Automated Anonymisation of Visual and Audio Data in Classroom Studies

Ömer Sümer¹, Peter Gerjets², Ulrich Trautwein¹, Enkelejda Kasneci¹
¹ University of Tübingen
² Leibniz-Institut für Wissensmedien
Tübingen, Germany
{oomer.suemer,ulrich.trautwein,enkelejda.kasneci}@uni-tuebingen.de
p.gerjets@iwm-tuebingen.de

Abstract

Understanding students’ and teachers’ verbal and non-verbal behaviours during instruction may help infer valuable information regarding the quality of teaching. In education research, there have been many studies that aim to measure students’ attentional focus on learning-related tasks: Based on audio-visual recordings and manual or automated ratings of behaviours of teachers and students. Student data is, however, highly sensitive. Therefore, ensuring high standards of data protection and privacy has the utmost importance in current practices. For example, in the context of teaching management studies, data collection is carried out with the consent of pupils, parents, teachers and school administrations. Nevertheless, there may often be students whose data cannot be used for research purposes. Excluding these students from the classroom is an unnatural intrusion into the organisation of the classroom. A possible solution would be to request permission to record the audio-visual recordings of all students (including those who do not voluntarily participate in the study) and to anonymise their data. Yet, the manual anonymisation of audio-visual data is very demanding. In this study, we examine the use of artificial intelligence methods to automatically anonymise the visual and audio data of a particular person.

Introduction

Visual and audio recording of classroom instructions has been widely used in education research for many purposes such as self-reflection, peer collaboration, teacher coaching, or classroom observation research for assessment and evaluation of teaching quality. Besides the traditional approaches in classroom observation and behaviour coding systems, there are recent efforts in multimodal learning analytics that aim to automate these workflows. The progress in the area of machine learning and artificial intelligence have additionally paved the way to conduct classroom studies in large-scale and automate these analyses. Unlike traditional types of data such as questionnaires or written reports, audio-visual recordings of a classroom cannot be easily anonymised as they lose the information which is required for further manual or automated analysis.

A typical practical challenge during such studies is that there may be students who do not want to consent in the study or their data being used by education practitioners. A common approach to overcome this limitation is to reorder the classroom by changing the seats of these persons so they can sit out of the video coverage. However, this constitutes an unnatural intervention in the usual form of classroom organisation. Furthermore, the students who do not participate in the study may raise their hands and actively participate in the ongoing instruction by speaking. Since voice also contains private information, the collection, storage, distribution, and analysis of this kind of data might cause severe violations of data protection laws and regulations.

In fact, the current digital transformation of our society goes along with a corresponding change and regulation of data protection laws. Whereas the US data protection legislation is developing and, in comparison, Germany has the most comprehensive and the first data protection law in the world (Hessen, 1970) in Europe, the General Data Protection Regulation (GDPR) of the European Union came into effect in May 2018. According to DLA Piper, there are also several Asian countries which recently passed data protection laws. There is also an increasing interest in the privacy of personal data, independent of the underlying societal and individual foundations and the scope of regulations.

In August 2019, Sweden issued its first fine to a public board as they used facial recognition technology to keep track of class participation during a few weeks in a pilot study that aimed to automate the class register. Even though the data was collected and stored in local and locked computers without internet connection, according to the Swedish data protection agency, they violated the GDPR in three ways: (i) by processing personal data in a more intrusive manner than what was necessary for the purpose (monitoring of attendance), (ii) processing sensitive personal data without legal basis, and (iii) not fulfilling the requirements of data protection impact assessment and prior consultation. The Swedish ex-
ample shows that even a simple use of visionary technologies may cause data breaches and that data protection in educational situations is highly critical and must be carried out after prior consultation. Contrary to the common understanding that computer vision and machine learning are used to collect and analyse private, personal data, we show that by leveraging these technologies, multimodal data can be efficiently and semi-automatically anonymised.

