Liveness is Not Enough: Enhancing Fingerprint Authentication with Behavioral Biometrics to Defeat Puppet Attacks

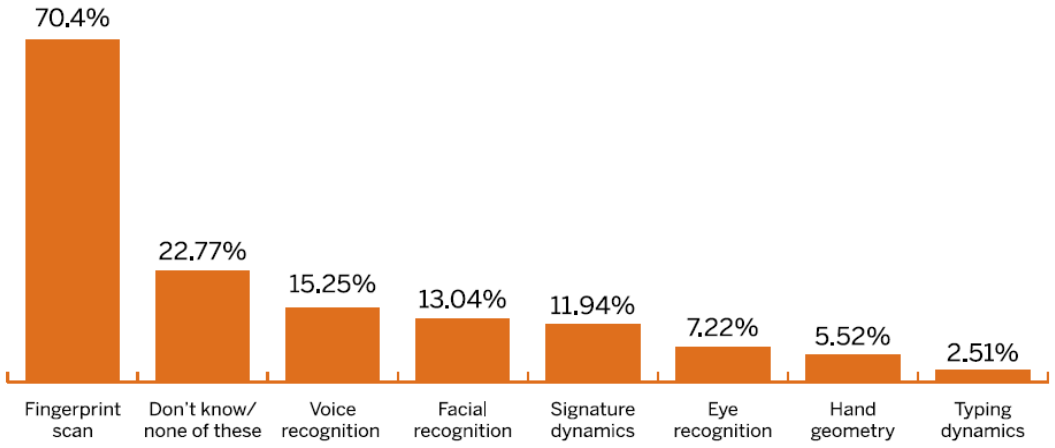
Cong Wu[1,2], Kun He[1], Jing Chen[1,2], Ziming Zhao[4], Ruiying Du[1,3]

[1] Wuhan University, China
[2] Shenzhen Institute of Wuhan University, China
[3] Collaborative Innovation Center of Geospatial Tech., China
[4] Rochester Institute of Technology, USA

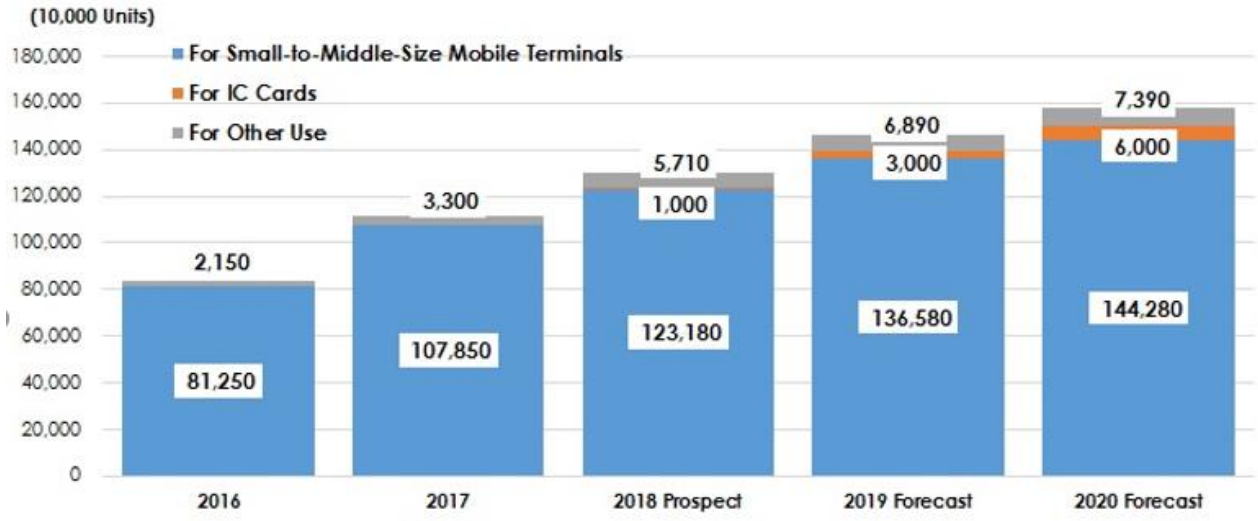
WUHAN UNIVERSITY RIT | Rochester Institute of Technology

The Prevailing Fingerprint Authentication

PHOTO: https://www.fingerprints.com/



German, R. L., & Barber, K. S. (2018). Consumer attitudes about biometric authentication. *The University of Texas at Austin*.



Report: Yano Research Institute Ltd.

Attacks on Fingerprint Authentication

ICS › 35 › 35.240 › 35.240.15

ISO/IEC 30107-1:2016

Information technology — Biometric presentation attack detection — Part 1: Framework

Author:
Lindsey O'Donnell

April 8, 2020 / 9:00 am

15:30 minute read

Write a comment

Share this article:

New research used 3D printing technology to bypass fingerprint scanners, and tested it against Apple, Samsung and Microsoft mobile products.

New research has found that it's possible to use 3D printing technology to create "fake fingerprints" that can bypass most fingerprint scanners used by popular devices. But, creating the attack remains costly and time-consuming.

Researchers with Cisco Talos created different threat models that use 3D printing technology, and then tested them on mobile devices (including the iPhone 8 and Samsung S10), laptops (including the Samsung Note 9, Lenovo Yoga and HP Pavilion X360) and smart devices (such as a smart padlock).

ACM NEWS

Attackers Can Bypass Fingerprint Authentication with an ~80% Success Rate

By Ars Technica
April 8, 2020
Comments

VIEW AS: SHARE:

For decades, the use of fingerprints to authenticate users to computers, networks, and restricted areas was mostly limited to large and well-resourced organizations that used specialized and expensive equipment. That all changed in 2013 when Apple introduced TouchID. Within a few years, fingerprint-based validation became available to the masses as computer, phone, and lock manufacturers added sensors that gave users an alternative to passwords when unlocking the devices.

Although hackers managed to defeat TouchID with a fake fingerprint less than 48 hours after the technology was rolled out in the iPhone 5, fingerprint-based authentication over the past few years has become much harder to defeat. Today, fingerprints

Puppet Attack

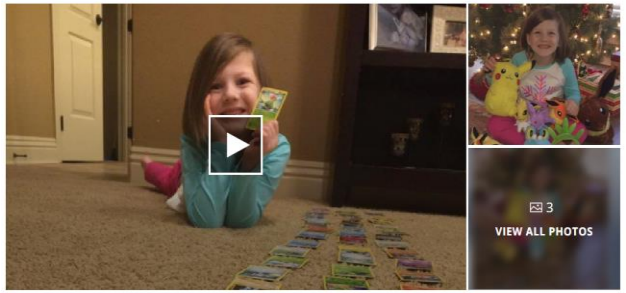
Police 'visit funeral home to unlock dead man's phone'

23 April 2018 Share

Police in Florida have been criticised for allegedly entering a funeral home in a futile bid to unlock a dead man's smartphone.

