Global Feature Analysis and Comparative Evaluation of Freestyle In-Air-Handwriting Passcode for User Authentication

Presented at Annual Computer Security Applications Conference (ACSAC), 2021

Duo Lu[1], Yuli Deng[2], Dijiang Huang[2]

[1]dlu@rider.edu
[2]{ydeng19, dijiang.huang}@asu.edu

[1] Rider University, Lawrence, New Jersey, USA
[2] Arizona State University, Tempe, Arizona, USA

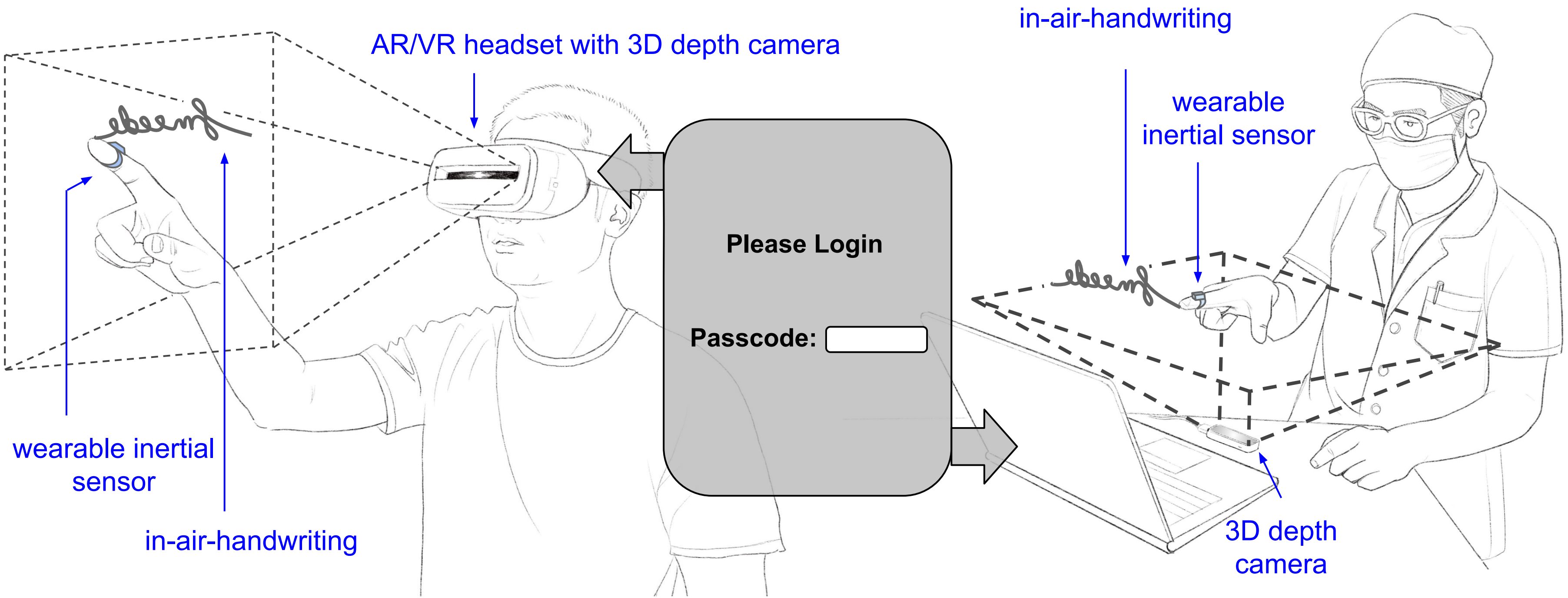
[1] This work is done when Duo Lu is a PhD student at Arizona State University

RIDER UNIVERSITY

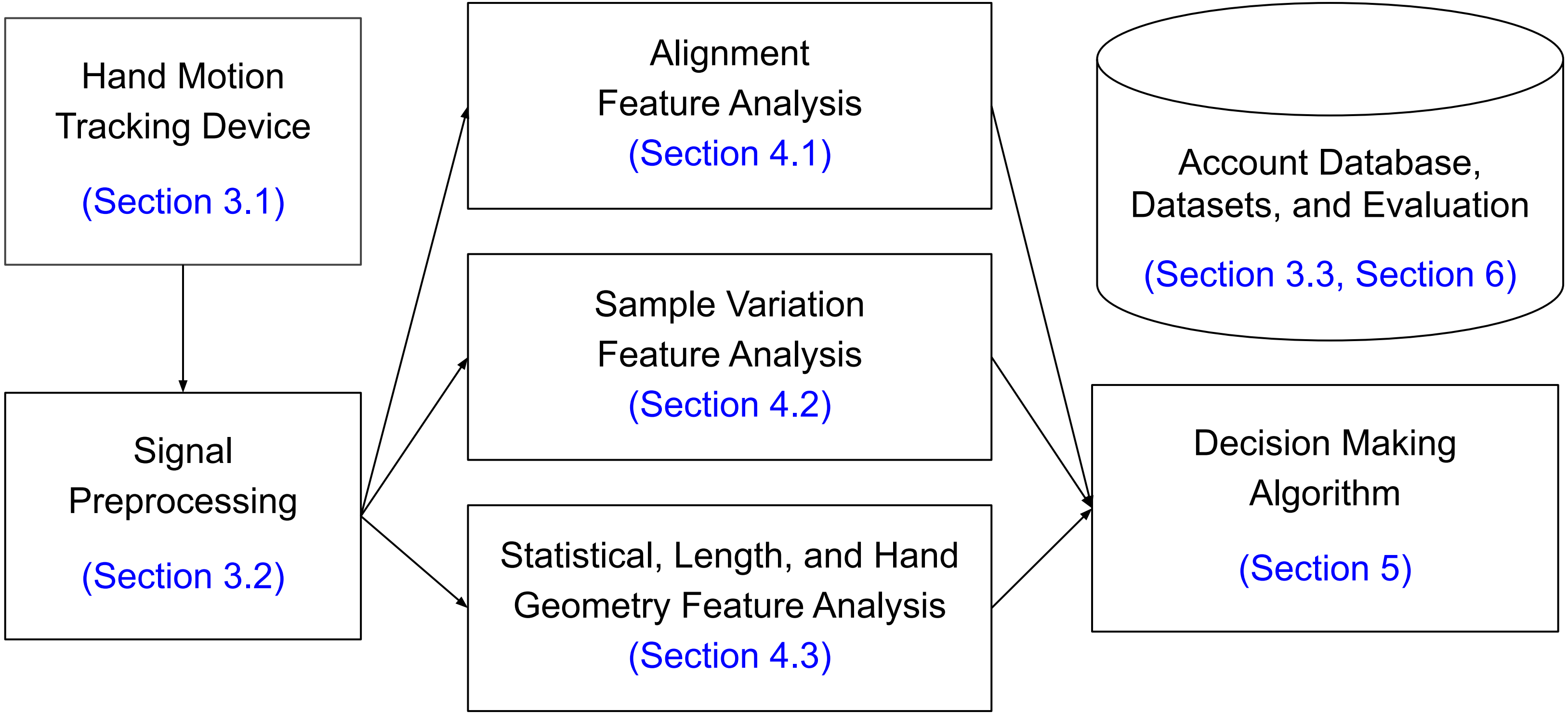
ASU IRA A. FULTON SCHOOLS OF engineering

