The VoicePrivacy 2024 Challenge Evaluation Plan

Version **1.0**

organisers@lists.voiceprivacychallenge.org[1]

[1]Inria, France
[2]Singapore Institute of Technology, Singapore
[3]Institute for Natural Language Processing, University of Stuttgart, Germany
[4]National Institute of Informatics, Tokyo, Japan
[5]Audio Security and Privacy Group, EURECOM, France

https://voiceprivacychallenge.org

For new participants — Executive summary

- The task is to develop a voice anonymization system for speech data which conceals the speaker's voice identity while protecting linguistic content and emotional states.
- The organizers provide development and evaluation datasets and evaluation scripts, as well as baseline anonymization systems and a list of training resources formed on the basis of the participants' requests. Participants apply their developed anonymization systems, run evaluation scripts and submit evaluation results and anonymized speech data to the organizers.
- Results will be presented at a workshop held in conjunction with Interspeech 2024 to which all participants are invited to present their challenge systems and to submit additional workshop papers.

For readers familiar with the VoicePrivacy Challenge — Changes w.r.t. 2022

- In line with the considered application scenarios, the requirements that anonymization preserves voice distinctiveness and intonation are removed, hence the associated G_{VD} and ρ^{F_0} metrics are no longer used. All the data are anonymized on the *utterance level*.
- An extended list of datasets and pretrained models, formed on the basis of the participants' requests, will be provided for training anonymization systems.
- The complexity of the evaluation protocol and the running time of the evaluation scripts have been greatly reduced. The scripts are now primarily in Python, which makes it easy for participants who are new to the field to catch up.
- Only objective evaluation will be performed. Three complementary metrics will be used: the equal error rate (EER) as the privacy metric and two utility metrics, namely the word error rate (WER) for automatic speech recognition (ASR) and the unweighted average recall (UAR) for speech emotion recognition (SER).
- Models for utility evaluation (ASR and SER) are trained on original (unprocessed) data to ensure that linguistic and emotional content is undistorted. These models are provided with the evaluation scripts, hence utility evaluation is much faster.

1 Challenge objectives

Speech data fall within the scope of privacy regulations such as the European General Data Protection Regulation (GDPR). Indeed, they encapsulate a wealth of personal (a.k.a. personally identifiable) information such as the speaker's identity, age and gender, health status, personality, racial or ethnic origin, geographical background, social identity, and socio-economic status [1]. Formed in 2020, the VoicePrivacy initiative [2] is spearheading efforts to develop privacy preservation solutions for speech technology. So far, it has focused on promoting the development of *anonymization* solutions which conceal all personal information, facilitating their comparison using common datasets and protocols, and defining meaningful evaluation metrics through a series of competitive benchmarking challenges. The first two editions of VoicePrivacy were held in 2020 and 2022 [2–5]. VoicePrivacy 2024, the third edition, starts in March 2024 and culminates in the VoicePrivacy Challenge workshop held in conjunction with the 4nd Symposium on Security and Privacy in Speech Communication (SPSC)[1], a joint event co-located with Interspeech 2024[2] in Kos Island, Greece.

Anonymization requires a combination of solutions to alter not only the speaker's voice, but also linguistic content, extra-linguistic traits, and background sounds which might reveal the speaker's identity. In keeping with the previous VoicePrivacy Challenge editions, the current edition focuses on the subgoal of *voice anonymization*, that is the task of altering the speaker's voice to conceal their identity to the greatest possible extent, while leaving the linguistic content and paralinguistic attributes intact. Specifically, this edition focuses on preserving the emotional state, that is the key paralinguistic attribute in many real-world application scenarios of voice anonymization, e.g., in call centers to enable the use of third-party speech analytics. In the following, we often refer to "voice anonymization" as "anonymization" alone for the sake of conciseness.

This document describes the challenge task, the data, pretrained models and baseline systems that participants can use to build their own voice anonymization system, and the evaluation metrics and rules that will be used for assessment, in addition to guidelines for registration and submission.

2 Task

Privacy protection is formulated as a game between a *user* who shares data for a desired downstream task and an *attacker* who accesses this data or data derived from it and uses it to infer information about the data subjects [2, 6, 7]. Here, we consider the scenario where the user shares anonymized utterances for downstream automatic speech recognition (ASR) and speech emotion recognition (SER) tasks, and the attacker wants to identify the speakers from their anonymized utterances.

2.1 Voice anonymization task

The utterances shared by the user are referred to as *trial* utterances. In order to hide the identity of the speaker within each utterance, the user passes the utterance through a voice anonymization system prior to sharing. The resulting utterance sounds as if it was uttered by another speaker, which we refer to as a *pseudo-speaker*. The pseudo-speaker might, for instance, be an artificial voice not corresponding to any real speaker.

The task of challenge participants is to develop this voice anonymization system. It should:

(a) output a speech waveform;

(b) conceal the speaker identity on the *utterance level*;

(c) not distort the linguistic and emotional content.

The utterance-level anonymization requirement (b) means that the voice anonymization system must assign a pseudo-speaker to each utterance independently of the other utterances. The pseudo-speaker assignment process must be identical across all utterances and not rely on speaker labels. When this process involves a random number generator, the random number(s) generated must be different for each utterance, typically resulting in a different pseudo-speaker for each utterance. Voice anonymization systems that assign a single pseudo-speaker to all utterances also satisfy this requirement.

