MEIJI UNIVERSITY

No anonymity in metaverse: VR user identification based on DTW distance of head-and-arms motions

Koki Miura and **Hiroaki Kikuchi**

Meiji University, Tokyo

Background

- VR space = metaverse

出典『メタバース進化論』

Issue in Metaverse

- *Anonymity*
  - ❑freedom of expression
  - ❑creative experimentation
  - ❑privacy-conscious participation

True

=

- Users are assumed to be unidentifiable.

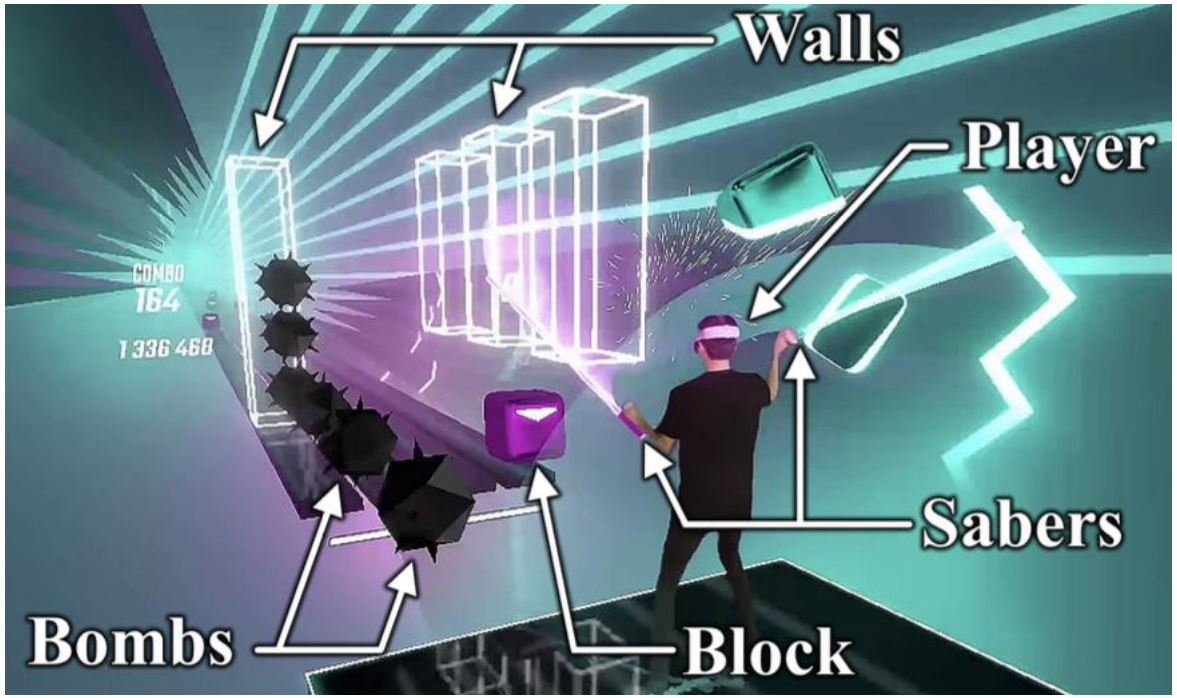
Bogus!

Related works

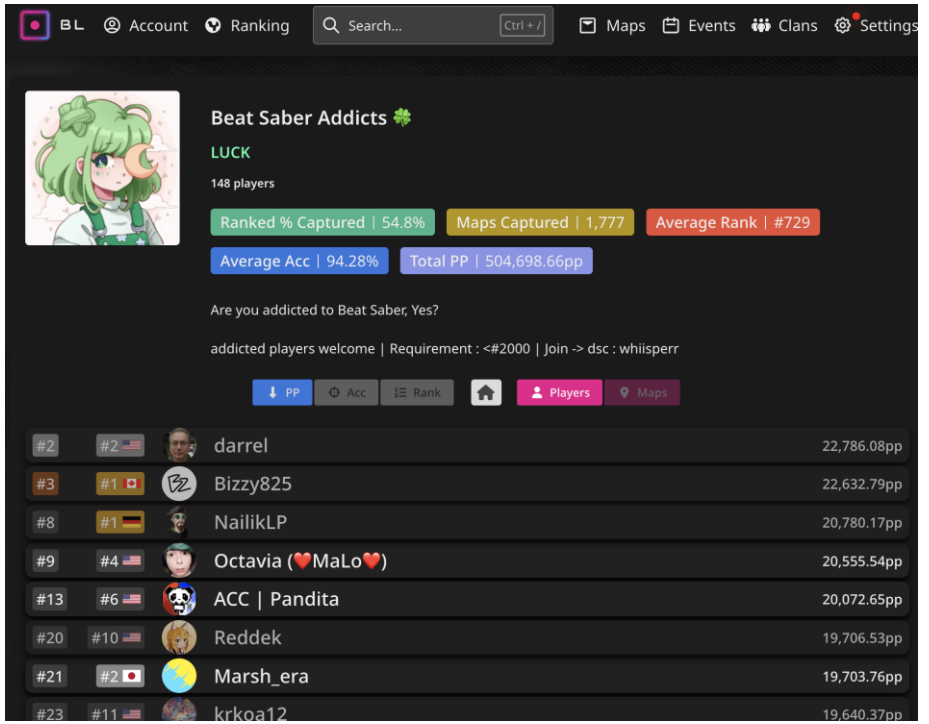
- Hierarchical classification model [Nair+, Usenix2023]
  - 50,000 VR users in "Beat Saber" are identified accurately (73%) in 10 seconds.
- Multi-class classification [Liebers+, VRST 2023]
  - Stability over time, using random forest model with 72 statistical features of movements of HMD and hand controllers.