Let us consider an audio-visual recording of teaching situations at schools, which is typical research means in the field of classroom management since the 1990s. Under the national data protection laws and the GDPR, the current practice is to pseudo-anonymise the questionnaire data (pre- and post-tests). Pseudo-anonymisation of categorical data can be done using code words assigned to students, instead of using their names. However, audio-visual data cannot be easily anonymised because they need to either be watched by education researchers or processed by computer algorithms.

In studies that necessitates audio-visual data collection in the classroom or small group discussions, there may be subjects who do not want to participate in the research. Excluding these students may be impractical and raise other complicated issues. In contrast to longer storage and data processing, we propose to collect and store classroom data for only a short period (a few hours to max. one day). During this time, the collected audio-visual data can be automatically processed, anonymised, and validated immediately.

**Our contributions.** We create a small-scale classroom observation dataset that is composed of 6.5 hours of instruction in varying subjects and show the feasibility of automated anonymisation approaches on audio-visual data. Even though our focus is educational data such as classroom observation recordings our approach is applicable to any other domain of audio-visual data and makes the anonymisation much more effective.

### Related Works

In this section, we will review the previous works that concern data anonymisation. As we mainly aim at audio-visual data anonymisation, our focus will be video and audio.

**Video.** Faces are perhaps the most characteristic features containing private information in video data. In the domain of computer vision, face detection, tracking, and recognition are among the widely studied problems. In the recent years, open and large-scale databases and the progress in the field of deep learning have led to fast and accurate results for face detection, tracking and recognition even under challenging conditions such as occlusion, lightning chances, eyeglasses, or make-up.

In categorical datasets, the injection of noise using differential privacy techniques is the right choice to protect private information (J., Lipton, and Elkan 2014). However, these methods are not suitable for images, and in particular, for face images since the injected noise deteriorates the required face features. Even though it is far from guaranteeing privacy protection, crafting adversarial samples (Goodfellow, Shlens, and Szegedy 2015) on images can at least ensure many trained face recognisers fail on perturbed images. However, the anonymisation of faces is not only addressing privacy protection for face identification algorithms but also face recognition by humans.

In recent years, there have been many successful applications of generative models to anonymise faces, such as adversarial generative networks and variational autoencoders. For example, a face can be swapped with another person’s face to hide the original identity. In (Ren, Jae Lee, and Ryoo 2018), a face modifier network was trained together with adversarial regulariser and an action recognition network, whose task is to recognise the action even in the modified face. In this way, anonymised data can be used to train action recognition models. In contrast, (Hukkelås, Mester, and Lindseth 2019) first filled the face that has to be anonymised with noise and applied then a conditional GAN using these patches and facial keypoints. In this manner, the authors constrained the background and head pose and guaranteed not to have any leakage of private information.

The audio-visual data is used for either automated analysis or manual inspection of behavioural data. We found two drawbacks of anonymisation based on generative models. First, they do not ensure temporally coherent generations and may induce flickering identities in some participants, which distracts the viewer who uses the material for educational purposes. Second, a face that looks like another identity does not guarantee that details in facial expressions are preserved.

In this paper, we are addressing the face in the visual domain. However, beyond faces, there are other features such as hair clothing, and body pose and they may contain private information. In the discussion section, we present how to fulfil different levels of anonymisation.

**Audio.** The task of audio anonymisation aims to identify all intervals of a participant whose voice is audible. This task can be approached using speaker diarisation. In general, diarisation is composed of several sub-tasks such as speaker activity detection, speaker change detection, extraction of an embedding representation and clustering. After having speaker diarisation, we acquire clusters of speaking patterns where each of them belongs to a different participant. Then, a possible way is to ask a human annotator to locate an exemplary of the anonymised person’s voice. Eventually, we can anonymise all parts assigned to the same cluster.

The focus in this field is to develop better embeddings, which in practice can be acquired from the internal representations of speaker recognition networks as in d-vectors (Variani et al. 2014) and (Garcia-Romero et al. 2017). Recently, (Zhang et al. 2019) modelled speakers using multiple instances of a parameter-sharing recurrent neural network. In contrast to previous works based on clustering, they identified different speakers interleaved in time.