The achievement of requirement (c) is assessed via *utility* metrics. Specifically, we will measure the WER and UAR obtained by ASR and SER systems trained on original (unprocessed) data.

[1] 4th Symposium on Security and Privacy in Speech Communication: http://www.spsc2024.mobileds.de/
[2] https://www.interspeech2024.org/

2.2 Attack model

For each speaker of interest, the attacker is assumed to have access to utterances spoken by that speaker, which are referred to as *enrollment* utterances. He then uses an automatic speaker verification (ASV) system to re-identify the speaker corresponding to each anonymized trial utterance.

In this work, we assume that the attacker has access to:

(a) several enrollment utterances for each speaker;

(b) the voice anonymization system employed by the user.

Using this information, the attacker anonymizes the enrollment utterances to reduce the mistmatch with the trial utterances, and trains an ASV system adapted to that specific anonymization system. This attack model is the strongest known to date, hence we consider it as the most reliable for privacy assessment.

The protection of identity information is assessed via a *privacy* metric. Specifically, we will measure the EER obtained by the attacker.

3 Data and pretrained models

Publicly available resources will be used for the training, development and evaluation of voice anonymization systems. The development and evaluation data are fixed, while the choice of training resources is open to the participants.

3.1 Training resources

In addition to the training data used in the previous challenge editions and those used to train the baseline anonymization systems (see Section 5), the participants are allowed to propose additional resources to build and train anonymization systems. These include both data and pretrained models.

Requirements for training data and pretrained models

- All the proposed training data and pretrained models (e.g., wav2vec, wavLM, HuBERT, Whisper, etc.) should be openly available to everyone at no cost.
- Each registered participant can submit a list of proposed data and models (with the corresponding URLs) to the organizers at organisers@lists.voiceprivacychallenge.org by **20th March**.
- The organizers will verify these requests and publish the list of training data and pretrained models allowed for training anonymization systems in an updated version of the evaluation plan to be shared with the participants on **21st March**. Any other data or models not included the list will not be allowed for training anonymization systems.

3.2 Development and evaluation data

Development and evaluation data comprise subsets of the following corpora:

- ***LibriSpeech***[3] [8] is a corpus of read English speech derived from audiobooks and designed for ASR research. It contains 960 hours of speech sampled at 16 kHz. This data will be used for ASV and ASR evaluation. The *LibriSpeech* evaluation and development sets are the same as in the previous challenge editions.
- ***IEMOCAP*** [9] is an emotional audio-visual dataset that will be used for SER evaluation. It contains 12 hours of speech sampled at 16 kHz corresponding to improvised and scripted two-speaker conversations between 5 female and 5 male English actors. We consider only 4 emotions out of the 9 annotated ones: *neutral*, *sadness*, *anger*, and *happiness*. Following [10–12], we merge the original happiness and excitement classes into the happiness class to balance the number of utterances in each class. To accommodate for the small number of speakers and the small amount of data, we adopt a leave-one-conversation out cross-validation protocol. In each

[3]LibriSpeech: http://www.openslr.org/12

cross-validation fold, four conversations (eight speakers) are used to train the SER evaluation system[4], while the two speakers from the remaining conversation form the development and evaluation sets, respectively.

A detailed description of the datasets provided for development and evaluation is presented in Tables 1 and 2 below.

Table 1: Statistics of the *LibriSpeech* development and evaluation sets for ASV and ASR evaluation.

Subset			**Female**	**Male**	**Total**	**#Utterances**
Development	LibriSpeech dev-clean	Enrollment	15	14	29	343
		Trial	20	20	40	1,978
Evaluation	LibriSpeech test-clean	Enrollment	16	13	29	438
		Trial	20	20	40	1,496

Table 2: Construction and statistics of the *IEMOCAP* development and evaluation sets for SER evaluation. *Train* subsets refer to the training data for the SER evaluation system.

Conversation		**#Utterances**	**Fold 1**	**Fold 2**	**Fold 3**	**Fold 4**	**Fold 5**
Session 1	Female	528	Dev	Train	Train	Train	Train
	Male	557	Eval				
Session 2	Female	481	Train	Eval			
	Male	542		Dev			
Session 3	Female	522		Train	Dev		
	Male	629			Eval		
Session 4	Female	528			Train	Eval	
	Male	503				Dev	
Session 5	Female	590				Train	Eval
	Male	651					Dev

4 Privacy and utility evaluation

We consider one objective privacy metric to assess the speaker re-identification risk and two objective utility metrics to assess the fulfillment of the downstream tasks specified in Section 2.

4.1 Objective assessment of the privacy-utility tradeoff

Three metrics will be used for the objective ranking of submitted systems: the equal error rate (EER) as the privacy metric and two utility metrics: word error rate (WER) and unweighted average recall (UAR). These metrics rely on automatic speaker verification (ASV), automatic speech recognition (ASR), and speech emotion recognition (SER) systems. The ASR system is trained on *LibriSpeech-train-clean-360* and the ASV system on the full *LibriSpeech-train-960* dataset, whose statistics are presented in Table 3. The SER system for each *IEMOCAP* cross-validation fold is trained on the corresponding *IEMOCAP* training subset, whose statistics are reported in Table 2. Training and evaluation will be performed with the provided recipes and models.[5] More specifically, models

[4]Trained SER evaluation systems corresponding to the 5 folds are provided by the organizers. The participants should not use this data for their own training purposes.

