OcuLock: Exploring Human Visual System for Authentication in Virtual Reality Head-mounted Display

Shiqing Luo∗, Anh Nguyen∗, Chen Song†, Feng Lin‡, Wenyao Xu§, Zhisheng Yan∗

∗Georgia State University

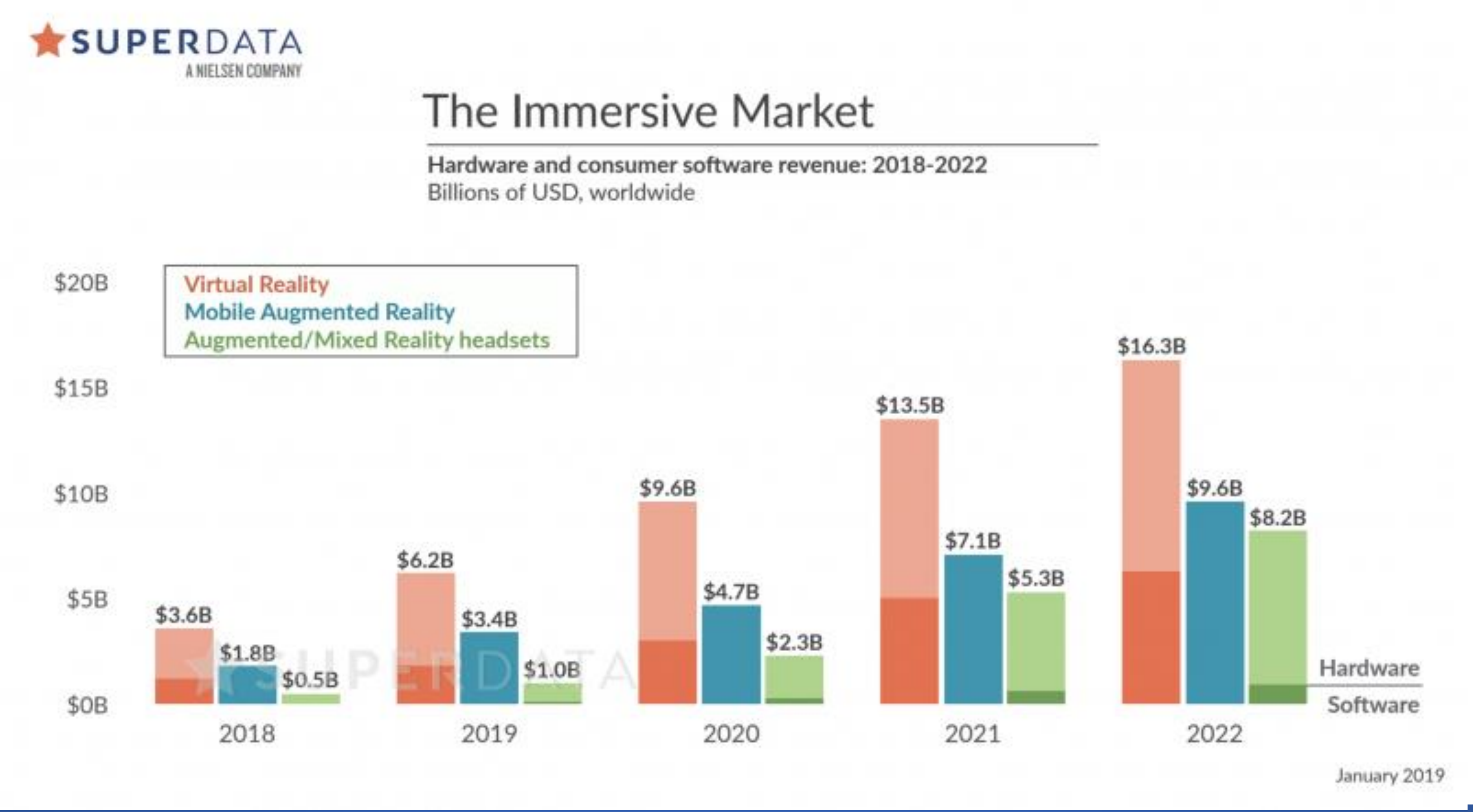
†San Diego State University

‡Zhejiang University

§SUNY Buffalo

Virtual Reality (VR) technology is boosting.