SNAC Secure Networking And Computing Research Group

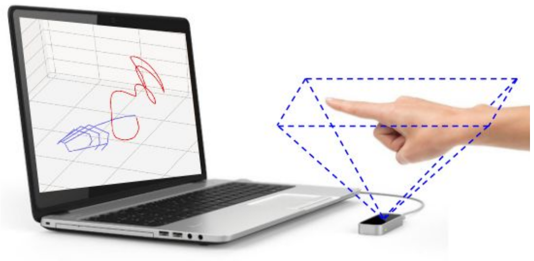
Freestyle In-Air-Handwriting Passcode



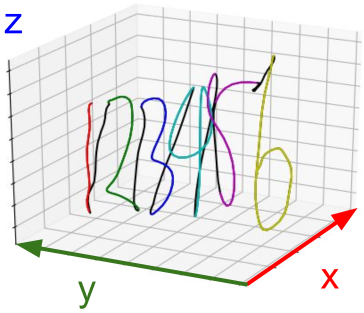
System Architecture



Devices and Signals

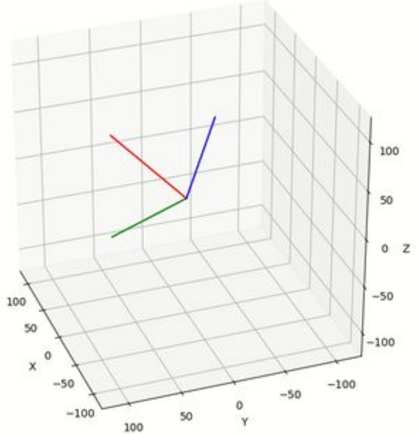


the camera device



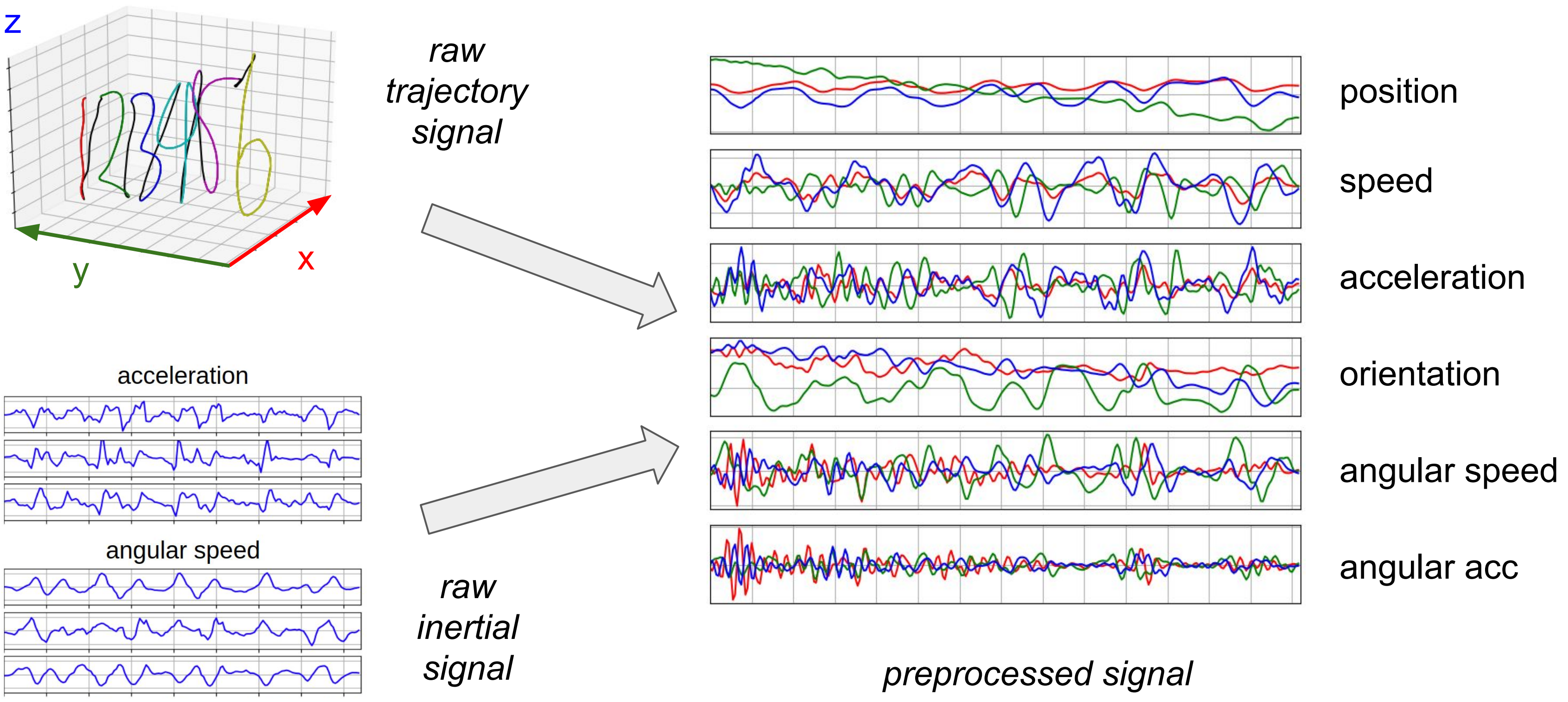
trajectory signal example

the glove device

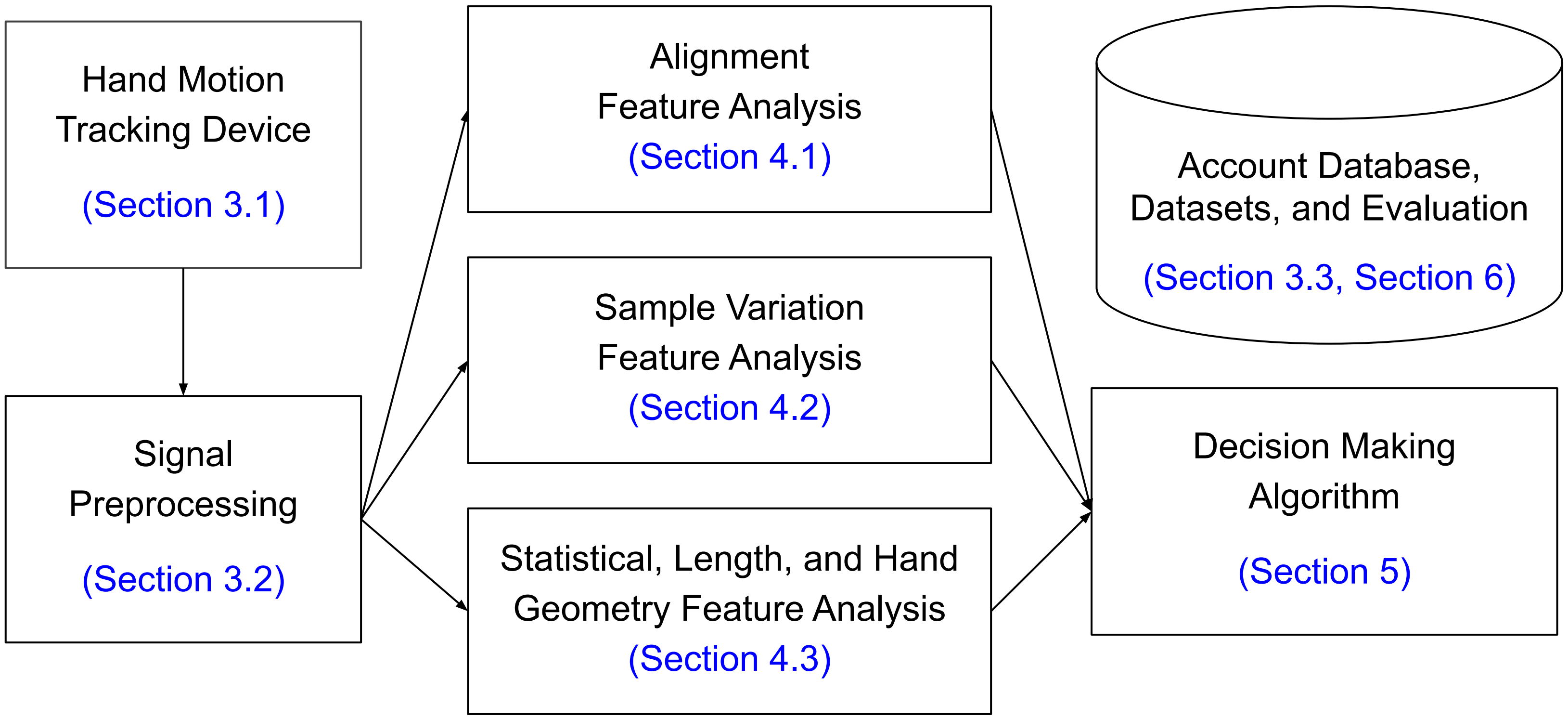


orientation signal example

Preprocessing



System Architecture



Datasets

dataset	# signals	description
ID-passcode	7,200	Legitimate users create two meaningful strings as an ID and a passcode.
collision	36,000	Imposters attack with the knowledge of string meaning.
spoofing	18,000	Imposters attack based on watching recorded videos of legitimate users.