6-year-old uses sleeping mom's thumb to go on Amazon shopping spree

by WKRC | Wednesday, December 28th 2016

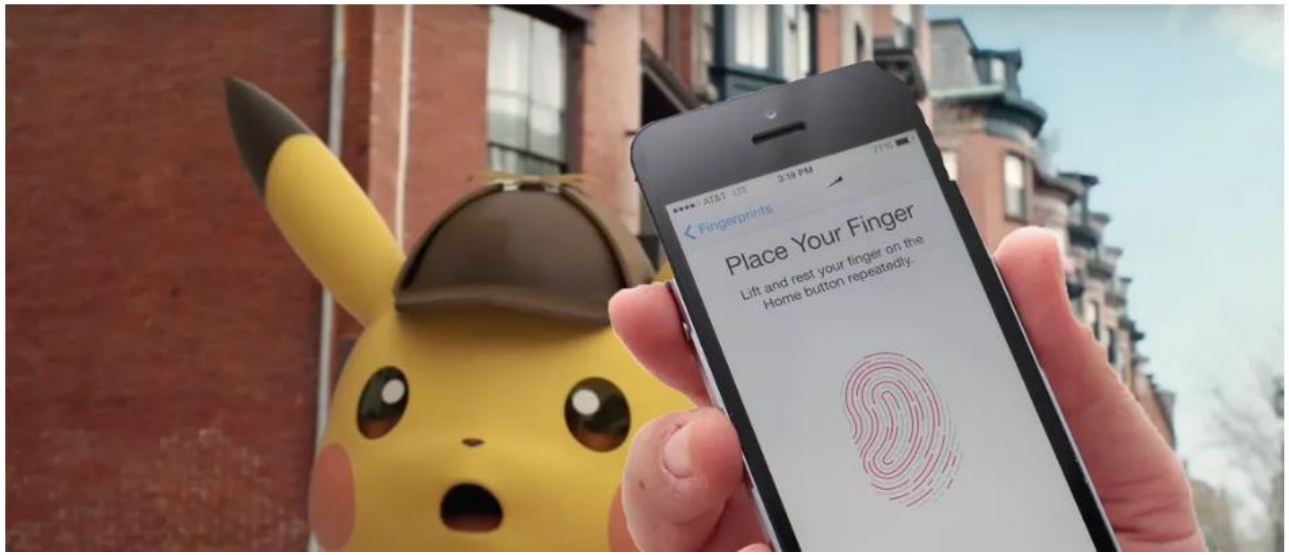


6-year-old uses sleeping mom's thumb to go on Amazon shopping spree (Provided by/used with permission: Bethany Johnson Howell)

Child uses sleeping mom's fingerprints to buy Pokemon gifts

When you want to buy $250 worth of Pokemon presents, desperate times call for desperate measures.

Alfred Ng Dec. 27, 2016 6:25 a.m. PT 16



I got drunk last night and got robbed because I was using Touch ID :-(

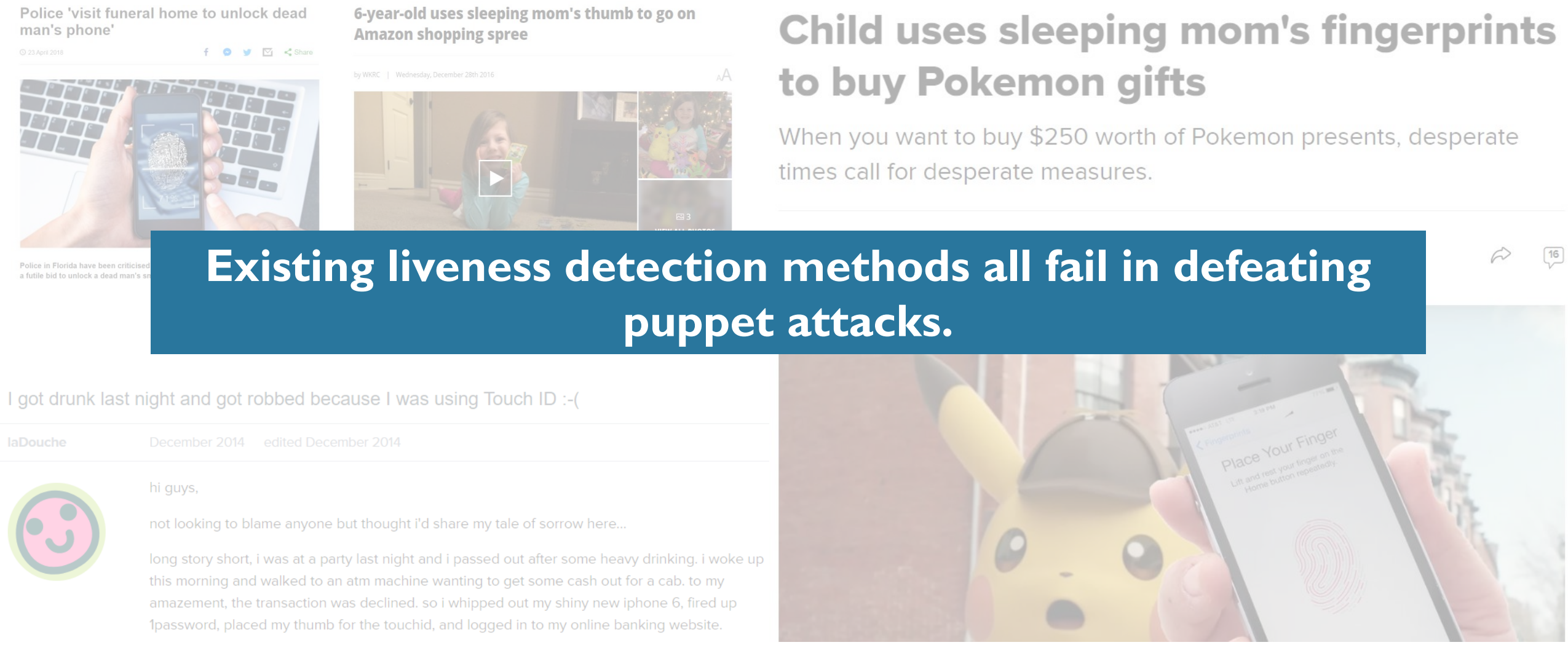
laDouche December 2014 edited December 2014

hi guys,

not looking to blame anyone but thought i'd share my tale of sorrow here...

long story short, i was at a party last night and i passed out after some heavy drinking. i woke up this morning and walked to an atm machine wanting to get some cash out for a cab. to my amazement, the transaction was declined. so i whipped out my shiny new iphone 6, fired up 1password, placed my thumb for the touchid, and logged in to my online banking website.

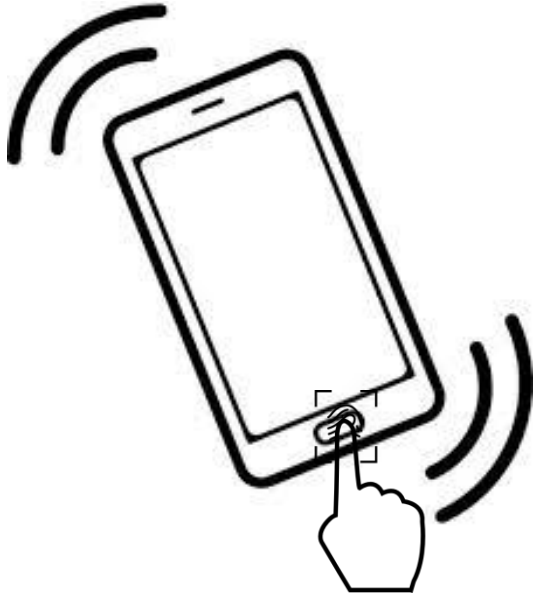
Puppet Attack



Existing liveness detection methods all fail in defeating puppet attacks.