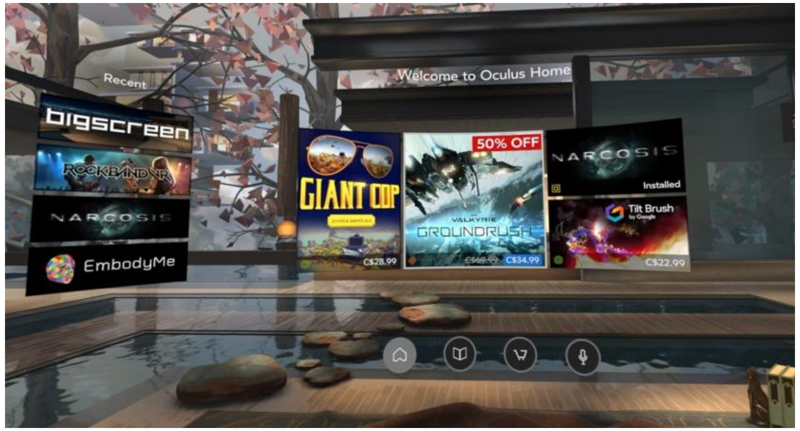
- The market size reached 3.6 billion dollars in 2018*.



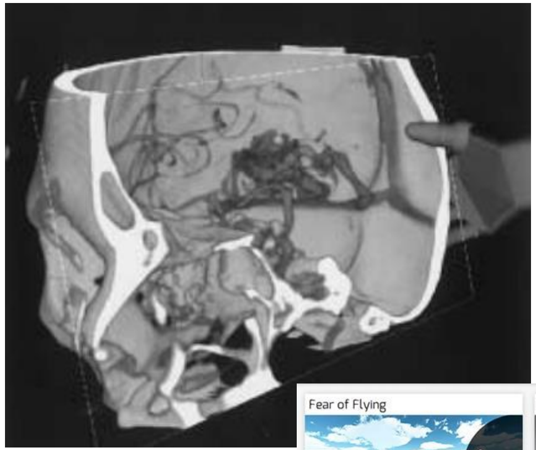
*Viar360, "Virtual reality market size in 2018 with forecast for 2019," 2019.

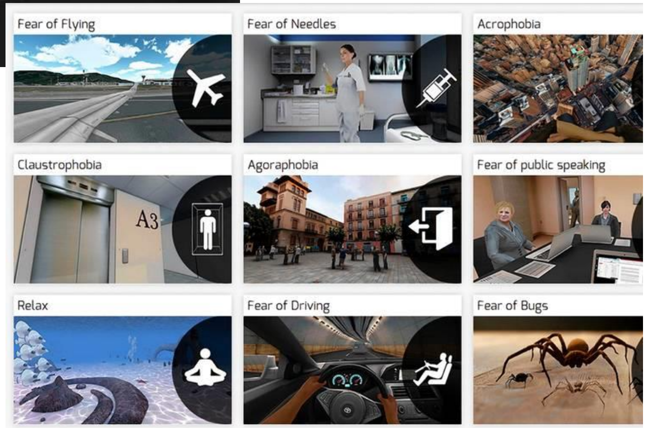
Diverse Applications

Entertainment



Healthcare





Military

Diverse Applications

Entertainment

Healthcare

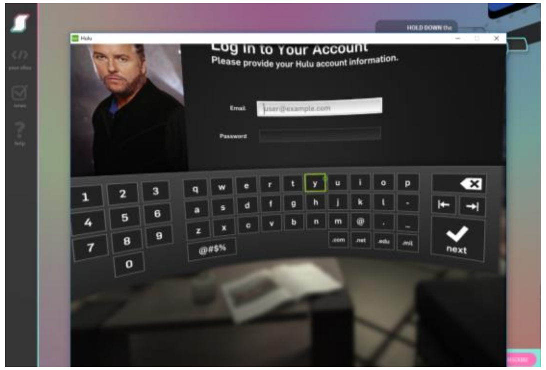
Military

Authentication System

- Protect HMD from unauthorized access.

