Poster Abstract: Privacy-Preserving Data Augmentation for Thermal Sensation Dataset Based on Variational Autoencoder

Hiroki Yoshikawa
Kyoto Tachibana University
Kyoto, Japan
yoshikawa-h@tachibana-u.ac.jp

Akira Uchiyama
Osaka University
Osaka, Japan
uchiyama@ist.osaka-u.ac.jp

ABSTRACT

Machine learning-based methods show high performance in estimating the thermal sensation of a person. These methods are based on a huge amount of personal data. The dataset used for the training of the estimator includes personal physiological data, which includes people’s private information. Generative models have received significant attention to anonymize such data, including private information. In this paper, we propose privacy-preserving data augmentation for the thermal sensation dataset, including the subject’s physiological data using Variational Autoencoder. The generative model trained with a thermal sensation dataset collected in the uncontrolled environment tends to be biased because subjects in the environment rarely report extreme thermal sensation labels. To tackle this problem, we introduce a weighted loss function for the generative model to mitigate the bias of the thermal sensation labels. The evaluation result shows that our method generates an anonymized dataset that works to train a thermal sensation estimator as well as the original dataset.

CCS CONCEPTS

• Information systems → Information integration; • Computing methodologies → Machine learning algorithms.

KEYWORDS

Data Augmentation, Data Anonymization, Thermal Sensation

ACM Reference Format:

Hiroki Yoshikawa and Akira Uchiyama. 2022. Poster Abstract: Privacy-Preserving Data Augmentation for Thermal Sensation Dataset Based on Variational Autoencoder. In The 9th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation (BuildSys ’22), November 9–10, 2022, Boston, MA, USA. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3563357.3567747

1 INTRODUCTION

Machine learning-based methods attract the interest of researchers working on thermal sensation estimation. These methods achieve high performance in estimating personal thermal sensation using a huge amount of personal data collected by multiple subjects. The dataset used to train the estimator contains personal data such as physiological data. Physiological data includes the user’s personal information that can be used to identify the user. Therefore, some people may refuse to participate in data collection. In order to preserve privacy, a federated learning-based method is proposed for thermal comfort management [Khalil et al. 2022]. On the other hand, generative models such as Autoencoder and Generative Adversarial Networks have received significant attention to anonymize data collected by subjects for electric health records [Venugopal et al. 2022] and facial images [Wu et al. 2019]. The frameworks can preserve the data in any organization because they can communicate and integrate the anonymized dataset, contrary to federated learning-based methods. This feature enhances the availability of the dataset as open data. However, a thermal sensation vote (TSV) dataset collected in uncontrolled environments tends to be biased because subjects in such an environment rarely report extreme thermal sensations. This aspect of TSV causes an imbalance between the number of samples in different classes. Also, the imbalance of the ground truth labels causes biased generation by the generative model. Because of that, the application of the generative model to the TSV dataset becomes challenging.

This paper proposes a privacy-preserving data augmentation for the thermal sensation dataset containing the subject’s physiological data using Variational Autoencoder (VAE). As mentioned above, TSV datasets collected in uncontrolled environments tend to be biased, which may cause biased generation. To tackle it, we introduce a weighted loss function in the generative model to mitigate the effect of the class imbalance. The evaluation results show that we have successfully generated an anonymized dataset that works like the original dataset for training a thermal sensation estimator.

2 METHOD

We use VAE to generate the dataset to train TSV estimator. The architecture of the VAE is shown in Fig. 1. An encoder and decoder construct the VAE. Both of them have three parts. Each part includes
a fully connected layer and a rectified linear unit layer. We change the number of parameters $N_1$, $N_2$, $N_3$ in the Section 3.

To train the generative model based on VAE, we use a weighted loss function for VAE as below.

$$L = \left( \frac{1}{N} \sum_{x \in \{X, y\}} (x - \hat{x})^2 \right) \cdot W(x) + (KL \_Divergence).$$

where $N(x)$ is the number of samples in class $c(x \in c)$. $|samples|$ is the number of samples in the training data, and $|classes|$ is the number of classes in Ref. [Yoshikawa et al. 2021a].

### 3 EVALUATION

For the evaluation, we use data collected in an uncontrolled environment. The dataset was obtained using TSVNet [Yoshikawa et al. 2021b]. This dataset was collected for a total of 123 days from 21 subjects in static and dynamic environments. The subjects also reported their thermal sensation using ASHRAE 7-point thermal scale. Although opportunistic and time-series features are used in TSVNet, we use only the opportunistic features because we cannot directly input the time-series features to the proposed model. In addition, we merged the hot/cold, warm/cool, and slightly warm/slightly cool samples into the warm/cool samples because of the lack of rare samples. Therefore, we converted TSV labels into three classes, i.e., warm, neutral, and cool.