Our Approach

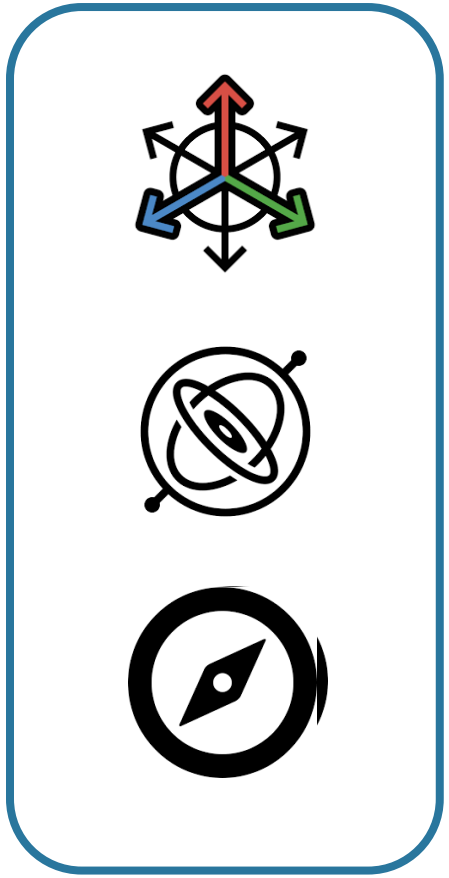
Fingerprint



Fingertip-touch behavior

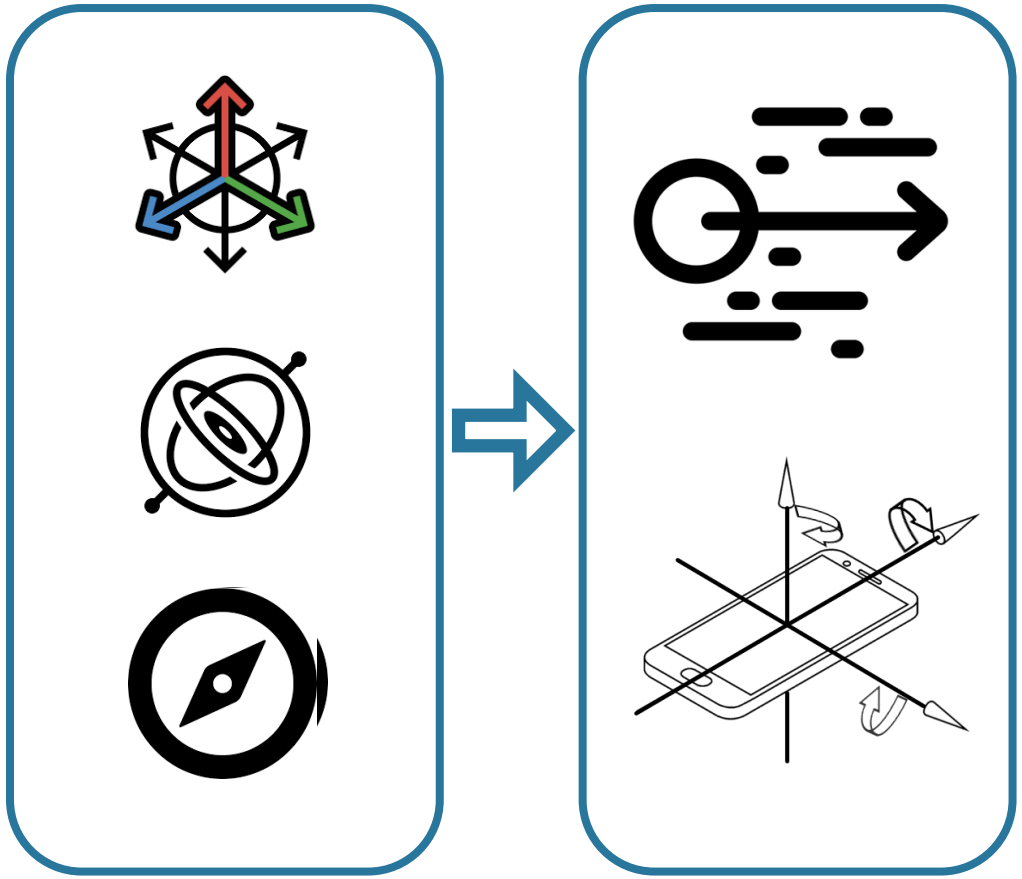
Complement fingerprint authentication with fingertip-touch behavioral characteristics