[5]Evaluation scripts: https://github.com/Voice-Privacy-Challenge/Voice-Privacy-Challenge-2024

Table 3: Statistics of the *LibriSpeech* training sets for ASV and ASR evaluation.

System	**Subset**	**Size,h**	**#Speakers**			**#Utterances**
			Female	**Male**	**Total**	
ASV	LibriSpeech train-clean-360	363.6	439	482	921	104,014
ASR	LibriSpeech train-960	960.9	1128	1210	2338	281,241

for privacy evaluation will be trained by participants on their anonymized training data with the provided training scripts, while the models for utility evaluation are provided by the organizers.

As in the 2022 edition, multiple evaluation conditions specified with a set of minimum target privacy requirements will be considered. For each minimum target privacy requirement, submissions that meet this requirement will be ranked according to the resulting utility for each utility metric separately. The goal is to measure the privacy-utility trade-off at multiple operating points, e.g. when systems are configured to offer better privacy at the cost of utility and vice versa. This approach to assessment aligns better the VoicePrivacy Challenge with the user expectation of privacy and allows for a more comprehensive evaluation of each solution, while also providing participants with a set of clear optimisation criteria. The privacy and utility metrics will be used for this purpose.

Minimum target privacy requirements are specified with a set of N minimum target EERs: $\{\text{EER}_1, \ldots, \text{EER}_N\}$. Each minimum target EER constitutes a separate evaluation condition. Participants are encouraged to submit solutions to as many conditions as possible. Submissions to any one condition i should achieve an average EER on the VoicePrivacy 2024 evaluation set greater than the corresponding EER_i. The set of valid submissions for each EER_i will then be ranked according to the corresponding WER and UAR. The VoicePrivacy 2024 Challenge involves $N = 4$ conditions with minimum target EERs of: $\text{EER}_1 = 10\%$, $\text{EER}_2 = 20\%$, $\text{EER}_3 = 30\%$, $\text{EER}_4 = 40\%$.

The lower the WER for a given EER condition, the better the rank of the considered system in ASR results ranking. Similarily, the higher the UAR for a given EER condition, the better the rank of the considered system in SER results ranking. A depiction of example results and system rankings according to this methodology is shown in Figure 1.

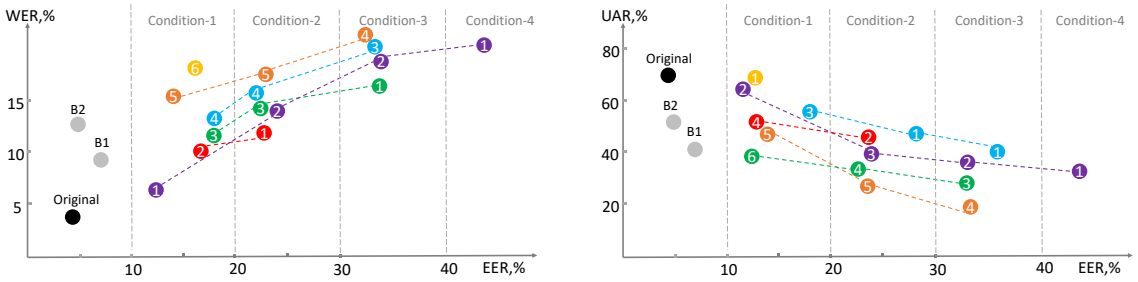

Figure 1: Example system rankings according to the privacy (EER) and utility (WER and UAR) results for 4 minimum target EERs. Different colors correspond to 6 different teams. Numbers within each circle show system ranks for a given condition. Grey circles correspond to the baseline systems, and the black circle to the original (unprocessed) data.

4.2 Privacy metric: equal error rate (EER)

The ASV system used for privacy evaluation is an ECAPA-TDNN [13] with 512 channels in the convolution frame layers, implemented by adapting the *SpeechBrain* [14] *VoxCeleb* recipe to *LibriSpeech*. As seen in Figure 2, we consider a *semi-informed* attacker, who has access to the anonymization system under evaluation [3,7]. Using that system, the attacker anonymizes the original enrollment data so as to reduce the mismatch with the anonymized trial data. In addition, the attacker anonymizes the *LibriSpeech-train-clean-360* dataset and retrains the ASV system (denoted $ASV^{\text{anon}}_{\text{eval}}$) on it, so that it is adapted to this specific anonymization system.[6] Anonymization is conducted on the *utterance level*, using the same pseudo-speaker assignment process as the trial data. For a given speaker, all enrollment utterances are used to compute an average speaker vector for enrollment.

For every pair of enrollment and trial speaker vectors in the *LibriSpeech* development and evaluation sets, the cosine similarity score is computed from which a same-speaker vs. different-speaker decision is made by thresholding. Denoting by $P_{\text{fa}}(\theta)$ and $P_{\text{miss}}(\theta)$ the false alarm and miss rates at threshold θ, the EER metric corresponds to the threshold θ_{EER} at which the two detection error rates are equal, i.e., $\text{EER} = P_{\text{fa}}(\theta_{\text{EER}}) = P_{\text{miss}}(\theta_{\text{EER}})$. The higher the WER, the greater the privacy. The number of same-speaker and different-speaker pairs is given in Table 4.

[6] It is critical that the $ASV^{\text{anon}}_{\text{eval}}$ system is well trained, indeed a badly trained system can overestimate the EER and give a false sense of privacy [15]. The organizers will use the anonymized data submitted by the participants to check it. In the event when some submissions do not satisfy it, the organizers reserve the right to modify the ASV evaluation scripts or to mark those submissions accordingly to ensure a fair competition.