persistence	8,000	Ten sessions of data of legitimate users writing the ID and the passcode.

We constructed four datasets using two types of devices from **180** users.

Our dataset and code library is openly available at https://github.com/duolu/fmkit

Feature Extraction and Matching

Five different types of features are extracted and five corresponding matching scores are computed.

(1) Alignment cost: δ_{AC}

(2) Signal sample distance: δ_{TTV}

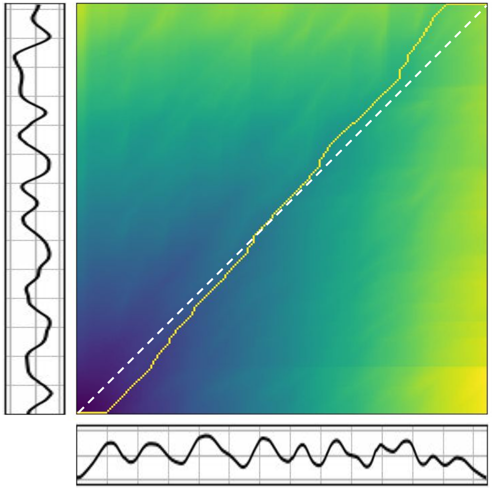
(3) Signal statistical difference: δ_{SD}

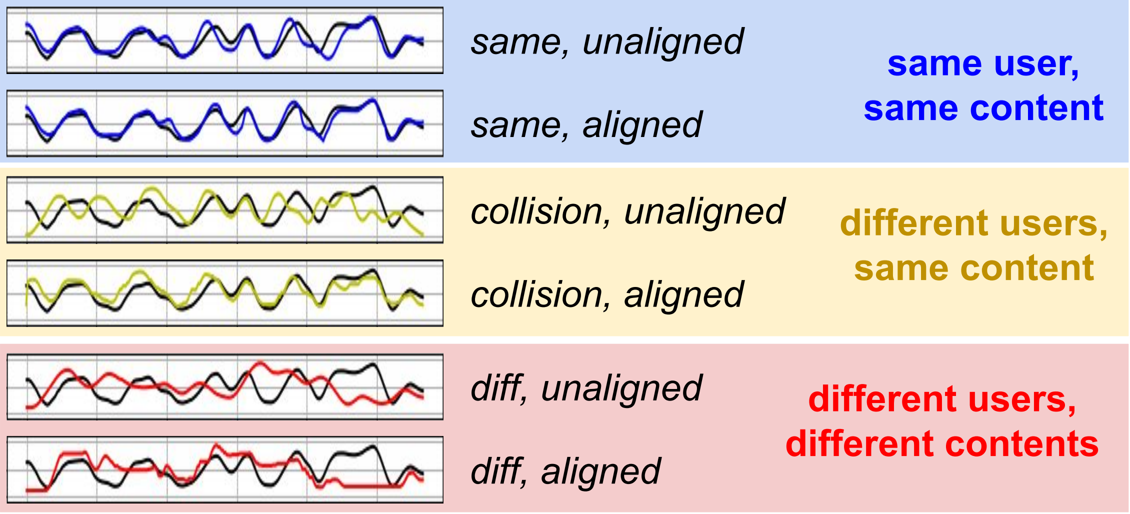
(4) Signal length difference: δ_{LD}

(5) Hand geometry difference: δ_{HGD}

Alignment Cost

Given the segment [i'_s , i'_e] of the signal is aligned to the ith sample of the template, $\delta_{AC} = \sum_{i}^{l} i - \frac{i'_s + i'_e}{2}$