- Vivek Nair and Wenbo Guo, Justus Mattern, Rui Wang , James F. O'Brien, Louis Rosenberg, Dawn Song, "Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data", the 32nd USENIX Security Symposium, pp.895-910, USENIX, 2023.
- Jonathan Liebers and Christian Burschik, Uwe Gruenefeld, Stefan Schneegass, "Exploring the Stability of Behavioral Biometrics in Virtual Reality in a Remote Field Study", Virtual Reality Software and Technology 2023, pp.1-12, VRST, 2023.

Beat Saber – popular rhythm-based game



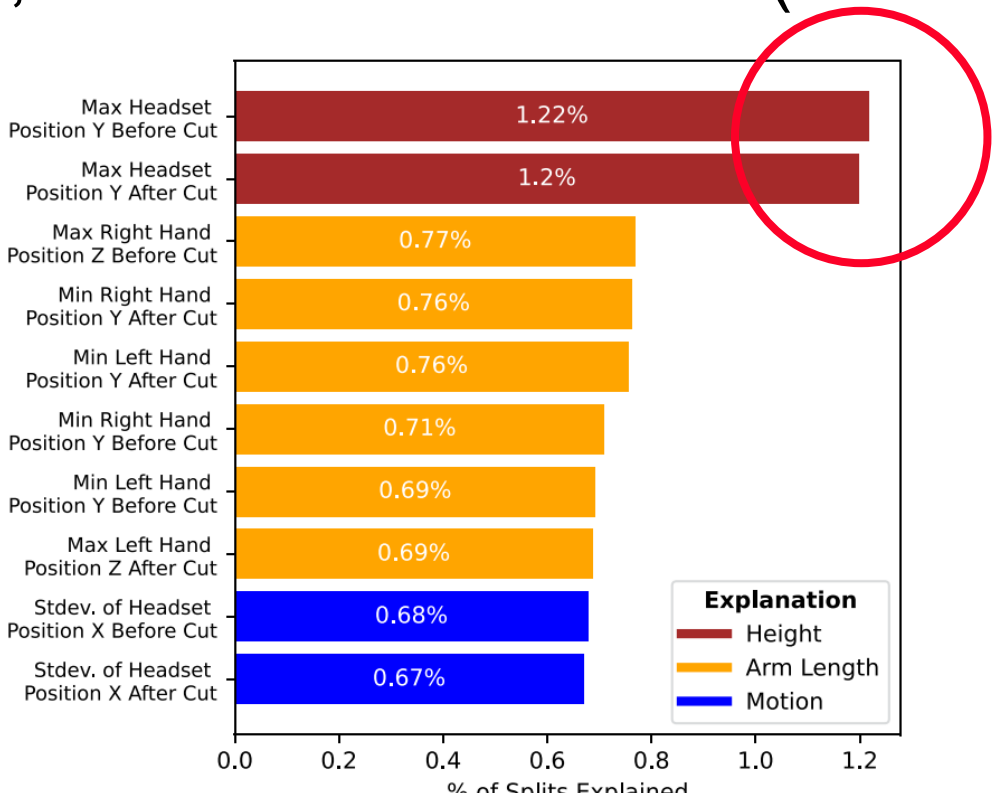
Beat Saber



Beat Leader – leader board of 50,000 users

Limitations of Nair et al.'s work

- Identification on Static features
  - The most influential features used for identification were static, e.g., Y-coordinate of HMD (= a user's height)