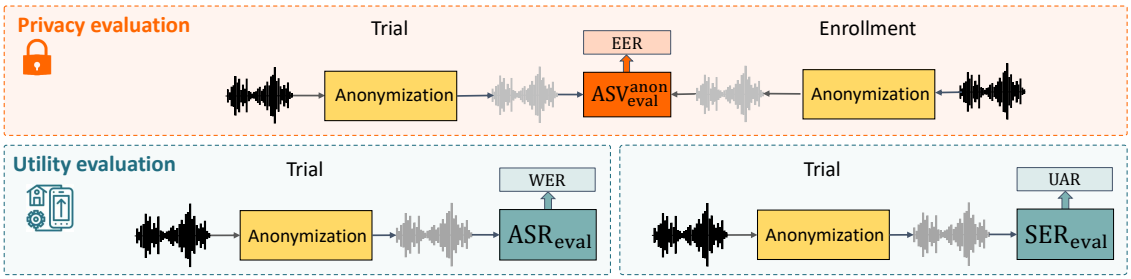

Figure 2: Privacy and utility evaluation.

Table 4: Number of same-speaker and different-speaker pairs considered for evaluation.

Subset		Trials	Female	Male	Total
Development	LibriSpeech dev-clean	Same-speaker	704	644	1,348
		Different-speaker	14,566	12,796	27,362
Evaluation	LibriSpeech test-clean	Same-speaker	548	449	997
		Different-speaker	11,196	9,457	20,653

4.3 Utility metrics

4.3.1 Word error rate (WER)

The ability of the anonymization system to leave the linguistic content undistorted is assessed using an ASR system[7] (denoted ASR_{eval}) fine-tuned on *LibriSpeech-train-960* from *wav2vec2-large-960h-lv60-self*[8] using a *SpeechBrain* recipe. Unlike the 2022 challenge edition, this ASR evaluation model is fixed, and trained and fine-tuned on original (unprocessed) data.

For every anonymized trial utterance in the *LibriSpeech* development and evaluation sets, the ASR system outputs a word sequence. The WER is calculated as

$$\text{WER} = \frac{N_{\text{sub}} + N_{\text{del}} + N_{\text{ins}}}{N_{\text{ref}}},$$

where N_{sub}, N_{del}, and N_{ins} are the number of substitution, deletion, and insertion errors, respectively, and N_{ref} is the number of words in the reference. The lower the WER, the greater the utility.

4.3.2 Unweighted average recall (UAR)

The ability of the anonymization system to leave the emotional content undistorted is assessed using an SER system (denoted SER_{eval}) trained using the *SpeechBrain* recipe for SER on *IEMOCAP*. It is a wav2vec2-based model that has been trained separately for each of the training folds in Table 2.

Within each fold, emotion recognition performance is quantified on the anonymized *IEMOCAP* development and evaluation sets using the standard UAR metric calculated as the sum of class-wise recalls R_i divided by the number of classes N_{class}:

$$\text{UAR} = \frac{\sum_{i=1}^{N_{\text{class}}} R_i}{N_{\text{class}}}.$$

The recall R_i for each class i is computed as number of true positives divided by the total number of samples in that class. The obtained UARs are then averaged across the five folds. The higher the UAR, the greater the utility.

5 Baseline voice anonymization systems

Baseline voice anonymization systems are released to help participants develop their own system.

[7] https://huggingface.co/speechbrain/asr-wav2vec2-librispeech
[8] https://huggingface.co/facebook/wav2vec2-large-960h-lv60-self

Established and upcoming baseline systems

In the current version of the evaluation plan (1.0), we provide a description and evaluation results for two established baseline systems inspired from past challenge editions, that will be used to gauge progress with respect to these editions. In the next version of the evaluation plan to be published mid-March, we will release new, more powerful baseline systems.

5.1 Anonymization using x-vectors and a neural source-filter model: B1

The baseline anonymization system **B1** is based on a common approach to x-vector modification and speech synthesis. It is identical to the **B1.b** baseline from the VoicePrivacy 2022 Challenge [5], except that anonymization is now performed on the utterance level instead of the speaker level.

B1 is based on the voice anonymization method proposed in [16] and shown in Figure 3. Anonymization is performed in three steps:

- **Step 1 – Feature extraction:** extraction of the speaker x-vector [17], the fundamental frequency (F0) and bottleneck (BN) features from the original audio waveform.
- **Step 2 – X-vector anonymization:** generation of an anonymized (pseudo-speaker) x-vector using an external pool of speakers.
- **Step 3 – Speech synthesis:** synthesis of an anonymized speech waveform from the anonymized x-vector and the original BN and F0 features using a neural source-filter (NSF) model.

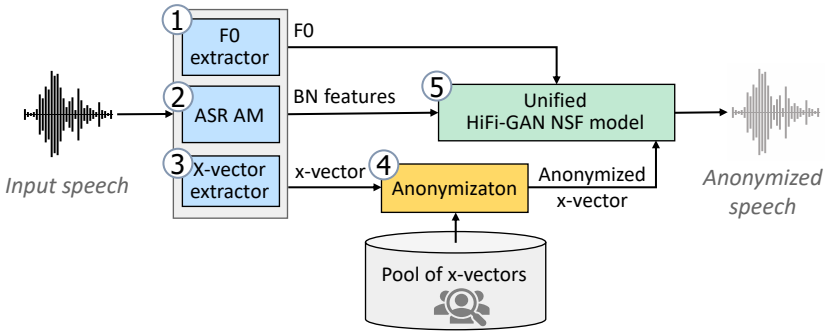

Figure 3: Baseline anonymization system **B1**.