System Overview



Data capture

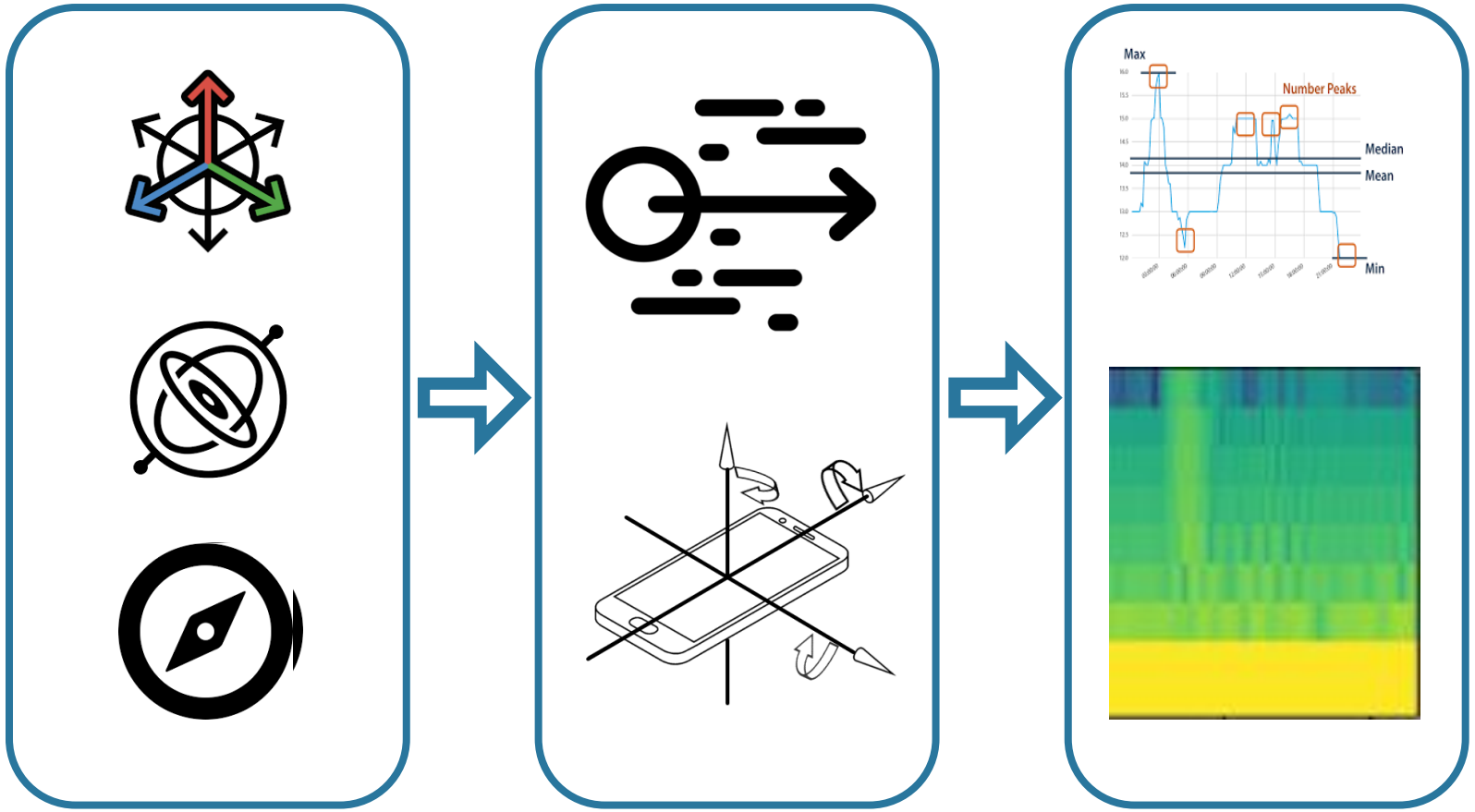
System Overview



Data capture

Behavior characterizing

System Overview

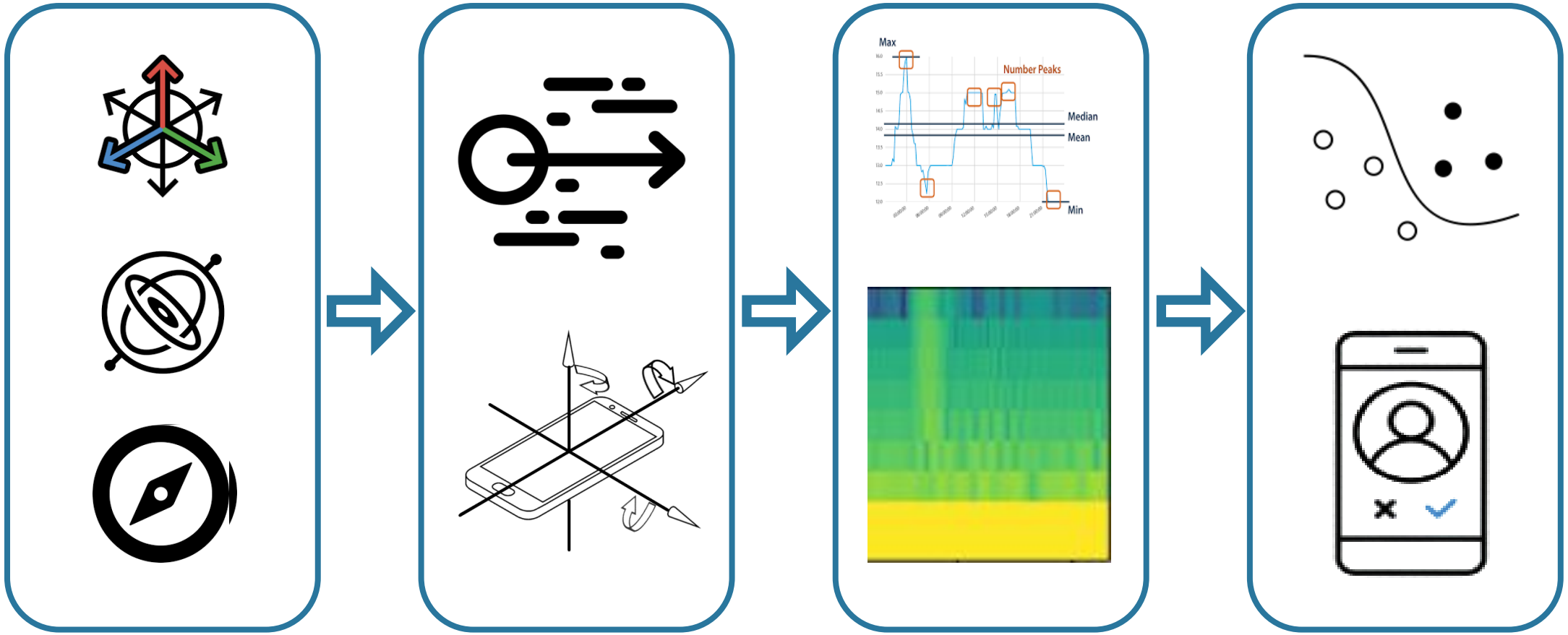


Data capture

Behavior characterizing

Feature extraction

System Overview



Data capture

Behavior characterizing

Feature extraction

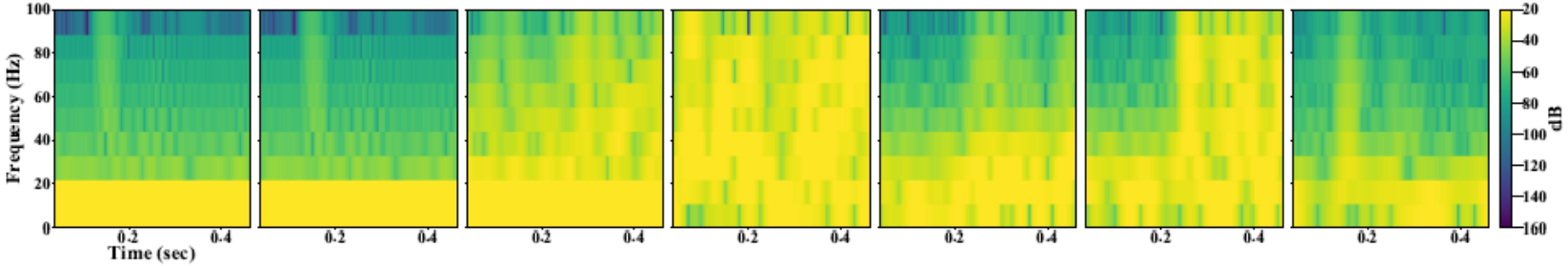
Model training /Authentication

Time- and Frequency- Domain Features (TFF)

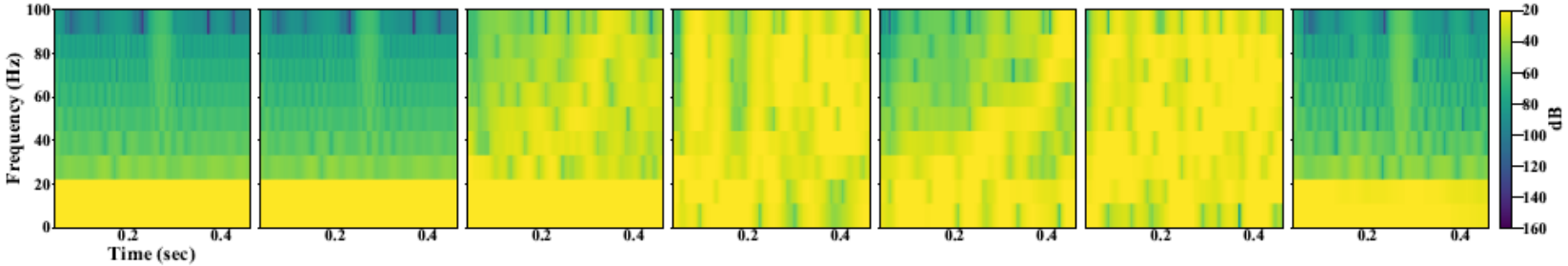
Table 1: Time- and frequency-domain features and their normalized fisher's scores.