Similar to changing faces with a fake identity, there exist various anonymisation approaches in the context of audio analysis. For example, (Fang et al. 2019) extracted speaker identity features from an utterance and synthesised the input by replacing the identity part with a pseudo-identity.
The most important part is to locate the speaking patterns of a person. Later, there are two possible alternatives: either to synthesise the voice by removing private acoustic parameters or directly silence these parts. We prefer the latter one because when they did not give consent to participate in the study, storage of behavioural data would not be an option even by removing identity information. Furthermore, there can be private cues in the content of their speech.

**Approach**

In practice, we have two working scenarios. (i) We are given one or several participants to anonymise their data, and (ii) we are being asked to anonymise all student data except for the teacher’s instruction (e.g. when the teacher’s instruction is used for rhetorical analysis of teacher). Our audio-visual anonymisation workflow is based on multiple machine learning steps and shown in Figure 1. The modalities that contain private information in our application are video and audio (including the spoken information during the conversations in the learning context). Depending on the level of anonymisation expected, there can be varying levels of anonymisation in visual and audio data. In this section, we describe our approach to anonymise faces in the videos and speaking patterns in the audio recordings.

**Anonymising faces.** Videos can be taken from handheld or static cameras. Also, they can contain footage taken from different cameras. The first step is, therefore, to locate shot boundaries and create scenes. To detect shot boundaries, including hard cuts and gradual transitions, we used the TransNet (Soucek, Moravec, and Lokoc 2019) approach, which is based on 3D dilated CNNs.

After detecting shot boundaries, we can define scenes, \( s_i = [I^1, ..., I^{N_i}] \), where each scene \( s_i \) can be in varying length, either a few seconds or minutes. In each scene, we employ the RetinaFace face detector (Deng et al. 2019) which is trained on the WIDER face dataset (Yang et al. 2016). On the contrary to the face detection methods in the literature that require several stages of networks, RetinaFace is trained using multiple losses which combines extra-supervision and self-supervised multitask learning objectives. These additional losses include face classification, bounding box regression, extra supervision of facial landmark regression, and self-supervised mesh decoder for predicting a pixel-wise 3D shape face.

We acquire a set of faces with bounding boxes \( \{[b^1_t, ..., b^N_t], ..., [b^t_1, ..., b^t_n]\} \), where \( t \) is the index of frames that belong to the scene, \( s_i \), and \( n_t \) is a varying number of faces detected in each frame. Either in small groups or traditional classroom formation often students sit in their usual seats and do not change their seats in a scene. Furthermore, the face detector shows very decent performance even under challenging situations, such as motion blur, partial occlusion, or low image resolution. Thus, we employ a location-based tracking approach.

We first calculate the Intersection over Union (IoU) scores between the bounding boxes in the consecutive frames:

\[
s(b_t, b_{t+1}) = \frac{b_t \cap b_{t+1}}{b_t \cup b_{t+1}}
\]

where \( b = [x, y, w, h] \)’s are bounding boxes. Then, we convert the IoU scores to a cost matrix and assign the faces in the current frame to the next one using minimum weight matching in bipartite graphs that is also known as Hungarian algorithm (Kuhn 1955). In this way, we find correspondences that minimize the cost between the detections of consecutive frames. As we maximize the intersection between bounding boxes of the same faces, the IoU scores are negated. Even though a combination of several cost terms (i.e. additionally visual similarity between faces) can yield more reliable tracklets, in practice, we observed that the location cue is enough to create tracklets in classroom scenes.