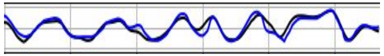
warping path example

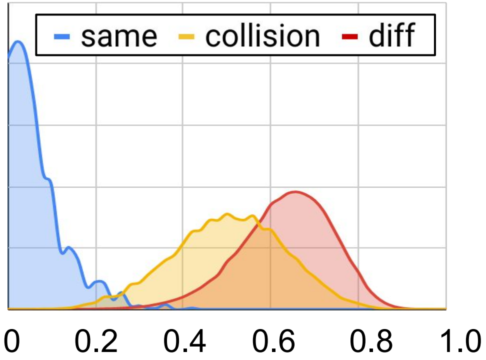
alignment example

Signal Sample Distance

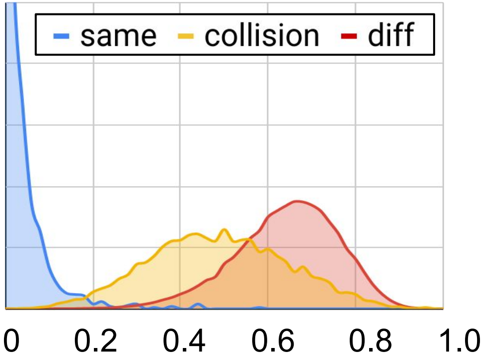
$$\delta_{TTV} = \frac{1}{l}\sum_{i}^{l} round[\frac{1}{d}\sum_{j}^{d} TTV(D_{ij} * P_{ij} * Q_{ij})]$$

element-wise difference



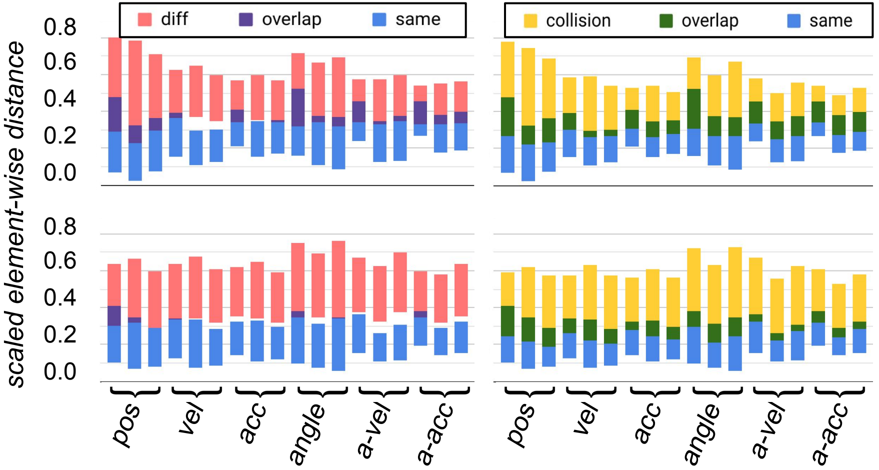


(a) distribution of δ_{TTV}, camera

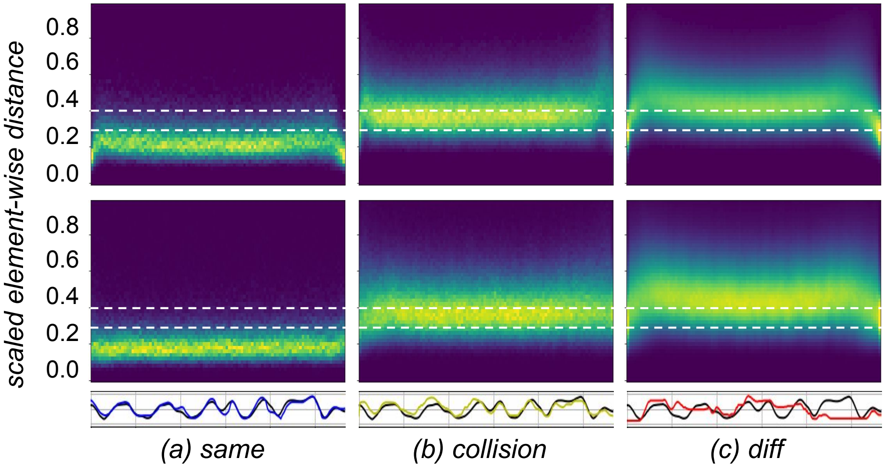


(b) distribution of δ_{TTV}, glove

Signal Sample Distance Analysis



Analysis on multiple sensor axes.



Analysis along time.

The signal sample distance feature can be used to distinguish different writers and contents.

Statistical Feature

$f(R) = (\mathbf{M}, \mathbf{\Sigma}, \mathbf{P}, \mathbf{\Lambda}, \mathbf{L})$

- **Mean:** Mean of each sensor axis, $\mathbf{M} = (\mu_1, \ldots, \mu_d)$, where $\mu_j = \text{mean}(S_j)$.
- **Variance:** Variance of each sensor axis, $\mathbf{\Sigma} = (\sigma_1, \ldots, \sigma_d)$, where $\sigma_j = \text{var}(S_j)$.
- **Correlation:** Correlation among sensor axes, $\mathbf{P} = (\alpha_{xy}, \alpha_{yz}, \alpha_{xz}, \beta_{xy}, \beta_{yz}, \beta_{xz}, \ldots\ldots)$,

  where α_{xy} , β_{xy} , γ_{xy} is the correlation of acc, gyro, Euler axis x and y
- **Amplitude:** Sum of amplitude of each axis, $\mathbf{\Lambda} = (\lambda_1, \ldots, \lambda_d)$, where $\lambda_j = \Sigma|S_{ij}|$.
- **LF-ratio:** Portion of low frequency components (below 3 Hz), $\mathbf{H} = (\eta_1, \ldots, \eta_d)$,

