Anonymization for Skeleton Action Recognition

Saemi Moon*,[1] Myeonghyeon Kim*,[2] Zhenyue Qin,[3,4] Yang Liu,[3] Dongwoo Kim[1]

POSTECH[1], Scatter Lab[2], ANU[3], Tencent[4], *equal contribution

1. Introduction

Why Skeleton data for Action Recognition?

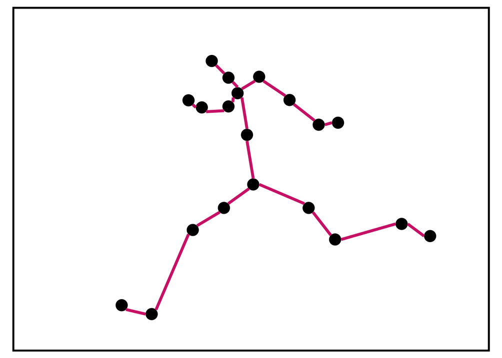
For action recognition application, it must ensure that private information is not abused before and after the analysis

<RGB video>

Action information
- Kick the ball

Private information
- Male
- Son Heung-min

<Skeleton data>



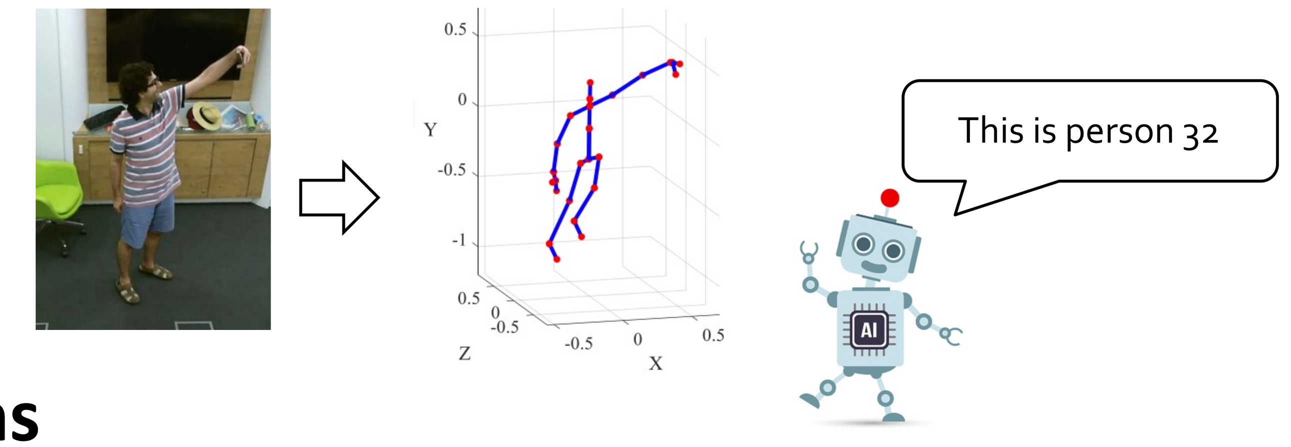
Action information
- Kick the ball

Private information
- ?
- ?

RGB video inevitably exposes private information, while skeleton data can protect sensitive information such as gender or age

Our Motivation

However, we raise a question about the privacy-safeness of skeleton datasets



Contributions

- We empirically show potential privacy leakage from skeleton datasets
- We propose a minimax framework for the skeleton anonymization model