![Figure 2: Evaluation setting.](image)

Fig. 2 shows the evaluation setting. We split the original dataset into the data for training and testing at a ratio of 7:3. Based on the preliminary experiment, we determine that the best parameters of $N_1$, $N_2$, and $N_3$ are 32, 8, and 8, respectively. First, we evaluate the performance of anonymization. We train an estimator of subject ID based on random forest classifier using the data for training extracted from the original dataset. The evaluation result is shown in Table 1. We found our method succeeds in anonymizing the

| Dataset for testing |原データ | 生成データ |
|---------------------|---------|-----------|
| Accuracy            | 0.63    | 0.06      |
| F1-score            | 0.65    | 0.02      |


| Dataset for training | 原データ | 生成データ |
|----------------------|---------|-----------|
| Accuracy             | 0.59    | 0.61      |
| F1-score             | 0.55    | 0.48      |

21 subjects because the estimation accuracy and macro-averaged F1-score using the generated dataset are 0.06 and 0.02, respectively. Second, we evaluate the performance of TSV estimation with the generated dataset. In this evaluation, we compare the performance of the TSV estimators trained using the original data and the generated data. The result is shown in Table 2. We found a slight increase of accuracy and slight decrease of macro-averaged F1-score of TSV estimation. Therefore, our method succeeds anonymization with a slight decrease of the quality of the data for TSV estimation.

### 4 CONCLUSION

In this paper, we propose a privacy-preserving data augmentation method for TSV dataset based on VAE with a weighted loss function. We evaluated the performance of our data augmentation method from two aspects, i.e., subjects’ anonymity and the quality of the generated dataset for TSV estimation. The result shows that our method keeps the performance of the estimator of TSV with the generated dataset, which is anonymized using VAE.

### ACKNOWLEDGMENTS

This work was supported by JSPS KAKENHI Grant Number 21K21297 and 22K17885.

### REFERENCES

Mayasaa Khalil, Moez Esseghir, and Leila Merghem-Boulahia. 2022. A federated learning approach for thermal comfort management. Advanced Engineering Informatics 52 (2022), 101526. [https://doi.org/10.1016/j.aei.2022.101526](https://doi.org/10.1016/j.aei.2022.101526)

Diederik P. Kingma and Max Welling. 2014. Auto-Encoding Variational Bayes. In Proceedings of the 2nd International Conference on Learning Representations (ICLR) 2014. [https://doi.org/10.48550/arXiv.1312.6114](https://doi.org/10.48550/arXiv.1312.6114)

Rohit Venugopal, Noman Shafqat, Ishwar Venugopal, Benjamin Mark John Tillbury, Harry Demetrios Stafford, and Aikaterini Bourazeri. 2022. Privacy preserving Generative Adversarial Networks to model Electronic Health Records. Neural Networks 153 (2022), 339–348. [https://doi.org/10.1016/j.neunet.2022.06.022](https://doi.org/10.1016/j.neunet.2022.06.022)

Yifan Wu, Fan Yang, Yong Xu, and Haibin Ling. 2019. Privacy-Protective-GAN for Privacy Preserving Face De-Identification. Journal of Computer Science and Technology 34 (2019), 47–60. [https://doi.org/10.1007/s11390-019-1898-8](https://doi.org/10.1007/s11390-019-1898-8)

Hiroki Yoshikawa, Akira Uchiyama, and Teruo Higashino. 2021a. Data Balancing for Thermal Comfort Datasets Using Conditional Wasserstein GAN with a Weighted Loss Function. In Proceedings of the 8th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation (Coimbra, Portugal) (BuildSys 22). 264–267. [https://doi.org/10.1145/3456611.3491132](https://doi.org/10.1145/3456611.3491132)

Hiroki Yoshikawa, Akira Uchiyama, and Teruo Higashino. 2021b. TSVNet: Combining Time-Series and Opportunistic Sensing by Transfer Learning for Dynamic Thermal Sensation Estimation. IEEE Access 9 (2021), 102835–102846. [https://doi.org/10.1109/ACCESS.2021.3097882](https://doi.org/10.1109/ACCESS.2021.3097882)