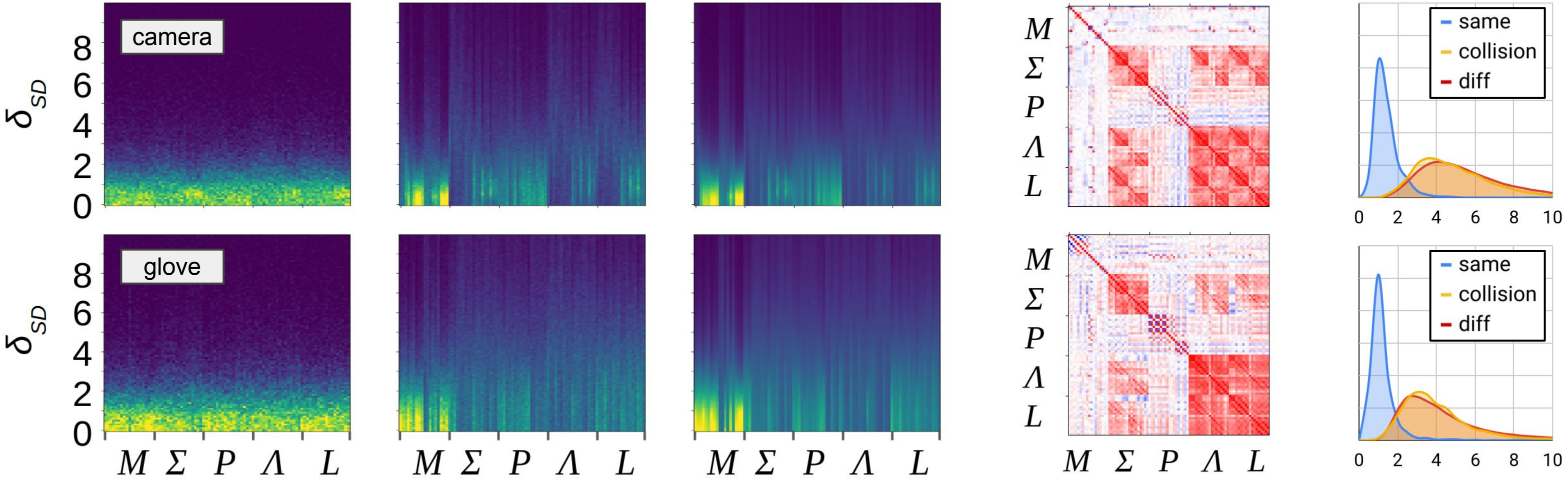
Statistical Feature Difference & Length Difference

$$\delta_{SD} = mean(abs(f(R) - \boldsymbol{\mu}_{SF})/\boldsymbol{\sigma}_{SF})$$

$$\delta_{LD} = |l_R - l_T|/l_T$$

$$\boldsymbol{\mu}_{SF} = mean(f(R^{(1)}), f(R^{(2)}), ..., f(R^{(m)}))$$

$$\boldsymbol{\sigma}_{SF} = std(f(R^{(1)}), f(R^{(2)}), ..., f(R^{(m)}))$$

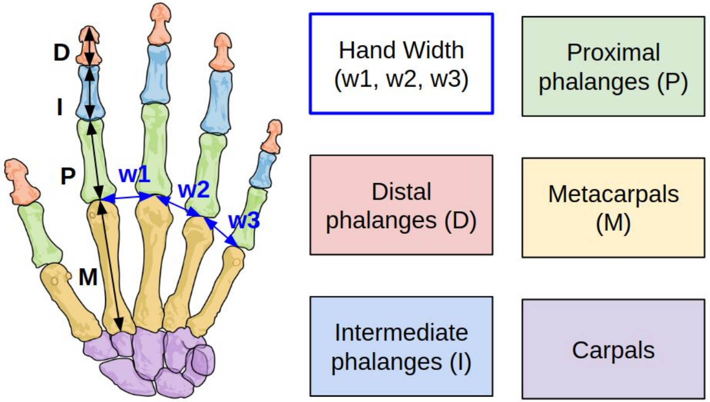


(a) same (b) collision (c) diff (d) correlation (e) distribution of δ_{SD}

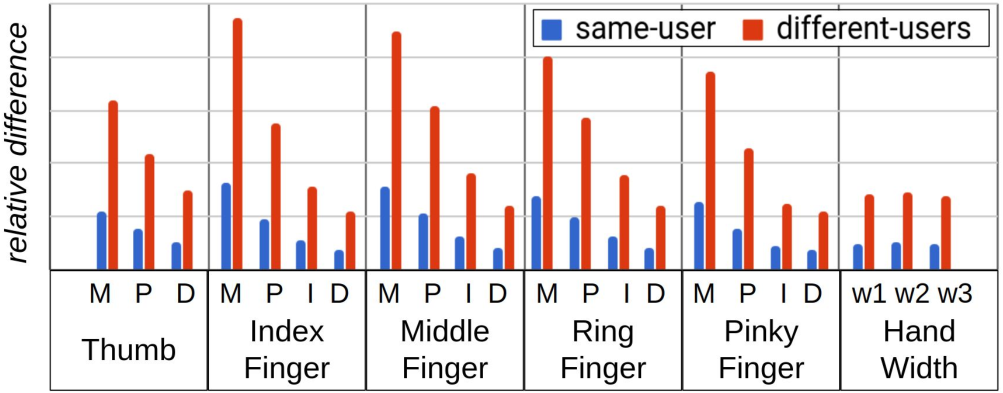
Hand Geometry Difference

$$\delta_{HGD} = mean(abs(\mathbf{h}_R - \mathbf{h}_T)/\mathbf{h}_T)$$

Only available for the camera device.



(a) definition of hand geometry features



(b) length difference of each hand geometry component

Generally, alignment cost, statistical differences, length differences, and hand geometry differences are weak features.