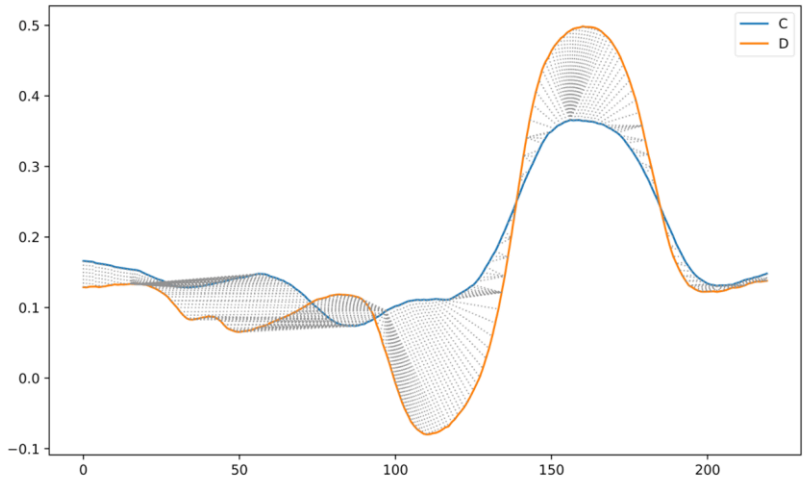


Our objective

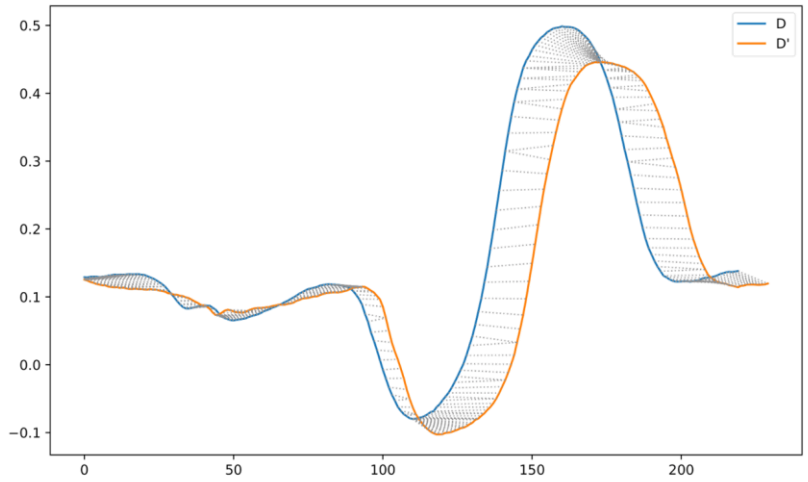
- Goal
  - A VR user identification focuses on dynamic rather than static features.
  - An improvement in the accuracy of SOTA VR methods.
  - A more stable and resilient metric in long-term observation.

Our approach

- Dynamic Time Warping (DTW)
  - A measure of the similarity between time series data.



DTW distance between subject C and D (X-coordinate of right-hand movement)



DTW distance between two movements of the same person (subject D)

Imposter 50.48 > genuie15.68

DTW distance

- Definition
  - Distance d(P,Q) between time series data P = (p_1,..,p_{np}) and Q = (q_1,…,q_{nq}), where np ≠ nq and f(i,j) is defined as

$$f(i,j) = \|p_i - q_j\| + \min \left\{ \begin{array}{l} f(i,j-1), \\ f(i-1,j), \\ f(i-1,j-1) \end{array} \right\}$$

with initial f(0,0) = 0, f(i,0) = f(0,j) = ∞ .

Proposed Algorithm

- Require: A set of n users with VR devices
  - 1. (Template) For each user i = 1,..,n, we measure a motion data y_i, consisting of 3D coordinates of the HMD and both hand controllers.
  - 2. (Identification) Given a new motion data x_j for some (unknown) user j, we compute the DTW distance between x_j and each of the n reference template y_i and identify one with the smallest DTW distance, as

$$j^* = \underset{i \in \{1,\ldots,n\}}{\operatorname{argmin}} d(y_i, x_j)$$

Our questions

- RQ1. Which is a higher risk to user identifiability, the proposed method with dynamic features or the conventional one with static features?
- RQ2. Are there any task performed periodically and involved with individual differences?

Our experiments

- Experiment 1 (Four beat)
  - 12 subjects perform conducting gesture, in 2024.
  - 6 trials = 2 test + 4 references.
- Experiment 2 (Beat Saber)
  - Single-session training.
  - Multi-sessions training. (N=8)
  - Compared with Liebers [2] (Random Forest)