In order to implement these steps, four different models are required, as shown in Figure 3. Details for training these components are presented in Table 5.

In *Step 1*, to extract BN features, an ASR acoustic model (AM) is trained (#1 in Table 5). We assume that the BN features represent the linguistic content of the speech signal. The ASR AM has a factorized time delay neural network (TDNN-F) model architecture [18, 19] and is trained using the Kaldi toolkit [20]. To encode speaker information, an x-vector extractor with a TDNN model topology (#2 in Table 5) is also trained using Kaldi.

In *Step 2*, for a given source speaker, a new anonymized x-vector is computed by averaging a set of candidate x-vectors from the speaker pool. Probabilistic linear discriminant analysis (PLDA) is used as a distance measure between these vectors and the x-vector of the source speaker. The candidate x-vectors for averaging are chosen in two steps. First, for a given source x-vector, the N farthest x-vector candidates in the speaker pool are selected. Second, a smaller subset of N^* candidates are chosen randomly among those N vectors ($N = 200$ and $N^* = 100$). The x-vectors for the speaker pool are extracted from a disjoint dataset (*LibriTTS-train-other-500*).

In *Step 3*, the NSF model used to synthesize the anonymized speech waveform is trained on *LibriTTS-train-clean-100* in the same manner as HiFi-GAN [21] using the HiFi-GAN discriminators. After training, the discriminators can be safely discarded, and only the trained NSF model is used in the anonymization system.

More details about this model can be found in the scripts for VoicePrivacy 2022[9] and in [22, 23].

[9]To perform *utterance-level* (in contrast to *speaker-level*) anonymization of the enrollment and trial data for **B1**, the corresponding parameters should be setup in config.sh: `anon_level_trials=utt` and `anon_level_enroll=utt`.

[10]pYAAPT: `http://bjbschmitt.github.io/AMFM_decompy/pYAAPT.html`

Table 5: Modules and training corpora for the anonymization system **B1**. The module indexes are the same as in Figure 3. Superscript numbers represent feature dimensions.

#	Module	Description	Output features	Data
1	F0 extractor	pYAAPT[10], uninterpolated	$F0^{1}$	-
2	ASR AM	TDNN-F Input: $MFCC^{40}$ + i-$vectors^{100}$ 17 TDNN-F hidden layers Output: 6032 triphone ids LF-MMI and CE criteria	BN^{256} features extracted from the final hidden layer	LibriSpeech: train-clean-100 train-other-500
3	X-vector extractor	TDNN Input: $MFCC^{30}$ 7 hidden layers + 1 stats pooling layer Output: 7232 speaker ids CE criterion	speaker x-$vectors^{512}$	VoxCeleb-1,2
4	X-vector anonymization module		pseudo-speaker x-$vectors^{512}$	(Pool of speakers) LibriTTS: train-other-500
5	NSF model	sinc-hn-NSF in [24] + HiFi-GAN discriminators [21] Input: $F0^{1}$+ BN^{256} + x-$vectors^{512}$ Training criterion defined in Hifi-GAN [21]	speech waveform	LibriTTS: train-clean-100

5.2 Anonymization using the McAdams coefficient: B2

The second baseline anonymization system **B2** shown in Figure 4 is identical to the **B2** baseline from the VoicePrivacy 2022 Challenge [5]. In contrast to **B1**, it does not require any training data and is based upon simple signal processing techniques. It is a randomized version of the anonymization method proposed in [25], which employs the McAdams coefficient [26] to shift the pole positions derived from linear predictive coding (LPC) analysis of speech signals.

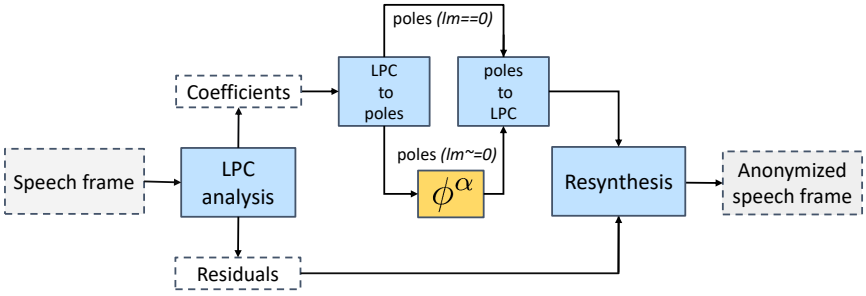

Figure 4: Baseline anonymization system **B2**.