Fusion of Features

score fusion
(less parameters)

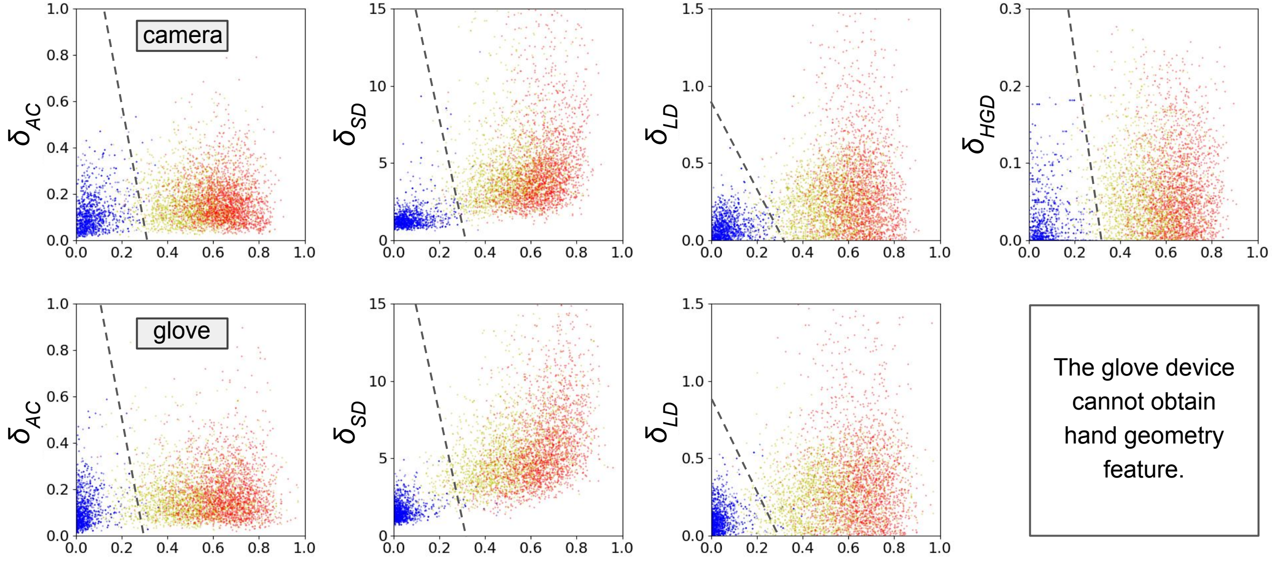
$$\delta_{other} = w_1\delta_{AC} + w_2\delta_{SD} + w_3\delta_{LD} + w_4\delta_{HGD},$$

$$\delta_{S-Fusion} = \delta_{TTV} + \delta_{other},$$

$$\delta_{T-Fusion} = b + \sum_{i=1}^{l}\sum_{j=1}^{d} w_{ij}D_{ij},$$

$$\delta_{F-Fusion} = \delta_{T-Fusion} + \delta_{other}.$$

feature fusion
(more parameters)



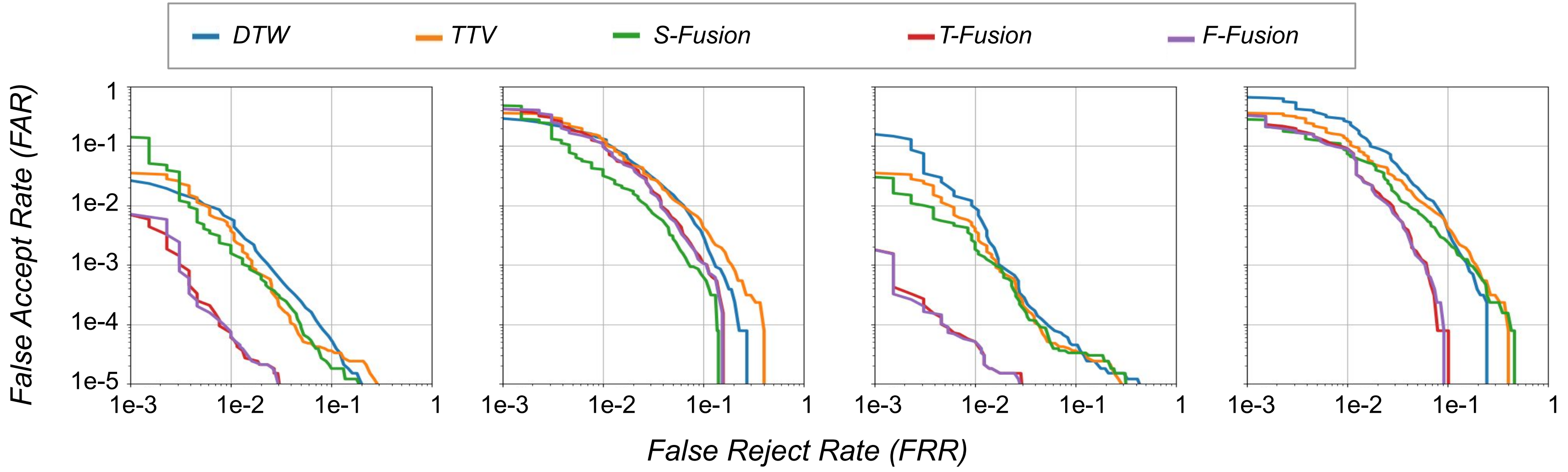
(a) δ_{AC} vs. δ_{TTV} (b) δ_{SD} vs. δ_{TTV} (c) δ_{SD} vs. δ_{TTV} (d) δ_{HGD} vs. δ_{TTV}

Comparison with the Two Types of Devices

method	the camera device								the glove device							
	using data from the camera device								using data from the glove device							
	without collision (in %)					with collision (in %)			without collision (in %)					with collision (in %)		
	EER	FAR 1K	FAR 10K	Zero FAR	Zero FRR	EER	FAR 1K	Zero FAR	EER	FAR 1K	FAR 10K	Zero FAR	Zero FRR	EER	FAR 1K	Zero FAR
DTW(2)	1.24	5.75	17.69	71.40	28.76	5.10	27.6	37.2	1.24	3.80	10.52	49.46	98.18	5.04	24.0	38.9
TTV(2)	1.00	4.81	12.18	44.57	16.49	3.64	19.9	37.2	1.12	2.97	7.30	48.84	50.97	4.17	23.0	38.9
DTW	0.81	2.39	7.56	56.36	25.00	3.08	13.3	29.5	0.75	1.33	5.26	43.80	8.56	2.95	12.0	19.6
TTV	0.70	2.38	7.99	23.64	15.54	2.16	15.2	34.8	0.68	0.85	2.86	35.50	11.23	2.39	13.6	23.6
S-Fusion	0.50	1.38	4.95	37.75	42.38	**1.83**	**7.4**	**15.4**	0.39	0.93	2.06	36.12	16.21	1.98	15.6	30.9
T-Fusion	0.22	0.32	0.78	12.33	7.35	2.61	10.9	17.0	**0.16**	**0.16**	**0.39**	2.95	6.57	1.51	4.7	6.2
F-Fusion	0.26	0.31	0.85	12.00	7.30	2.61	10.7	16.6	**0.16**	**0.16**	**0.39**	3.10	4.25	1.51	4.4	5.6
T-Fusion(A)	0.21	0.23	**0.57**	**10.62**	**3.23**	2.74	10.6	23.2	**0.16**	**0.16**	0.42	2.79	**0.50**	1.86	6.5	12.2
T-Fusion(E)	**0.10**	**0.12**	0.78	10.70	4.72	2.40	8.91	18.3	**0.16**	**0.16**	**0.39**	**2.02**	2.29	**1.38**	**3.5**	**5.1**

The performances with the two types of devices are close.

