y. Adi, M. Cisse, and J. Keshet, “Fooling End-To-End Speaker Verification With Adversarial Examples,” in ICASSP, 2018, pp. 1962–1966.
[9] X. Li, N. Li, C. Weng, X. Liu, D. Su, D. Yu, and H. Meng, “Replay and Synthetic Speech Detection with Res2Net Architecture,” in ICASSP, 2021, pp. 6354–6358.
[10] M. Todisco, H. Delgado, and N. Evans, “Constant Q Cepstral Coefficients: A Spoofing Countermeasure for Automatic Speaker Verification,” Computer Speech & Language, vol. 45, pp. 516–535, 2017.
[11] Z. Wu, J. Yamagishi, T. Kinnunen, C. Hanilçi, M. Sahidullah, A. Sizov, N. Evans, M. Todisco, and H. Delgado, “ASVspoof: The Automatic Speaker Verification Spoofing and Countermeasures Challenge,” IEEE Journal of Selected Topics in Signal Processing, vol. 11, no. 4, pp. 588–604, 2017.
[12] J. Yamagishi, X. Wang, M. Todisco, M. Sahidullah, J. Patino, A. Nautsch, X. Liu, K. A. Lee, T. Kinnunen, N. Evans, and H. Delgado, “ASVspoof 2021: Accelerating Progress in Spoofed and Deepfake Speech Detection,” in ASVspoof 2021 Workshop-Automatic Speaker Verification and Spoofing Countermeasures Challenge, 2021.
[13] S. H. Mohammad and A. Kain, “An Overview of Voice Conversion Systems,” Speech Communication, vol. 88, pp. 65–82, 2017.