Domain	Feature	Description	Normalized Fisher Score of $(\boldsymbol{a}_x, \boldsymbol{a}_y, \boldsymbol{a}_z, \boldsymbol{a}', \boldsymbol{\phi}, \boldsymbol{\theta}, \boldsymbol{\psi})$
Time	Mean	The mean of the time series.	$(0.45, 0.01, 0.22, \mathbf{0.68}, \mathbf{0.86}, \mathbf{0.84}, \mathbf{0.84})$
	Standard deviation	The standard deviation of the time series.	$(0.24, 0.56, 0.31, 0.41, 0.58, 0.32, \mathbf{0.74})$
	Relative standard deviation	The extent of variability in relation to its mean.	$(0.34, 0.15, 0.12, 0.56, \mathbf{0.71}, \mathbf{0.64}, \mathbf{0.82})$
	Sum of absolute differences	The sum over the absolute value of consecutive changes in the time series.	$(0.32, 0.27, \mathbf{0.72}, 0.52, 0.53, \mathbf{0.72}, \mathbf{0.78})$
	Absolute energy	The absolute energy of the time series.	$(\mathbf{0.63}, \mathbf{0.98}, \mathbf{0.85}, 0.57, \mathbf{0.72}, 0.57, 0.37)$
	Autocorrelation	The autocorrelation of the time series.	$(0.00, 0.14, 0.15, 0.21, \mathbf{0.94}, \mathbf{0.62}, \mathbf{0.64})$
Frequency	Spectral centroid	The center of mass of the spectrum is located.	$(0.34, 0.21, 0.38, 0.12, \mathbf{0.78}, \mathbf{0.98}, \mathbf{0.78})$
	Spectral spread	The average spread of the spectrum in relation to its centroid.	$(\mathbf{0.66}, 0.36, 0.32, \mathbf{0.78}, 0.46, \mathbf{0.82}, \mathbf{0.96})$
	Spectral skewness	The measurement of the asymmetry of the probability distribution of a real-valued random variable about its mean.	$(\mathbf{0.85}, 0.45, 0.58, \mathbf{0.84}, 0.56, \mathbf{0.85}, \mathbf{1.00})$
	Spectral kurtosis	The shape of a probability distribution.	$(0.34, 0.17, \mathbf{0.70}, \mathbf{0.86}, \mathbf{0.62}, 0.51, 0.42)$
	Power spectral density	Average of distribution of power into frequency components.	$(\mathbf{0.90}, \mathbf{0.71}, \mathbf{0.86}, 0.26, \mathbf{0.85}, \mathbf{0.68}, \mathbf{0.82})$
	Spectral entropy	The complexity of the signal in the frequency domain.	$(\mathbf{0.94}, 0.32, \mathbf{0.82}, 0.21, \mathbf{0.96}, \mathbf{0.82}, \mathbf{0.89})$

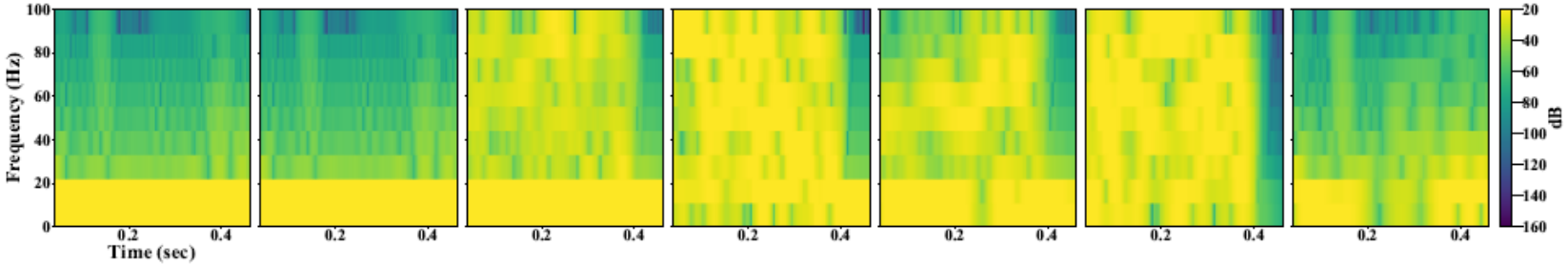
CNN-based Features (CNF)



(a) User A.



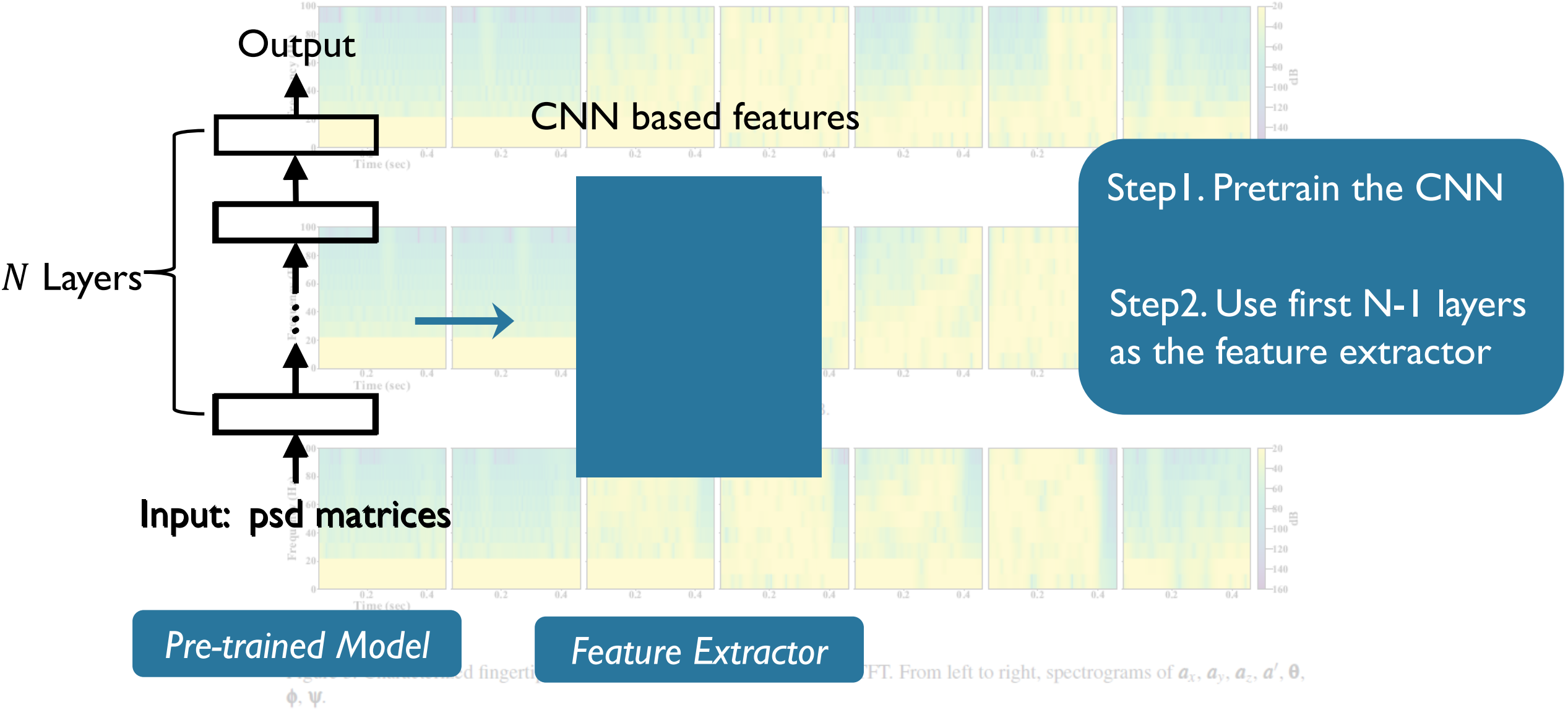
(b) User B.