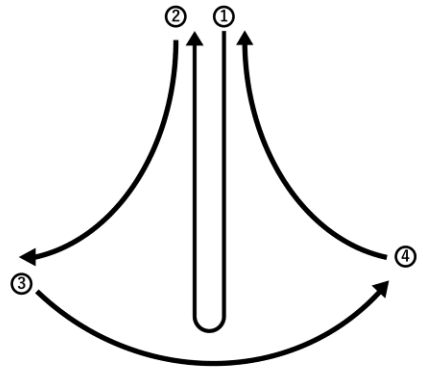


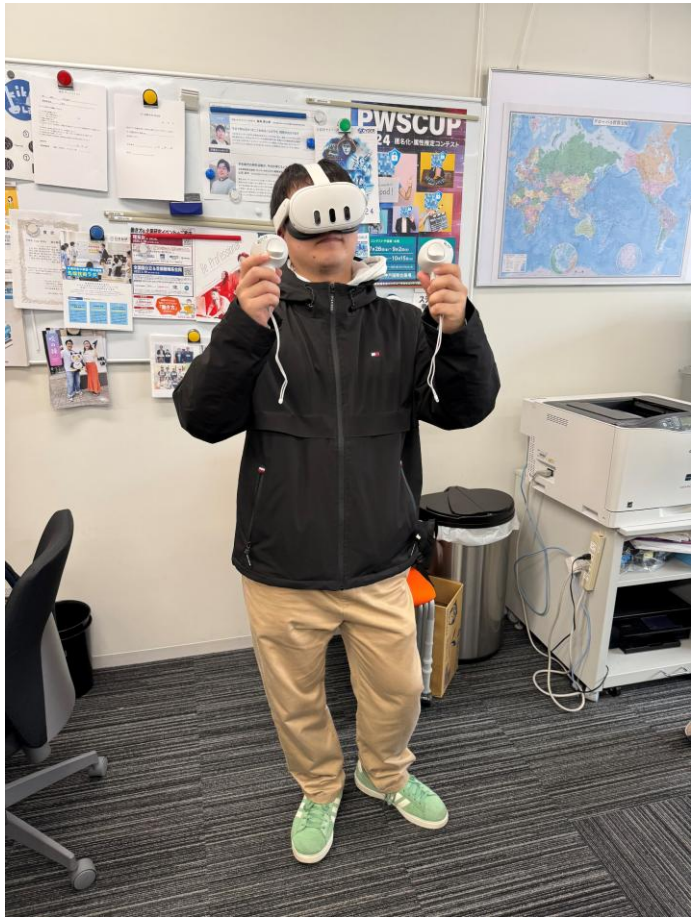
Table 1: Experiment Environment

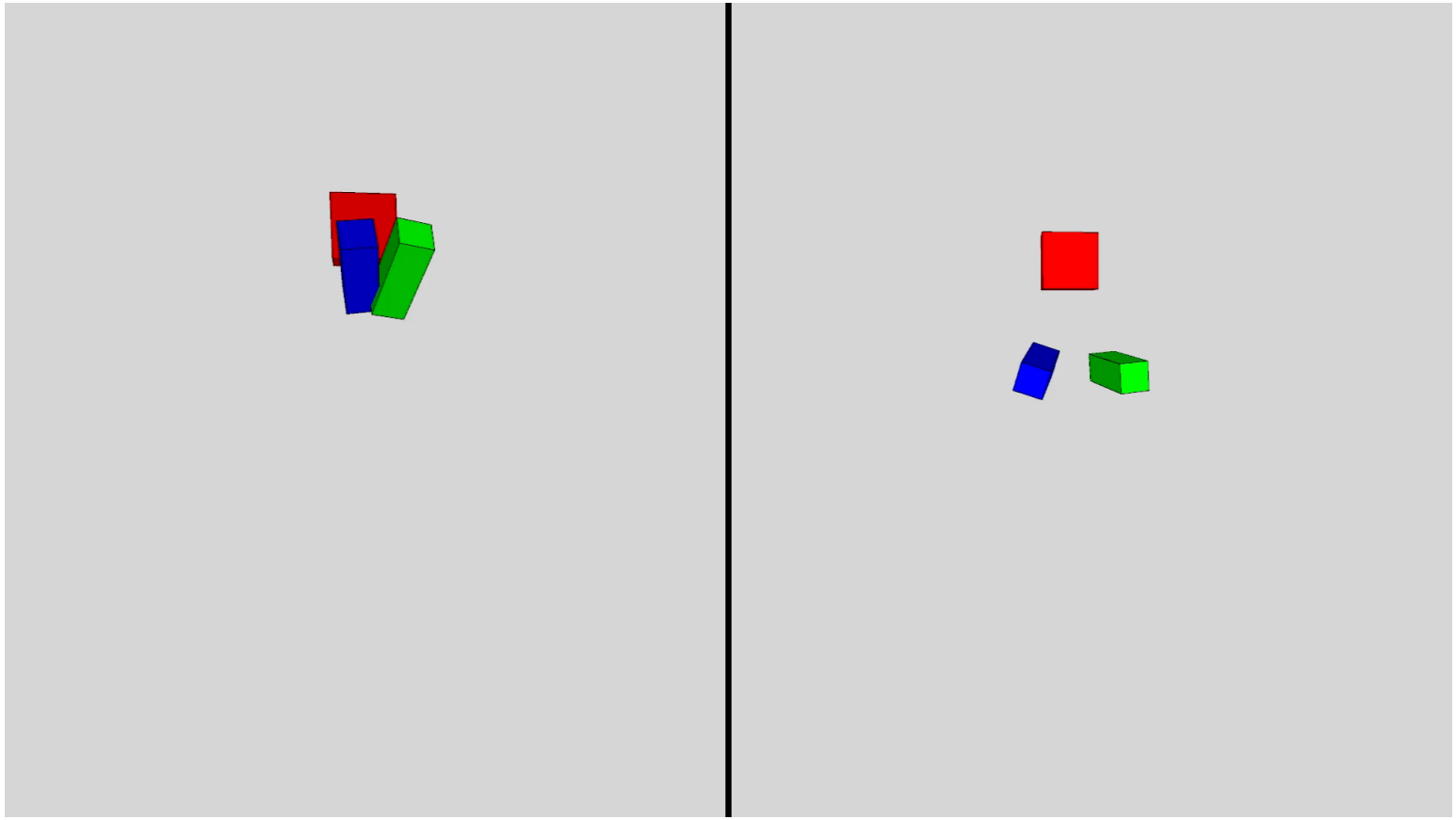
item	value
VR device	Meta Quest 3
development	Unity 2022.3.28f1
sampling rate	72 frame per second [fps]