Performance Results (ROC)



(a) w/o collision (camera)

(b) w/ collision (camera)

(c) w/o collision (glove)

(d) w/ collision (glove)

Roughly one or two mistakes over one thousand authentication attempts at best.

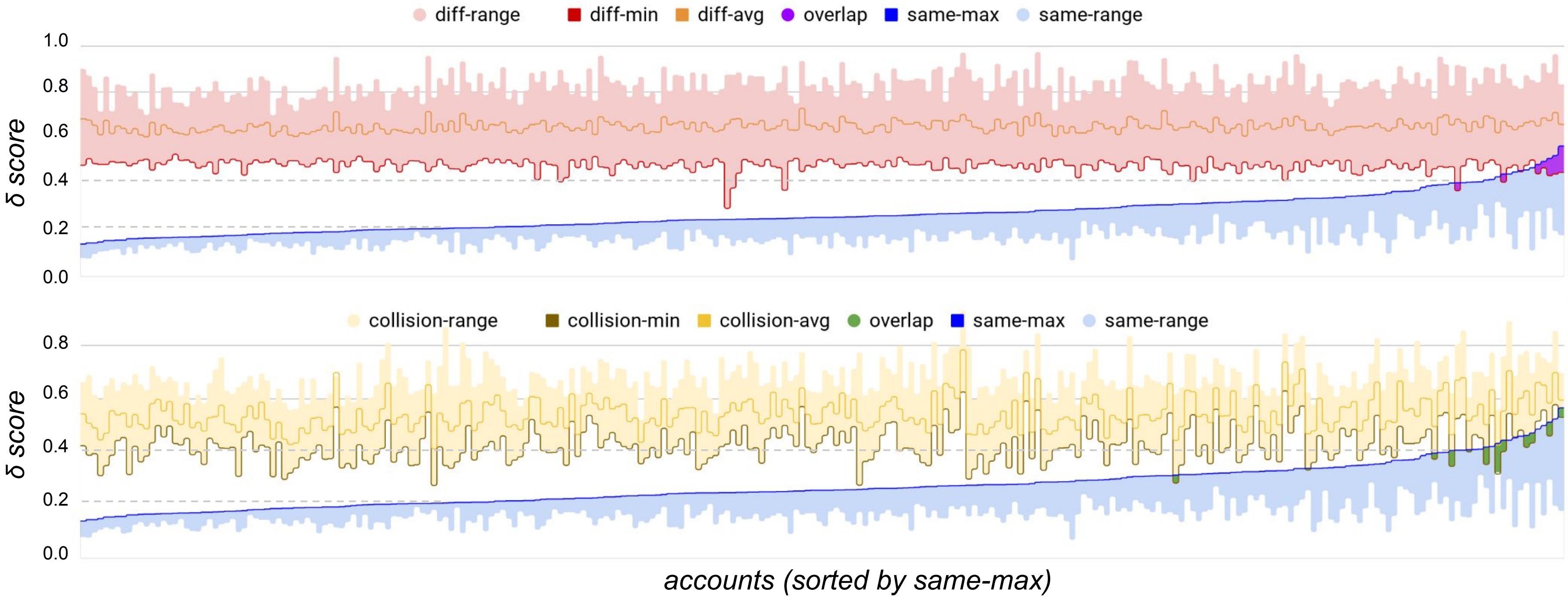
Comparison with Existing Works

Ref.	number of users	EER (w/o collision)	EER (w/ collision)	Device	Algorithm
Ours (camera)	180	0.10% ~ 1.24%	1.83% ~ 5.10%	Leap Motion	SVM, TTV, DTW
Ours (glove)	180	0.16% ~ 1.24%	1.38% ~ 5.04%	custom data glove	SVM, TTV, DTW
Liu et al.[17]	20 ~ 25	~ 3%	~10%	Wii remote	DTW
Bailador et al.[2]	96	1.8% ~ 2.1%	~ 5%	smartphone	DTW, Bayes, HMM
Bashir et al.[3]	40	~1.8%	N/A	custom digital pen	DTW
Chan et al.[6]	16	0.8%	N/A	Leap Motion	random forest
Tian et al.[31]	18	~2%	N/A	Kinect	DTW

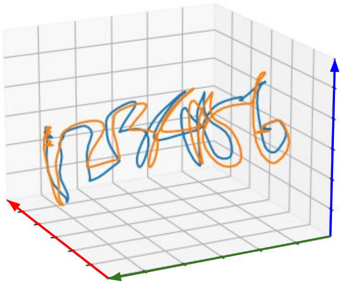
Our methods have slightly larger datasets and better performance.

Our work provides more comprehensive comparative evaluations and analyses.