(c) User C.

Figure 3: Characterized fingertip-touch behaviors of three users under STFT. From left to right, spectrograms of $\boldsymbol{a}_x$, $\boldsymbol{a}_y$, $\boldsymbol{a}_z$, $\boldsymbol{a}'$, $\boldsymbol{\theta}$, $\boldsymbol{\phi}$, $\boldsymbol{\psi}$.

CNN-based Features (CNF)



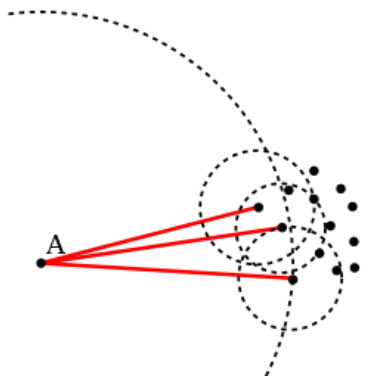
One-class Classifier

$$r_{XY} = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}}$$

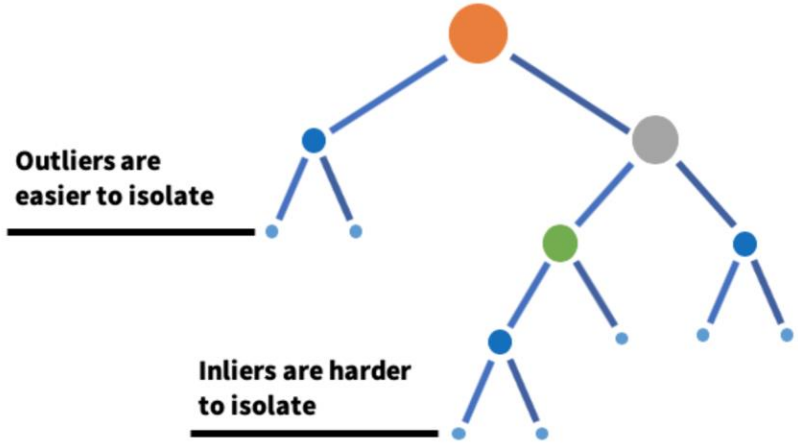
Pearson coefficient-based similarity comparison (PCC)

$$\min_{R,a} R^2 + C\sum_{i=1}^{n}\zeta_i$$
$$s.t. \, ||x_i - a||^2 \leq R^2 + \zeta_i, i = 1, \ldots, n$$
$$\zeta_i \geq 0, i = 1, \ldots, n$$

One-class support vector machine (OCSVM)



Local outlier factor (LOF)



Isolation forest (IF)

Data Collection

Table 3: Summary of the compiled datasets

Dataset	Week of Collection	# of Subjects / Attackers	Postures	Device	# of Data Points
1	1 †, 8 and 9 ‡	90	Sitting, standing, lying, walking, running	OnePlus3	63,000
2A	2, 3, 5, 7	24, 24, 22, 21	Sitting	OnePlus3	18,200
2B	10, 11, 12, 13	62, 61, 59, 53			47,000
3	Added Aug. 2019	64	Sitting	Xperia XZ1, Oneplus5, Vivo X21	3,200
4A					3,600
4B	2 †, 10 and 11 ‡	15	Sitting	OnePlus3	3,600
4C					3,600

Datasets

- 90 subjects in the data collection.
- Compiled three datasets in different postures[1], periods[2], and devices[3].
- Compiled one attack dataset[4] by considering three attacks with 15 subjects as adversaries.

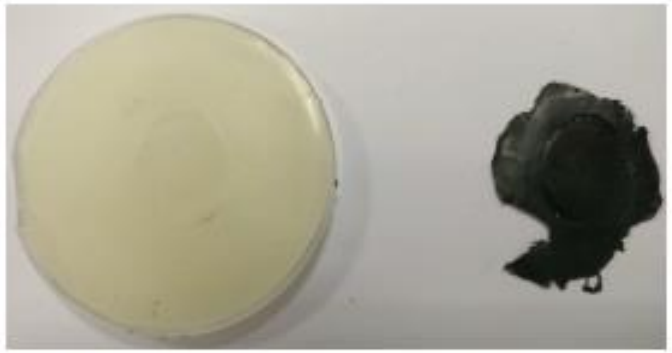
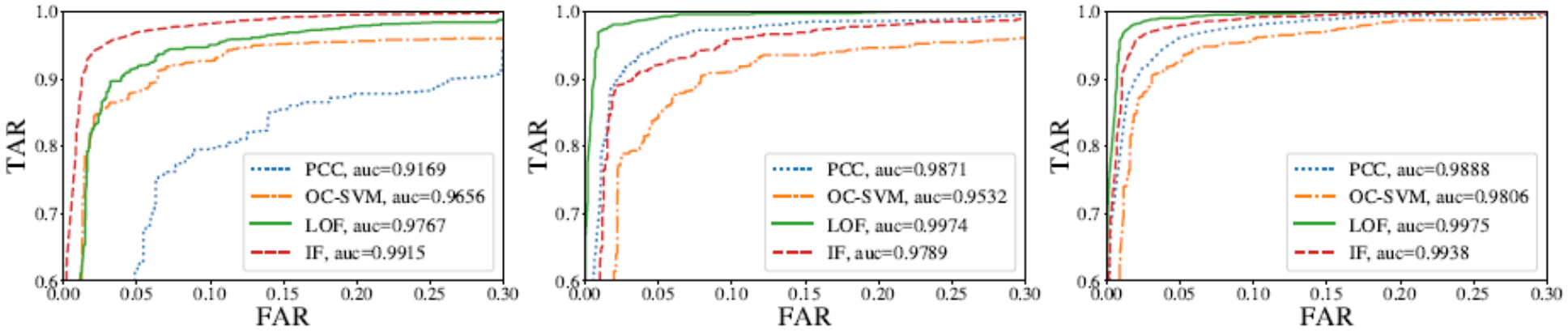