Table 2: Subjects

item	value
age	20—50 years old
gender	11 male and 1 female
total	12

Sample task



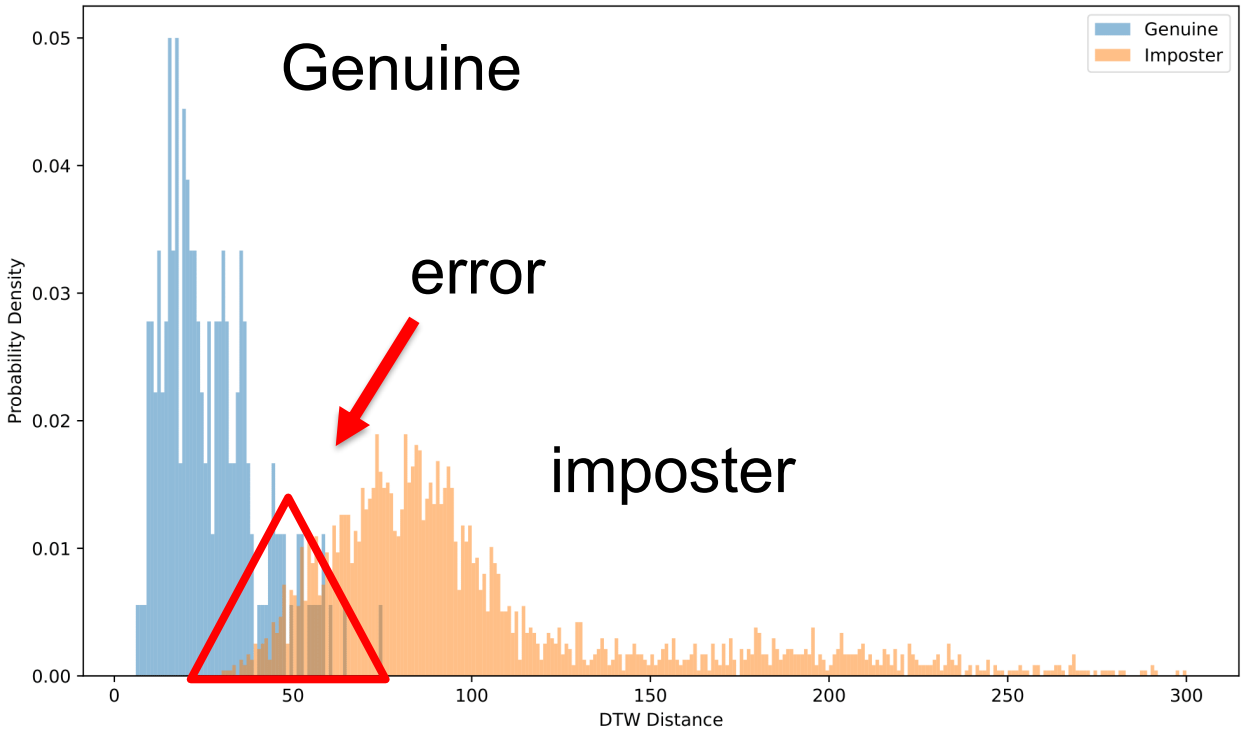


Subject A

A

B

Result 1: DTW dist.