B2 starts with the application of frame-by-frame LPC source-filter analysis to derive LPC coefficients and residuals. The residuals are set aside for later resynthesis, whereas the LPC coefficients are converted into pole positions in the z-plane by polynomial root-finding. Each pole corresponds to a peak in the spectrum, resembling a formant position. The McAdams' transformation is applied to the phase of each pole: while real-valued poles are left unmodified, the phase ϕ (between 0 and π radians) of poles with non-zero imaginary parts is raised to the power of the McAdams' coefficient α so that transformed poles have new, shifted phases of ϕ^{α}. The coefficient α is sampled for each utterance from a uniform distribution: $\alpha \sim U(\alpha_{\min}, \alpha_{\max})$, with $\alpha_{\min} = 0.5$ and $\alpha_{\max} = 0.9$. It implies a contraction or expansion of the pole positions around $\phi = 1$ radian. For a sampling rate of 16 kHz, i.e. for the data used in this challenge, $\phi = 1$ radian corresponds to approximately 2.5 kHz which is the approximate mean formant position [27]. The corresponding complex conjugate poles are similarly shifted in the opposite direction and the new set of poles, including original real-valued poles, are converted back into LPC coefficients. Finally, the LPC coefficients and the residuals are used to resynthesise a new speech frame in the time domain.

5.3 Results

Results for the two baselines are reported in Tables 6, 7, and 8. **B1** achieves a better average EER and WER than **B2**, while **B2** achieves a better UAR than **B1**.

Table 6: EER (%) achieved on data anonymized by **B1** or **B2** vs. original (Orig.) data.

Dataset	**Gender**	**EER (%)**		
		Orig.	**B1**	**B2**
LibriSpeech-dev	female	10.51	10.37	14.20
	male	0.93	6.99	2.02
Average dev		5.72	8.68	8.11
LibriSpeech-test	female	8.76	10.58	7.48
	male	0.42	6.68	2.91
Average test		4.59	8.63	5.20

Table 7: WER (%) achieved on data processed by **B1** or **B2** vs. original (Orig.) data.

Dataset	**WER (%)**		
	Orig.	**B1**	**B2**
LibriSpeech-dev	2.89	3.41	10.70
LibriSpeech-test	3.07	6.27	10.41

Table 8: UAR (%) achieved on data processed by **B1** or **B2** vs. original (Orig.) data.

Dataset	**UAR (%)**		
	Orig.	**B1**	**B2**
IEMOCAP-dev	69.08	43.13	55.61
IEMOCAP-test	71.06	42.31	53.49

6 Evaluation rules

- Participants are free to develop their own anonymization systems, using components of the baselines or not. These systems must operate on the *utterance level*.
- Participants are strongly encouraged to make multiple submissions corresponding to different privacy-utility tradeoffs (see Section 4.2).
- The three metrics (EER, WER, UAR) will be used for system ranking on the provided development and evaluation sets. Within each EER interval – [10,20), [20,30), [30,40), [40,100) – systems will be ranked separately in order of (1) increasing WER and (2) decreasing UAR.
- Participants can submit a list of proposed data and pretrained models they wish to use to build and train anonymization systems to the organizers by **20th March 2024**. The list of allowed training data and pretrained models will be published by the organizers on **21st March 2024** in an upcoming version of the evaluation plan. The use of any other data or models not included in the list published by the organizers is strictly prohibited.
- Participants must anonymize the development and evaluation sets and the *LibriSpeech-train-clean-360* dataset used to train the ASV evaluation model using the same anonymization system. They must then train the ASV evaluation model on the anonymized training data and compute the evaluation metrics (EER, WER, UAR) on the development and evaluation sets using the provided scripts. Modifications to the training or evaluation recipes (e.g., changing the ASV model architecture or hyperparameters, retraining the ASR and SER models, etc.) are prohibited.

7 Post-evaluation analysis

The organizers will run additional post-evaluation experiments in order to further characterize the performance of submitted systems. To do so, we ask all participants to share with us the anonymized speech data obtained when running their anonymization system on the training, development and evaluation sets. Further details about these experiments will follow in due course.

8 Registration and submission of results

8.1 Registration

Participants/teams are requested to register for the evaluation. Registration should be performed **once only** for each participating entity using the registration form. Participants will receive a confirmation email within ∼24 hours after successful registration, otherwise or in case of any questions they should contact the organizers:

organisers@lists.voiceprivacychallenge.org.

Also, for the updates, all participants and everyone interested the VoicePrivacy Challenge are encouraged to subscribe to the group:

https://groups.google.com/g/voiceprivacy.

8.2 Submission of results

Each participant may submit as many systems as they wish for each minimum target EER provided in Section 4.2. In the case of three or more submissions per condition, the organisers will only include the system with the lowest WER and the system with the highest UAR in the official ranking. These two systems (or this system in case it's the same one) will be ranked in terms of both WER and SER. Participants should submit audio data for these two best (ASR, SER) systems per condition.

Each single submission should include a compressed archive containing:

1. Directories with the result files, the corresponding cosine similarity scores (saved in `exp/asv_orig/cosine_out` and `exp/asv_anon<anon_data_suffix>/cosine_out`), and additional information generated by the evaluation scripts:
   - `exp/results_summary`
   - `exp/asv_orig`
   - `exp/asv_anon<anon_data_suffix>`
   - `exp/asr`
   - `exp/ser/*csv`.
2. The corresponding anonymized speech data (wav files, 16 kHz, with the same names as in the original corpus) generated from the development and evaluation sets and from the *LibriSpeech-train-clean-360* dataset used to train the ASV evaluation model. For evaluation, the wav files will be converted to 16-bit signed integer PCM format, and this format is recommended for submission. These data will be used by the challenge organizers to verify the submitted scores, perform post-evaluation analysis with other metrics and subjective listening tests. All anonymized speech data should be submitted in the form of a single compressed archive.