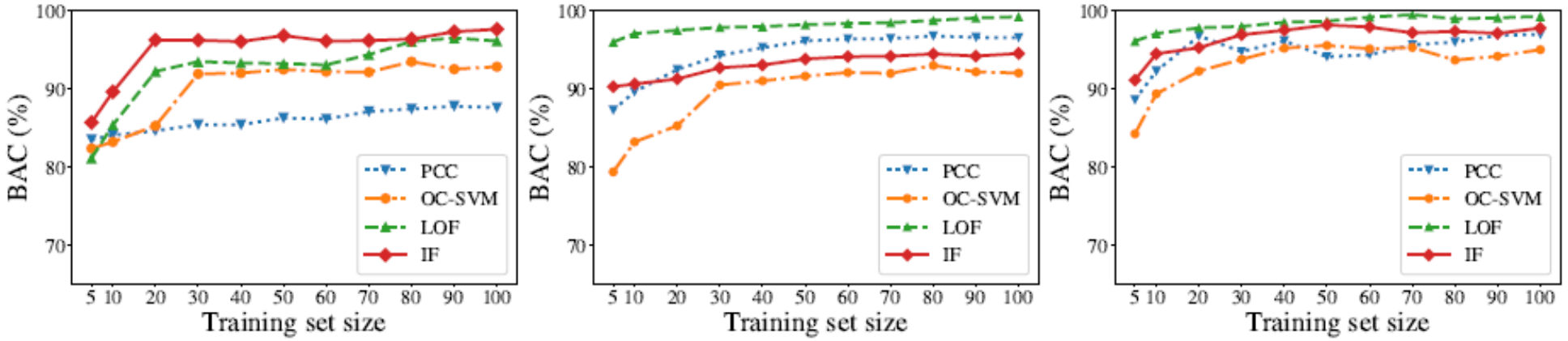
Figure 4: Artificial fingerprint replica. The left is the mold used to capture fingerprint; the right is a fake fingerprint crafted using silicone rubber.

Reliability Evaluation



(a) Time- and frequency-domain features (b) CNN-based features (c) The union of two feature sets

Figure 5: ROC curves of different feature sets under different one-class classifiers.

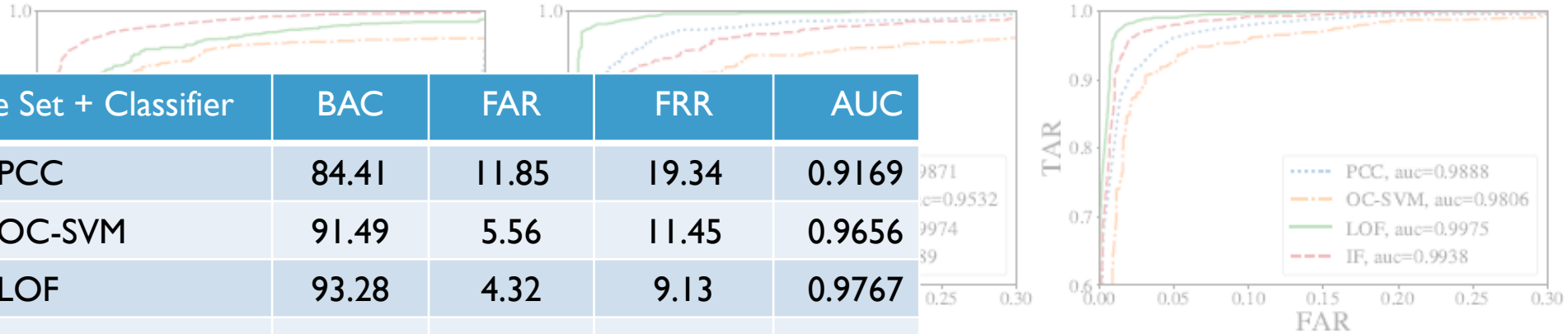


(a) Time- and frequency-domain features (b) CNN-based features (c) The union of two feature sets

Figure 6: BAC under different classifiers and different feature sets at varying training set sizes.

Reliability Evaluation

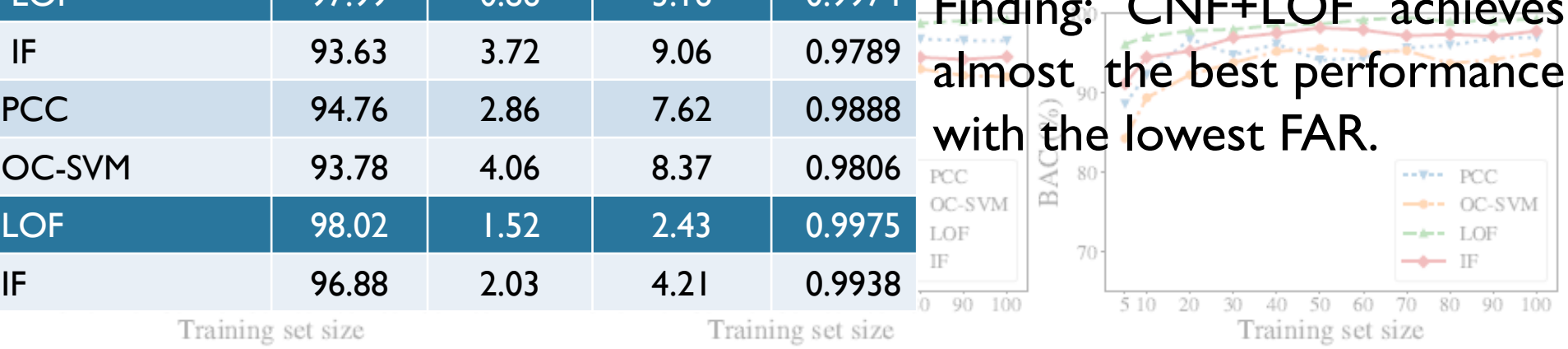
Feature Set + Classifier	BAC	FAR	FRR	AUC
TFF + PCC	84.41	11.85	19.34	0.9169
TFF + OC-SVM	91.49	5.56	11.45	0.9656
TFF + LOF	93.28	4.32	9.13	0.9767
TFF + IF	96.07	2.51	5.35	0.9915
CNF + PCC	94.65	3.30	7.40	0.9871
CNF + OC-SVM	90.69	6.41	12.21	0.9532
CNF + LOF	97.99	0.86	3.16	0.9974
CNF + IF	93.63	3.72	9.06	0.9789
UnF + PCC	94.76	2.86	7.62	0.9888
UnF + OC-SVM	93.78	4.06	8.37	0.9806
UnF + LOF	98.02	1.52	2.43	0.9975
UnF + IF	96.88	2.03	4.21	0.9938



(c) The union of two feature sets

different one-class classifiers.

Finding: CNF+LOF achieves almost the best performance with the lowest FAR.