Distribution of DTW distance

Statistics of # flams

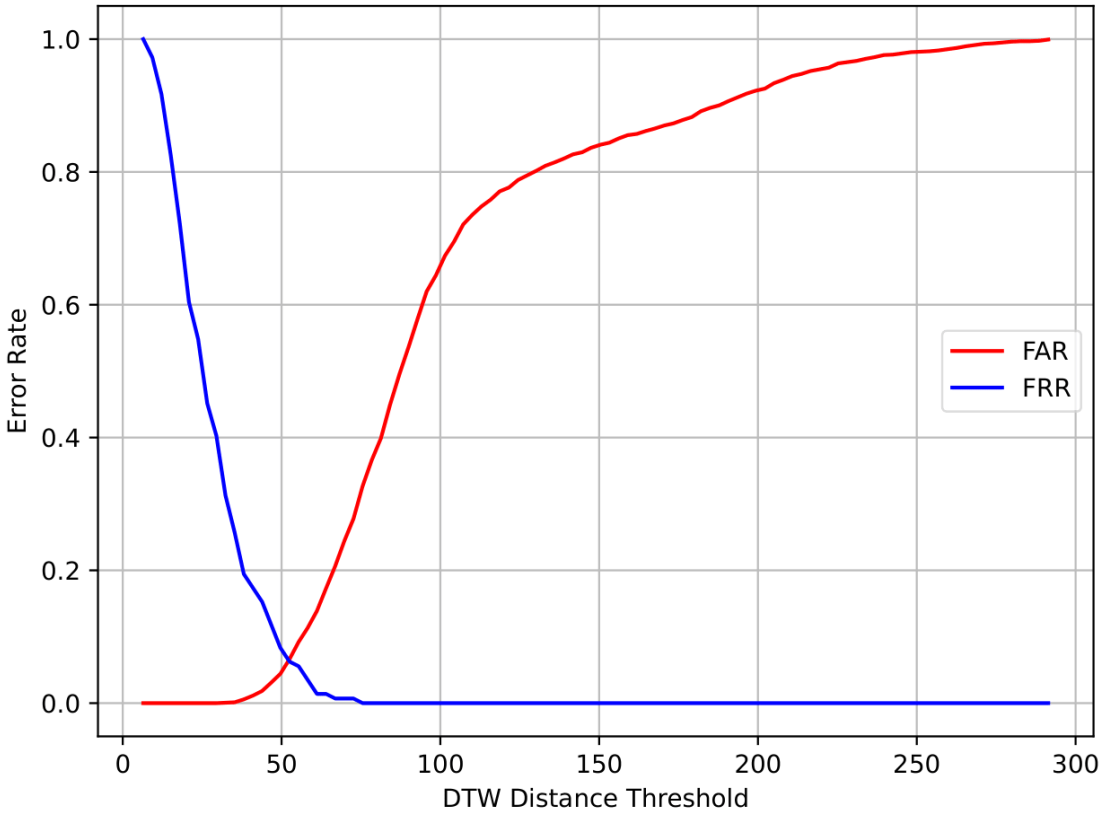
Subject	Mean	SD
A	232.5	8.3
B	180.3	13.3
C	224.3	13.4
D	225.7	11.6
E	208.5	**7.2**
F	202.7	20.6
G	227.7	21.1
H	222.2	15.9
I	186.5	15.3
J	246.8	9.1
K	167.7	11.8
L	221.2	10.6

Unstable rhythms

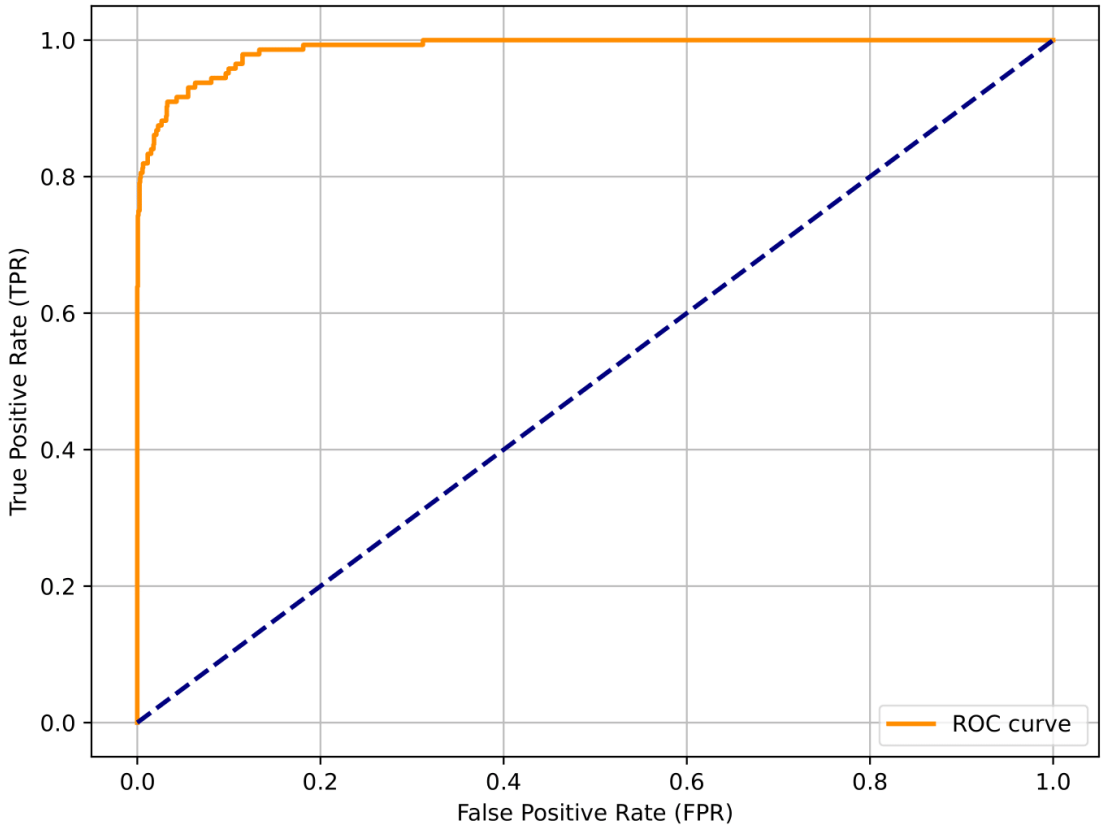
Longest

Characteristics of individuals

ROC curve



FAR and FRR



ROC

Experiment 1: accuracy

Proposed (DTW distance)