After having face tracks, we pick only one sample of the person that we want to anonymise and use this sample as a reference for the further face verification steps. Depending on the camera angle and the subjects’ movement, their
head poses may show significant variation. Thus, it is crucial to pick a face track that represents these variations, for instance, the one longer and containing different head poses. As a face embedding, we use the Inception ResNet (V1) trained minimizing Triplet loss (Schroff, Kalenichenko, and Philbin 2015) on the VGGFace2 dataset (Cao et al. 2018). Embedding vectors are $L_2$ normalised and their dimension is 512. To acquire the similarity of any face tracks in the video with respect to our reference, we use cosine similarities between them:

$$score = \min \frac{F(I(b_i,t_i)) \cdot F(I(b_j,t_j))}{||F(I(b_i,t_i))|| \cdot ||F(I(b_j,t_j))||}$$ (2)

where $F(\cdot)$ is the face embedding, $I(b_i,t_i) \in \mathcal{T}_{test}$ and $I(b_j,t_j)$ is any face track from the same video where we want to find a specific subject whose face has to be anonymised. Eventually, we threshold the cosine similarity scores to retrieve query identity and either make these faces blurry or set them to black.

**Finding speaking patterns.** Similar to the face information, human voice also contains biometric traits. The main task in our context is to find the speaking patterns of a participant whose data has to be anonymised. We use the Unbounded Interleaved-State Recurrent Neural Network (UIS-RNN) (Zhang et al. 2019) to diarise speaking patterns of different speakers.

An unbounded RNN network, the UIS-RNN, fed with d-vectors that is extracted from equal-length audio segments. The number of speakers is decided using a Bayesian non-parametric process, and different speakers are modelled within the states of RNN in the time domain. As the UIS-RNN approach performed better than k-means and Spectral Clustering of d-vectors on benchmark datasets, we address speaker diarisation using a pre-trained UIS-RNN model.

When we apply diarisation to classroom data, we deploy the speaker diarisation to the spectrograms of the entire classroom recordings. Subsequently, we show these clustered audio parts to annotators together with the original video and ask them to pick the cluster to be anonymised.

**Experimental Results**

In order to test the feasibility of the automated anonymisation in classroom observation videos, we first created a collection of classroom observation videos from YouTube. These videos are either recorded from a static point or using handheld cameras and contain shot transitions. More specifically, the video material consists of 18 classroom instruction videos, where the taught topics include English language arts, maths, and social studies. The total duration of this instruction material is approximately 6.5 hours. All videos are available in the resolution of 1280x720px. Sample keyframes are depicted in Figure 2.

When we apply diarisation to classroom data, we deploy the speaker diarisation to the spectrograms of the entire classroom recordings. Subsequently, we show these clustered audio parts to annotators together with the original video and ask them to pick the cluster to be anonymised.

![Figure 2: Snapshots from the classroom observation videos.](image)

![Figure 3: Face verification results on classroom observation videos: Precision vs. Recall and ROC curves.](image)
Discussion and Future Outlook

In this section, we first describe the levels of data anonymisation in classroom studies, summarise our key findings and give an outlook on our future work in this context.

Different levels of data anonymisation

We focus on the automated anonymisation of video (faces) and audio data in the educational context. In practice, the level of data anonymisation and needed modalities may vary. In this part, we first address the modalities in detail and then propose different levels of anonymisation.

**Questionnaires.** Many educational studies, including the ones that require video recording, use questionnaires. They may contain questions regarding personal information, educational, or socio-economical background of students. Particularly personal data, such as biometric data, rate, ethnicity, and political opinion requires the highest level of protection. The most common approach to this challenge is pseudonymisation.

It should be noted, however, that the pseudonymised data may still be vulnerable to re-identification and remains therefore personal. In order to prevent re-identification, differential privacy is the current practice (Francis 2019) and should be applied not only to data of specific participants who do not want to participate in the study, but to be considered for all participants.

**Video.** Faces in the videos are the primary modality that contains personal information. Therefore, our focus here was on finding and anonymising faces. However, there are other soft biometric traits (Jain, Dass, and Nandakumar 2004) which may require anonymisation. Some examples are hair colour, body posture, and gesture patterns. When the face of an anonymised person is detected and recognised, hair can be occluded, for example by extending the face bounding box around and top of the face.

So far, we did not consider body and gestures in our analysis since this can be done by employing human pose estimation. In case of a classroom recording including approximately 20 students, deploying a multi-person pose estimation method can considerably increase the processing time. However, we will exploit this issue in our future work.