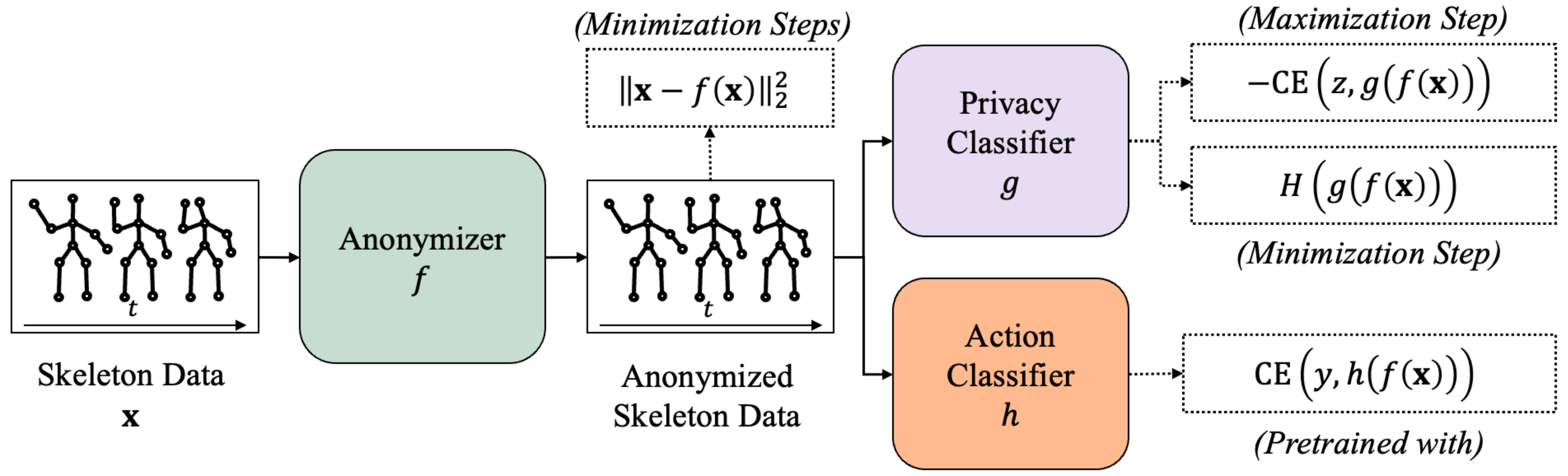
2. Privacy Leakage

The privacy information can be easily predicted by a classification model trained with private labels

	Re-identification Top-1	Re-identification Top-5	Gender Accuracy
Shift-GCN	$79.62_{\pm.70}$	$96.81_{\pm.09}$	$85.99_{\pm.40}$
MS-G3D	$82.23_{\pm.87}$	$97.51_{\pm.07}$	$87.90_{\pm.17}$
2s-AGCN	$76.89_{\pm1.83}$	$96.56_{\pm.32}$	$86.43_{\pm.47}$

3. Method

We propose an anonymization framework based on adversarial learning to protect potential privacy leakage from the skeleton dataset.



Anonymizer f

- Make anonymized skeleton data confuse privacy classifier g
- Make anonymized skeleton data preserve performance of the action classifier h
- Make anonymized skeleton data not very different from original skeleton data

(minimization step)

$$\min_{\theta} \mathbb{E}\Big[\mathrm{CE}(y, h_\psi(f_\theta(\vec{x}))) - \alpha \mathrm{H}(z, g_\phi(f_\theta(\vec{x}))) + \beta\|\vec{x} - f_\theta(\vec{x})\|_2^2\Big]$$

Use entropy to avoid inferring the true label issue

Privacy classifier g

- Train to classify the privacy information of anonymized skeleton data correctly

(maximization step)