true \ Est.	A	B	C	D	E	F	G	H	I	J	K	L
A	6	0	0	0	0	0	0	0	0	0	0	0
B	0	6	0	0	0	0	0	0	0	0	0	0
C	0	0	6	0	0	0	0	0	0	0	0	0
D	0	0	0	6	0	0	0	0	0	0	0	0
E	0	0	0	0	6	0	0	0	0	0	0	0
F	0	0	0	0	0	5	0	0	0	0	0	1
G	0	0	0	0	0	0	6	0	0	0	0	0
H	0	0	0	0	0	0	0	6	0	0	0	0
I	0	0	0	0	0	0	0	0	6	0	0	0
J	0	0	0	0	0	0	0	0	0	6	0	0
K	0	0	0	0	0	0	0	0	0	0	6	0
L	0	0	0	0	0	0	0	0	0	0	0	6

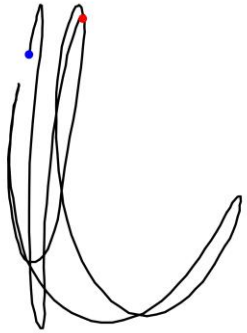
Random Forest [2]

true \ Est.	A	B	C	D	E	F	G	H	I	J	K	L
A	6	0	0	0	0	0	0	0	0	0	0	0
B	0	6	0	0	0	0	0	0	0	0	0	0
C	0	0	6	0	0	0	0	0	0	0	0	0
D	0	0	0	6	0	0	0	0	0	0	0	0
E	0	0	0	1	5	0	0	0	0	0	0	0
F	0	0	0	0	0	6	0	0	0	0	0	0
G	0	0	0	0	0	0	5	0	0	0	0	1
H	0	0	0	0	0	0	0	6	0	0	0	0
I	0	0	0	0	0	0	0	0	6	0	0	0
J	0	0	0	0	0	0	0	0	0	6	0	0
K	0	0	0	0	0	0	0	0	0	0	6	0
L	0	0	0	0	0	0	0	0	0	0	0	6