**Audio.** In our analysis, we tested speaker diarisation. Notably, the audio domain requires a more thorough understanding of the spoken conversation. For instance, even if we anonymised face and speaking patterns of a participant, other participants may talk about the anonymised person or content. In order to address this issue, we need a semantic understanding of the spoken text using speech-to-text approaches and efficient search techniques for the information relevant to selected keywords on the entire data.

In a manner that each level contains the anonymisation of previous modalities, we can categorise the varying levels of anonymisation for classroom studies as follows:

1. Pseudonymisation of questionnaires and personal data,
2. Anonymisation of hard biometric traits such as faces in the video and speaking time,
3. Anonymisation of soft biometric traits such as body posture, gestures, and hair appearance,
4. Anonymisation of the spoken information during the instruction unit (either by anonymised participants or other persons) such as students’ and school’s name or location.

The appropriate level of anonymisation can be chosen according to the nature of the data and institutional board review approval regarding ethical aspects of data collection, storage and processing.

We can summarise the key findings of our work as follows:

- We created a small classroom observation dataset that is representative of typical scenarios in educational studies.
- We investigated the feasibility of automated anonymisation on visual and audio domains. The essential modality on the visual domain is anonymisation of faces, for which we showed that it could be solved in the context of classroom observation data at high accuracy. Similarly, a speaker diarisation approach helps to find speaking clusters and those parts in the audio signal belonging to pointing to participants that have to be anonymised.

As it is the case in most vision and machine learning applications, none of the methods can guarantee completely accurate predictions. Furthermore, the owner of the data will be ethically and legally responsible for the proper and accurate anonymisation of the visual and audio modalities. Our proposed approach can be seen as an alternative to speed up anonymisation in a way that requires only quick manual inspection and correction.

For further manual inspection, we can export the output of face identification and speaker diarisation results in a compatible format with common multimedia annotation tools such as the VGG Image Annotator (Dutta and Zisserman 2019) or the ELAN software (Sloetjes and Wittenburg 2008).

In future work, we plan to create a simple interface that is compatible with available multimedia annotation tools and can be used by educational practitioners without any technical experience and to conduct a user study on real multimodal collection and analysis process of educational data.

Acknowledgements Ömer Sümer is a doctoral student at the LEAD Graduate School & Research Network (GSC1028), funded by the Excellence Initiative of the German federal and state governments. This work is also supported by Leibniz-WissenschaftsCampus Tübingen “Cognitive Interfaces”.

References

[Cao et al. 2018] Cao, Q.; Shen, L.; Xie, W.; Parkhi, O. M.; and Zisserman, A. 2018. Vggface2: A dataset for recognising faces across pose and age. In International Conference on Automatic Face and Gesture Recognition.

[Deng et al. 2019] Deng, J.; Guo, J.; Zhou, Y.; Yu, J.; Kotsia, I.; and Zafeiriou, S. 2019. Retinaface: Single-stage dense face localisation in the wild. CoRR abs/1905.00641.

[Dutta and Zisserman 2019] Dutta, A., and Zisserman, A. 2019. The VIA annotation software for images, audio and video. In Proceedings of the 27th ACM International Conference on Multimedia, MM ’19. New York, NY, USA: ACM.

[Fang et al. 2019] Fang, F.; Wang, X.; Yamagishi, J.; Echizen, I.; Todisco, M.; Evans, N.; and Bonastre, J.-F. 2019. Speaker anonymization using X-vector and neural waveform models. In ISW 2019, 10th ISCA Speech Synthesis Workshop, 20-22 September 2019, Vienna, Austria.

[Francis 2019] Francis, M. R. 2019.

[Garcia-Romo et al. 2017] Garcia-Romo, D.; Snyder, D.; Sell, G.; Povey, D.; and McCree, A. 2017. Speaker diarization using deep neural network embeddings. In 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 4930–4934.

[Goldberg et al. 2019] Goldberg, P.; Sümer, Ö.; Stürmer, K.; Wagner, W.; Göllner, R.; Gerjets, P.; Kasneci, E.; and Trautwein, U. 2019. Attentive or not?: Toward a machine learning approach to assessing students’ visible engagement in classroom instruction. Educational Psychology Review.