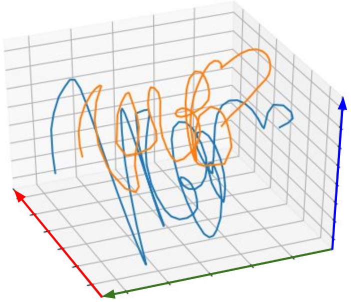
Analysis of Scores for All Accounts



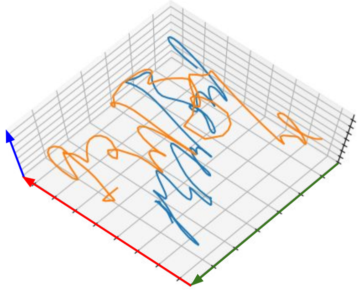
Easy Cases and Hard Cases



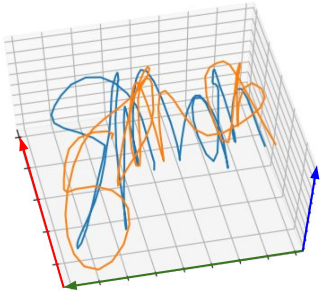
(a) same, δ = 0.187 (easy)



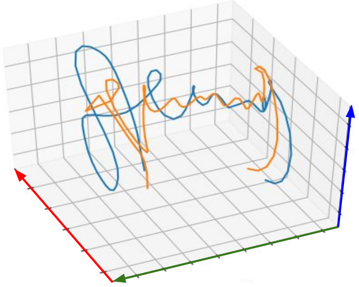
(b) same, δ = 0.524 (hard)



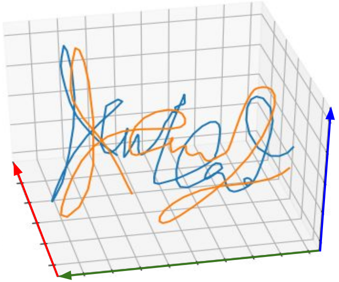
(c) same, δ = 0.566 (hard)



(d) collision, δ = 0.555 (easy)



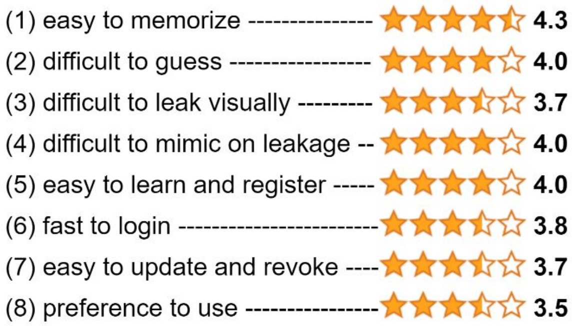
(e) diff, δ = 0.294 (hard)

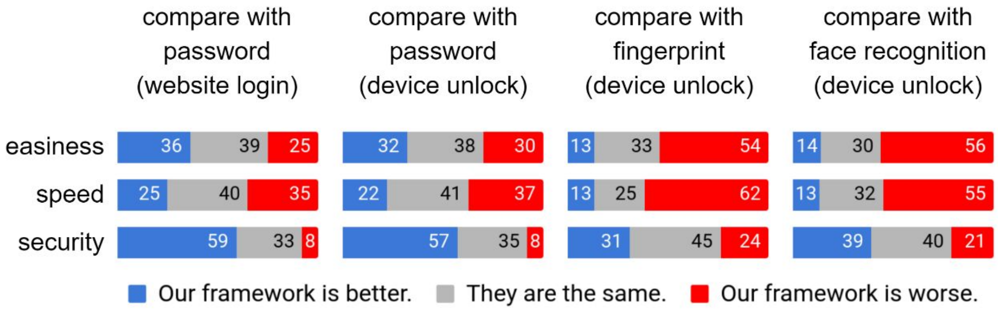


(f) diff, δ = 0.373 (hard)

More Analysis

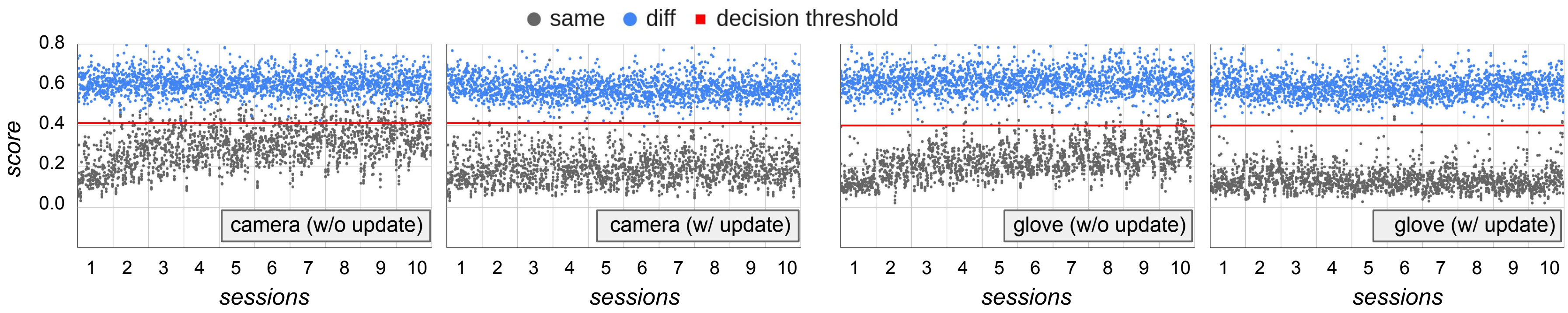
- Analysis with active spoofing attacks.
- Analysis of persistent performance with data from multiple sessions.
- Analysis of usability.

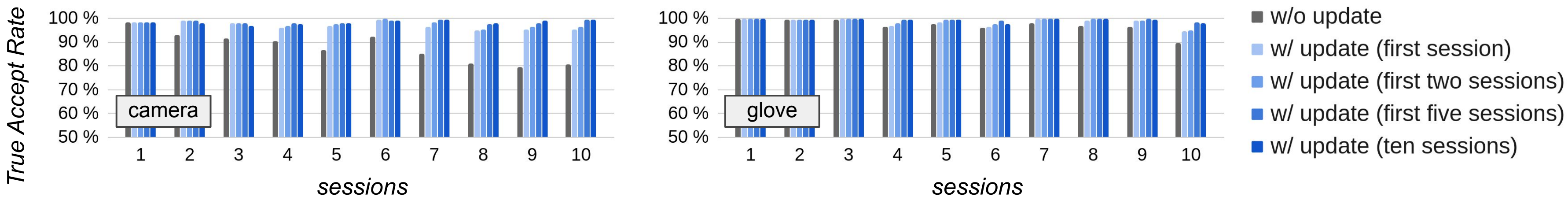




Our work analyzes the strength and limitations in various scenarios.

Long-Term Performance Analysis





Our work analyzes the long-term performance.

Thank you!

More details are available in our paper and at https://github.com/duolu/fmkit

Duo Lu[1], Yuli Deng[2], Dijiang Huang[2]

[1]dlu@rider.edu
[2]{ydeng19, dijiang.huang}@asu.edu

RIDER UNIVERSITY

ASU IRA A. FULTON SCHOOLS OF engineering

Secure Networking And Computing Research Group