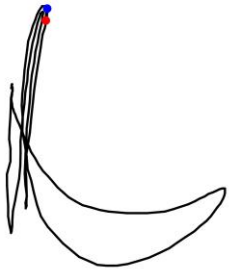
Discussion

Reasons for error

Subject F behaves like subject L



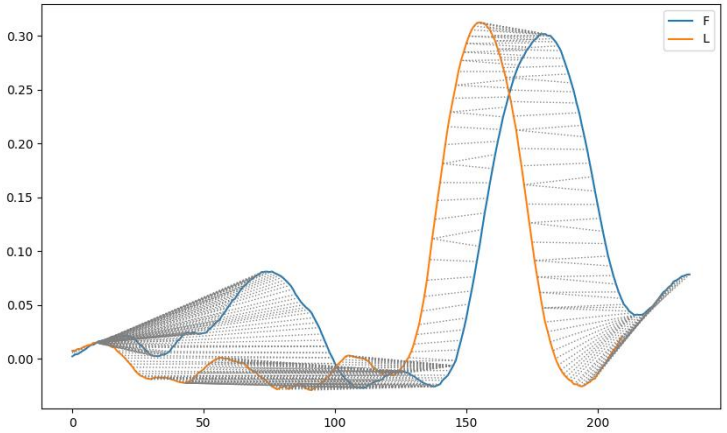
Subject F



Subject L

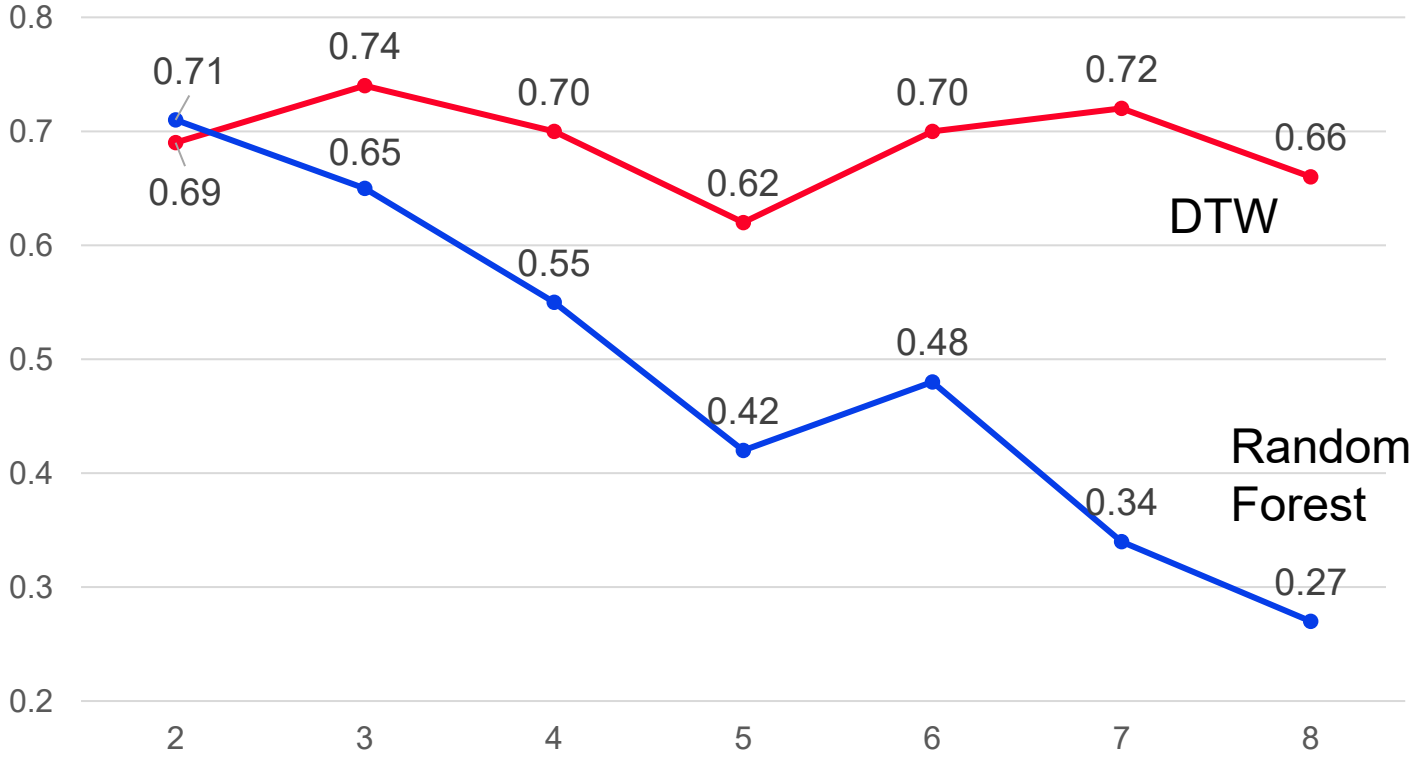
DTW distance between F and L

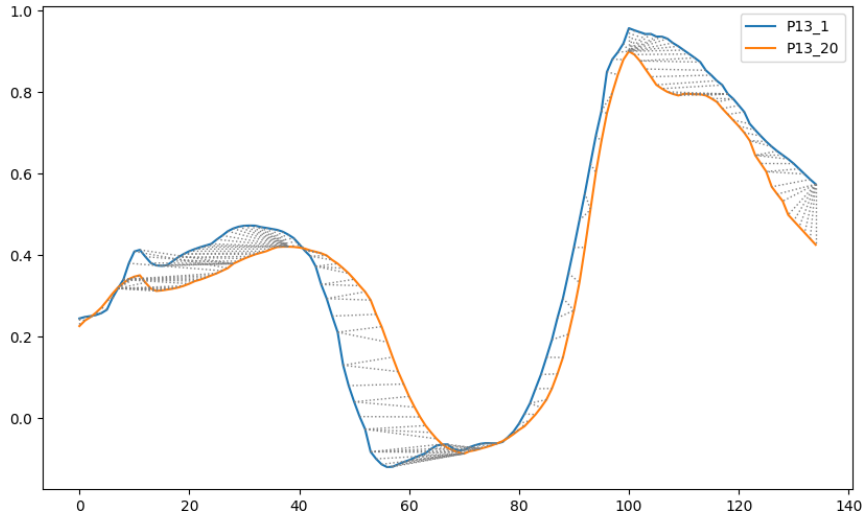
テンプレート \ テスト		F_1
Genuine	F_3	64.69
	F_4	57.34
	F_5	58.46
	F_6	58.62
imposter	L_3	39.10
	L_4	44.23
	L_5	44.18
	L_6	40.62



DTW distance of X-coordinates between F and L

Experiment 2:





DTW distance between 1st and 20th Player 13.

Robustness: DTW is less affected by temporal changes than random forest.

Mitigations

- to reduce details by
  - generalizing or coarsening the motion information to represent only the approximate movements consistent with the original gestures.
  - Lowering the data granularity, e.g., reducing the frame rate, can be expected to suppress individual differences in motion.
  - Injecting noise into motion data, e.g., differential privacy

Conclusions

- In this study, we proposed a method for personal identification based on Dynamic Time Warping (DTW) distances using time series data of 3D coordinates from an HMD and both hand controllers in a VR environment.
- We conducted an in-depth analysis to reveal the source of misclassification and primary factors for making the identification more robust. We also discussed some possible mitigations.
- For future work, we plan to expand large-scale experiments.