[Goodfellow, Shlens, and Szegedy 2015] Goodfellow, I.; Shlens, J.; and Szegedy, C. 2015. Explaining and harnessing adversarial examples. In International Conference on Learning Representations.

[Helmke 1992] Helmke, A. 1992. Selbstvertrauen und schulishe Leistungen. Hogrefe.

[Hoel and Chen 2018] Hoel, T., and Chen, W. 2018. Privacy and data protection in learning analytics should be motivated by an educational maxim—towards a proposal. Research and Practice in Technology Enhanced Learning 13(1):20.

[Hukkelås, Mester, and Lindseth 2019] Hukkelås, H.; Mester, R.; and Lindseth, F. 2019. Deeper privacy: A generative adversarial network for face anonymization. In Bebis, G.; Boyle, R.; Parvin, B.; Koracin, D.; Ushizima, D.; Chai, S.; Sueda, S.; Lin, X.; Lu, A.; Thalmann, D.; Wang, C.; and Xu, P., eds., Advances in Visual Computing, 565–578. Cham: Springer International Publishing.

[Jain, Dass, and Nandakumar 2004] Jain, A. K.; Dass, S. C.; and Nandakumar, K. 2004. Soft biometric traits for personal recognition systems. In Zhang, D., and Jain, A. K., eds., Biometric Authentication, 731–738. Berlin, Heidelberg: Springer Berlin Heidelberg.

[Ji, Lipton, and Elkan 2014] Ji, Z.; Lipton, Z. C.; and Elkan, C. 2014. Differential privacy and machine learning: a survey and review. CoRR abs/1412.7584.

[Kuhn 1955] Kuhn, H. W. 1955. The Hungarian Method for the Assignment Problem. Naval Research Logistics Quarterly 2(1–2):83–97.

[Ren, Jae Lee, and Ryoo 2018] Ren, Z.; Jae Lee, Y.; and Ryoo, M. S. 2018. Learning to anonymize faces for privacy preserving action detection. In The European Conference on Computer Vision (ECCV).

[Schroff, Kalenichenko, and Philbin 2015] Schroff, F.; Kalenichenko, D.; and Philbin, J. 2015. Facenet: A unified embedding for face recognition and clustering. In 2015 IEEE Conference on Computer Vision and Pattern Recognition, Vancouver, Canada.
Recognition (CVPR), 815–823. Los Alamitos, CA, USA: IEEE Computer Society.

[Sloetjes and Wittenburg 2008] Sloetjes, H., and Wittenburg, P. 2008. Annotation by category: ELAN and ISO DCR. In Proceedings of the Sixth International Conference on Language Resources and Evaluation (LREC’08). Marrakech, Morocco: European Language Resources Association (ELRA).

[Soucek, Moravec, and Lokoc 2019] Soucek, T.; Moravec, J.; and Lokoc, J. 2019. Transnet: A deep network for fast detection of common shot transitions. CoRR abs/1906.03363.

[Sümer et al. 2018] Sümer, O.; Goldberg, P.; Sturmer, K.; Seidel, T.; Gerjets, P.; Trautwein, U.; and Kasneci, E. 2018. Teachers’ perception in the classroom. In The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops.

[Swedish Data Protection Authority 2019] 2019. Supervision pursuant to the general data protection regulation (eu) 2016/679 – facial recognition used to monitor the attendance of students. https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf.

[Variani et al. 2014] Variani, E.; Lei, X.; McDermott, E.; Moreno, I. L.; and Gonzalez-Dominguez, J. 2014. Deep neural networks for small footprint text-dependent speaker verification. In Proc. ICASSP.

[Yang et al. 2016] Yang, S.; Luo, P.; Loy, C. C.; and Tang, X. 2016. Wider face: A face detection benchmark. In CVPR.

[Zhang et al. 2019] Zhang, A.; Wang, Q.; Zhu, Z.; Paisley, J.; and Wang, C. 2019. Fully supervised speaker diarization. In ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 6301–6305.