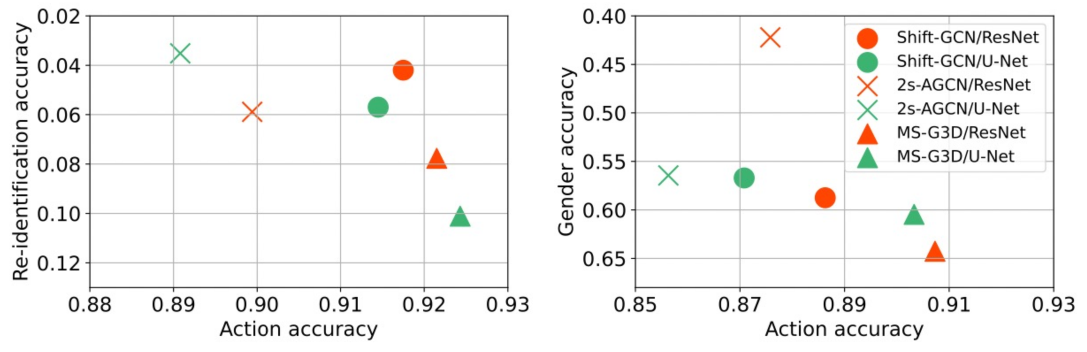
$$\max_{\phi} \mathbb{E}\Big[-\alpha\, \mathrm{CE}(z, g_\phi(f_\theta(\vec{x})))\Big]$$

Action classifier h

- Use a pre-trained action classifier and fix the parameters during training
- The fixed action classifier constrains the anonymized skeleton compatible with the pre-trained model

4. Anonymization Analysis

Anonymization Results



(a) Re-identification task (b) Gender classification

We can dramatically decrease the privacy accuracy while minimally sacrificing the action recognition accuracy

Comparison with Alternative Approaches

Method		Action.	Iden.
Not-anonymized		0.9510	0.8095
Random noise	$\sigma = 0.001$	0.7565	0.7450
	$\sigma = 0.005$	0.4430	0.3240
	$\sigma = 0.010$	0.2660	0.1735
	$\sigma = 0.020$	0.1265	0.1020
	$\sigma = 0.050$	0.0455	0.0840
	$\sigma = 0.100$	0.0450	0.0715
Adversarial attack	Attacked	0.9435	0.0000
	Non-Attacked	0.9435	0.3621
Our method		0.9175	0.0420

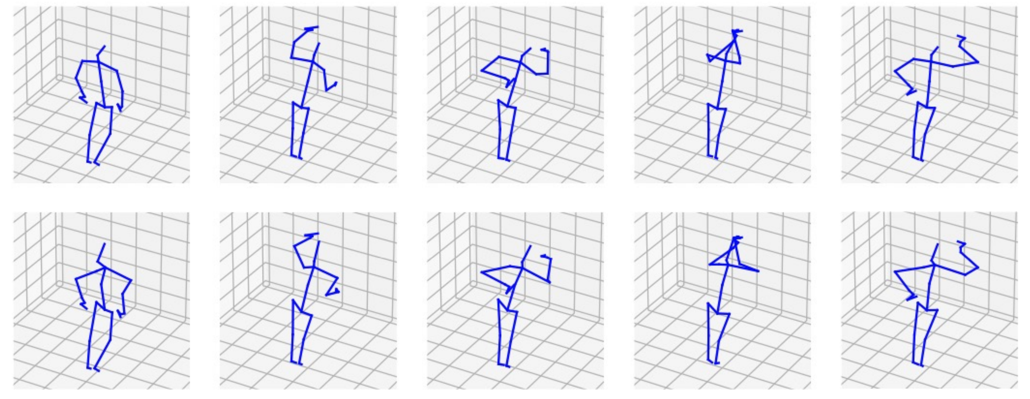
[1] Wang et al, Understanding the Robustness of Skeleton-based Action Recognition under Adversarial Attack, CVPR 2021

- Random noise: randomly inject white noise into the original skeleton
  → Can't preserve action information while reducing privacy leakage
- Adversarial attack: attack privacy information
  → Model-specific, difficult to generalize to unseen models
- Our method: performs well with any pre-trained model

Qualitative Analysis

Original

Gender Anonymized



<"Wiping face with a towel" from elderly female>

5. Takeaways

- We investigate privacy leakage from publicly available skeleton datasets
- We propose an anonymization skeleton framework at first
- Our experimental results reveal that our method effectively removes the privacy information while preserving the movement patterns