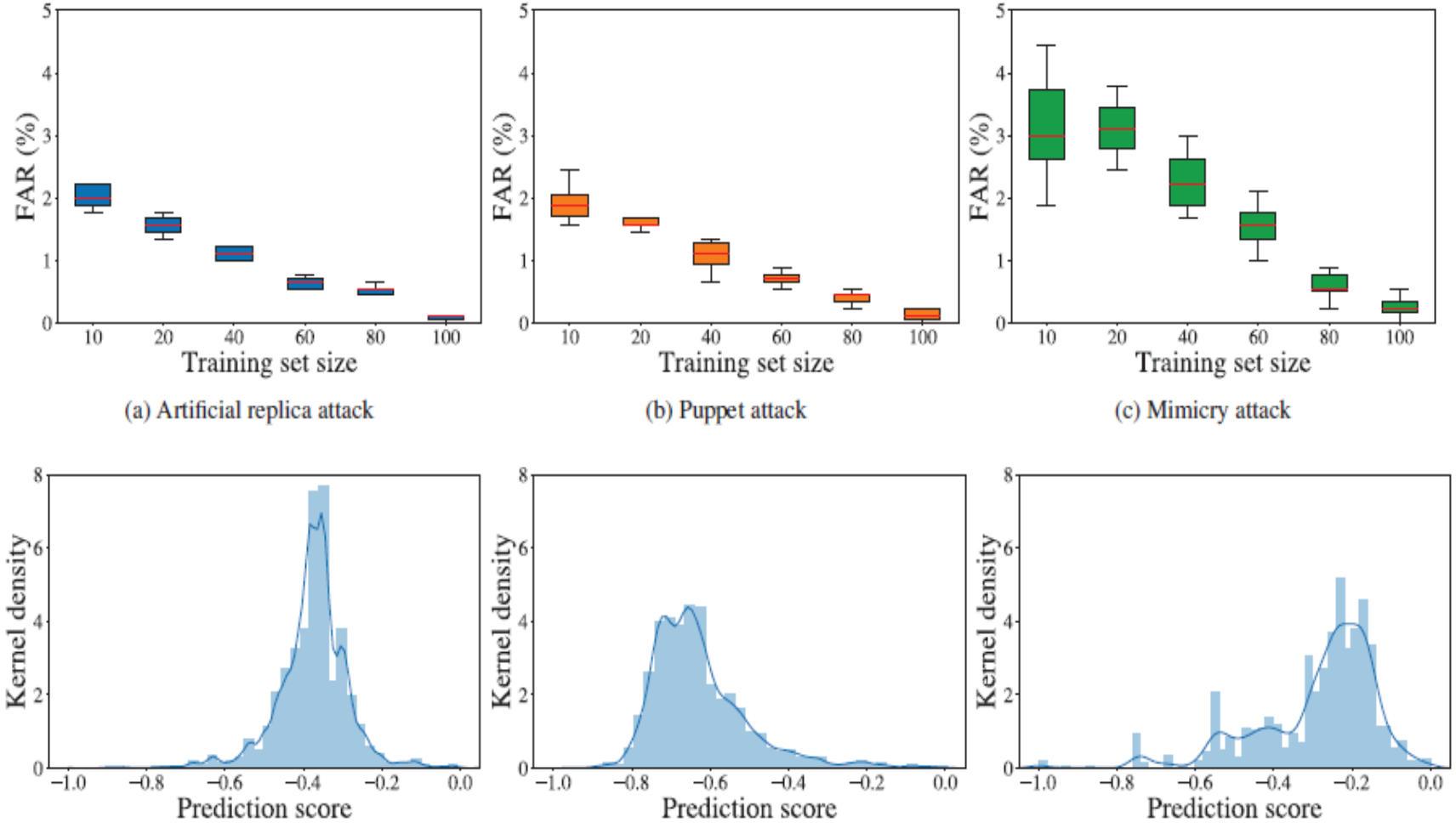
(a) Time- and frequency-domain features

(b) CNN-based features

(c) The union of two feature sets

Figure 6: BAC under different classifiers and different feature sets at varying training set sizes.

Evaluation of Presentation Attacks



FAR and kernel density of prediction score under attacks

Mean/standard deviation of FAR and prediction score

Attack	FAR	Score
ARA	0.08/0.06	-0.29/0.15
PA	0.12/0.08	-0.62/0.13
MA	0.25/0.14	-0.37/0.10

Limitations

Behavior variability with time elapsing?

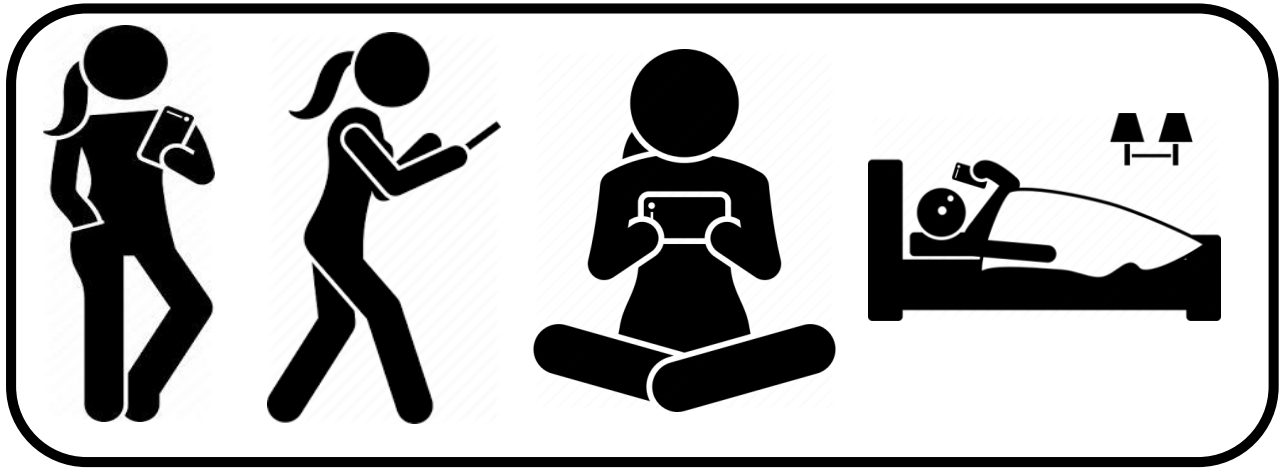
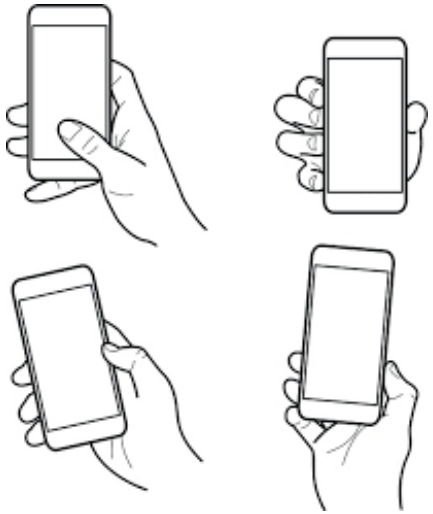
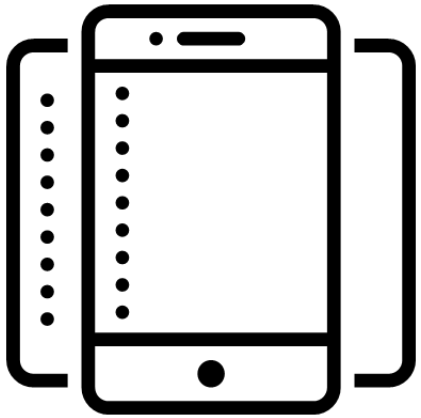


PHOTO: iconfinder.com

PHOTO: https://parker-marker.com/





Thank you!

Contact: Cong Wu, cnacwu@whu.edu.cn