A summary of the ASR, WER and UAR results on the development and evaluation sets is saved in a single file `exp/results_summary`) [11].

Each participant should also submit a single, detailed system description. All submissions should be made according to the schedule below. Submissions received after the deadline will be marked

[11] Example *results* files for the baseline systems:

- **B1**: https://github.com/Voice-Privacy-Challenge/Voice-Privacy-Challenge-2024/blob/main/results/result_for_rank_b1b
- **B2**: https://github.com/Voice-Privacy-Challenge/Voice-Privacy-Challenge-2024/blob/main/results/result_for_rank_mcadams

as 'late' submissions, without exception. System descriptions will be made publicly available on the Challenge website. Further details concerning the submission procedure will be published via https://groups.google.com/g/voiceprivacy, by email, or via the VoicePrivacy Challenge website.

9 VoicePrivacy Challenge workshop at Interspeech 2024

The VoicePrivacy 2024 Challenge will culminate in a joint workshop held in Kos Island, Greece in conjunction with **Interspeech 2024** and in cooperation with the ISCA SPSC Symposium.[1] VoicePrivacy 2024 Challenge participants are encouraged to submit papers describing their challenge entry according to the paper submission schedule (see Section 10). Paper submissions must conform to the format of the ISCA SPSC Symposium proceedings, detailed in the author's kit[12], and be 4 to 6 pages long excluding references. Papers must be submitted via the online paper submission system. Submitted papers will undergo peer review via the regular ISCA SPSC Symposium review process, though the review criteria applied to regular papers will be adapted for VoicePrivacy Challenge papers to be more in keeping with systems descriptions and results. Nonetheless, the submission of regular scientific papers related to voice privacy and anonymization are also invited and will be subject to the usual review criteria. Since subjective evaluation results will be released only after the submission deadline, challenge papers should report only objective evaluation results. The same paper template should be used for system descriptions but may be 2 to 6 pages in length.

Accepted papers will be presented at the joint ISCA SPSC Symposium and VoicePrivacy Challenge Workshop and will be published as other symposium proceedings in the ISCA Archive. Challenge participants without accepted papers are also invited to participate in the workshop and present their challenge contributions reported in system descriptions.

More details will be announced in due course.

10 Schedule

The result submission deadline is **15th June 2024**. All participants are invited to present their work at the joint SPSC Symposium and VoicePrivacy Challenge workshop that will be organized in conjunction with Interspeech 2024.

Table 9: Important dates

Release of evaluation data, software and baselines	8th March 2024
Deadline for participants to submit a list for training data and models	20th March 2024
Publication of the full final list of training data and models	21st March 2024
Submission of challenge papers to the joint SPSC Symposium and VoicePrivacy Challenge workshop	15th June 2024
Deadline for participants to submit objective evaluation results, anonymized data, and system descriptions	15th June 2024
Author notification for challenge papers	5th July 2024
Final paper upload	25th July 2024
Joint SPSC Symposium and VoicePrivacy Challenge workshop	6th September 2024

11 Acknowledgement

This work was supported by the French National Research Agency under project Speech Privacy and project IPoP of the Cybersecurity PEPR and jointly by the French National Research Agency and the Japan Science and Technology Agency under project VoicePersonae. The challenge organizers thank Ünal Ege Gaznepoğlu for his help with the code base.

References

[1] A. Nautsch, A. Jimenez, A. Treiber, J. Kolberg, C. Jasserand, E. Kindt, H. Delgado, M. Todisco, M. A. Hmani, A. Mtibaa, M. A. Abdelraheem, A. Abad, F. Teixeira, D. Matrouf, M. Gomez-Barrero, D. Petrovska-Delacrétaz, G. Chollet, N. Evans, T. Schneider, J.-F. Bonastre, and

[12] https://interspeech2024.org/author-resources/

C. Busch, "Preserving privacy in speaker and speech characterisation," *Computer Speech and Language*, vol. 58, pp. 441–480, 2019.

[2] N. Tomashenko, B. M. L. Srivastava, X. Wang, E. Vincent, A. Nautsch, J. Yamagishi, N. Evans, J. Patino, J.-F. Bonastre, P.-G. Noé, and M. Todisco, "Introducing the VoicePrivacy Initiative," in *Interspeech*, 2020, pp. 1693–1697.

[3] N. Tomashenko, X. Wang, E. Vincent, J. Patino, B. M. L. Srivastava, P.-G. Noé, A. Nautsch, N. Evans, J. Yamagishi, B. O'Brien, A. Chanclu, J.-F. Bonastre, M. Todisco, and M. Maouche, "The VoicePrivacy 2020 Challenge: Results and findings," *Computer Speech and Language*, vol. 74, p. 101362, 2022.

[4] ——, "Supplementary material to the paper. The VoicePrivacy 2020 Challenge: Results and findings," https://hal.archives-ouvertes.fr/hal-03335126, 2021.

[5] N. Tomashenko, X. Wang, X. Miao, H. Nourtel, P. Champion, M. Todisco, E. Vincent, N. Evans, J. Yamagishi, and J.-F. Bonastre, "The VoicePrivacy 2022 Challenge evaluation plan," *arXiv preprint arXiv:2203.12468*, 2022.

[6] J. Qian, F. Han, J. Hou, C. Zhang, Y. Wang, and X.-Y. Li, "Towards privacy-preserving speech data publishing," in *IEEE Conference on Computer Communications (INFOCOM)*, 2018, pp. 1079–1087.

[7] B. M. L. Srivastava, N. Vauquier, M. Sahidullah, A. Bellet, M. Tommasi, and E. Vincent, "Evaluating voice conversion-based privacy protection against informed attackers," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020, pp. 2802–2806.

[8] V. Panayotov, G. Chen, D. Povey, and S. Khudanpur, "LibriSpeech: an ASR corpus based on public domain audio books," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 5206–5210.

[9] C. Busso, M. Bulut, C.-C. Lee, A. Kazemzadeh, E. Mower, S. Kim, J. N. Chang, S. Lee, and S. S. Narayanan, "IEMOCAP: Interactive emotional dyadic motion capture database," *Journal of Language Resources and Evaluation*, vol. 42, pp. 335–359, 2008.

[10] R. Pappagari, T. Wang, J. Villalba, N. Chen, and N. Dehak, "X-vectors meet emotions: A study on dependencies between emotion and speaker recognition," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2020, pp. 7169–7173.

[11] J. Cho, R. Pappagari, P. Kulkarni, J. Villalba, Y. Carmiel, and N. Dehak, "Deep neural networks for emotion recognition combining audio and transcripts," in *Interspeech*, 2018, pp. 247–251.

[12] H. Nourtel, P. Champion, D. Jouvet, A. Larcher, and M. Tahon, "Evaluation of speaker anonymization on emotional speech," in *1st ISCA Symposium on Security and Privacy in Speech Communication (SPSC)*, 2021, pp. 62–66.

[13] B. Desplanques, J. Thienpondt, and K. Demuynck, "ECAPA-TDNN: Emphasized channel attention, propagation and aggregation in TDNN based speaker verification," in *Interspeech*, 2020, pp. 3830–3834.

[14] M. Ravanelli, T. Parcollet, P. Plantinga, A. Rouhe, S. Cornell, L. Lugosch, C. Subakan, N. Dawalatabad, A. Heba, J. Zhong, J.-C. Chou, S.-L. Yeh, S.-W. Fu, C.-F. Liao, E. Rastorgueva, F. Grondin, W. Aris, H. Na, Y. Gao, R. D. Mori, and Y. Bengio, "SpeechBrain: A general-purpose speech toolkit," *arXiv preprint arXiv:2106.04624*, 2021.

[15] P. Champion, "Anonymizing speech: Evaluating and designing speaker anonymization techniques," Ph.D. dissertation, Université de Lorraine, 2023.

[16] F. Fang, X. Wang, J. Yamagishi, I. Echizen, M. Todisco, N. Evans, and J.-F. Bonastre, "Speaker anonymization using x-vector and neural waveform models," in *Speech Synthesis Workshop*, 2019, pp. 155–160.

[17] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, and S. Khudanpur, "X-vectors: Robust DNN embeddings for speaker recognition," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2018, pp. 5329–5333.

[18] D. Povey, G. Cheng, Y. Wang, K. Li, H. Xu, M. Yarmohammadi, and S. Khudanpur, "Semi-orthogonal low-rank matrix factorization for deep neural networks." in *Interspeech*, 2018, pp. 3743–3747.

[19] V. Peddinti, D. Povey, and S. Khudanpur, "A time delay neural network architecture for efficient modeling of long temporal contexts," in *Interspeech*, 2015, pp. 3214–3218.

[20] D. Povey, A. Ghoshal, G. Boulianne, L. Burget, O. Glembek, N. Goel, M. Hannemann, P. Motlíček, Y. Qian, P. Schwarz, J. Silovský, G. Stemmer, and K. Veselý, "The Kaldi speech recognition toolkit," in *IEEE Automatic Speech Recognition and Understanding Workshop (ASRU)*, 2011.

[21] J. Kong, J. Kim, and J. Bae, "Hifi-GAN: Generative adversarial networks for efficient and high fidelity speech synthesis," *Advances in Neural Information Processing Systems*, vol. 33, pp. 17 022–17 033, 2020.

[22] B. M. L. Srivastava, N. Tomashenko, X. Wang, E. Vincent, J. Yamagishi, M. Maouche, A. Bellet, and M. Tommasi, "Design choices for x-vector based speaker anonymization," in *Interspeech*, 2020, pp. 1713–1717.

[23] B. M. L. Srivastava, M. Maouche, M. Sahidullah, E. Vincent, A. Bellet, M. Tommasi, N. Tomashenko, X. Wang, and J. Yamagishi, "Privacy and utility of x-vector based speaker anonymization," *IEEE/ACM Transactions on Audio, Speech and Language Processing*, vol. 30, pp. 2383–2395, 2022.

[24] X. Wang and J. Yamagishi, "Neural harmonic-plus-noise waveform model with trainable maximum voice frequency for text-to-speech synthesis," in *Speech Synthesis Workshop*, 2019, pp. 1–6.

[25] J. Patino, N. Tomashenko, M. Todisco, A. Nautsch, and N. Evans, "Speaker anonymisation using the McAdams coefficient," in *Interspeech*, 2021, pp. 1099–1103.

[26] S. McAdams, "Spectral fusion, spectral parsing and the formation of the auditory image," Ph.D. dissertation, Stanford University, 1984.

[27] S. Ghorshi, S. Vaseghi, and Q. Yan, "Cross-entropic comparison of formants of British, Australian and American English accents," *Speech Communication*, vol. 50, no. 7, pp. 564–579, 2008.