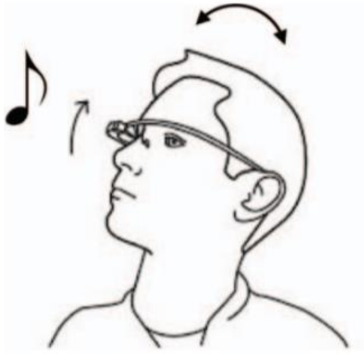
State-of-the-art Methods

Password

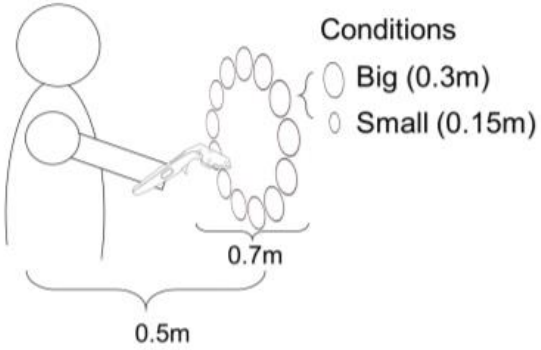


Unlock pattern

Head motion



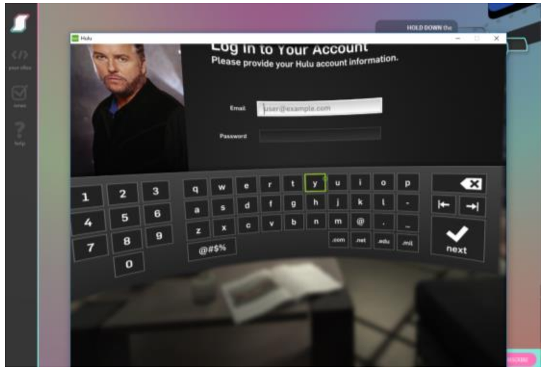
Body motion



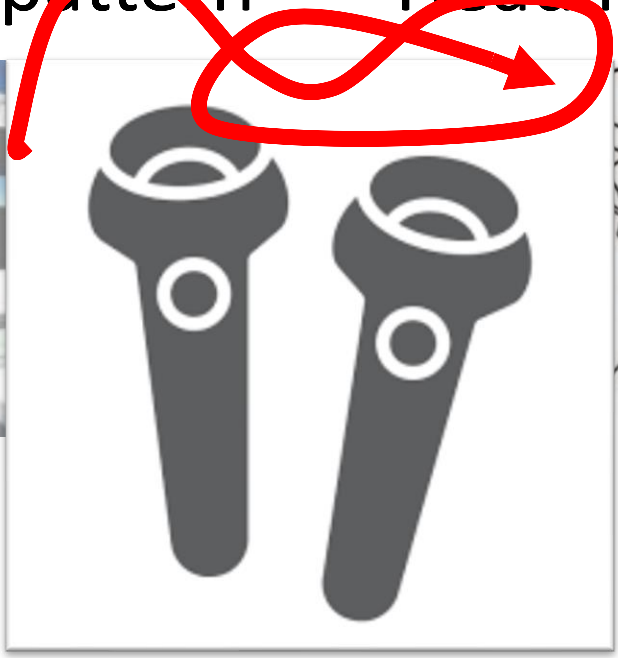
State-of-the-art Methods

- Expose authentication actions *.
- Behaviors change over time.

Password

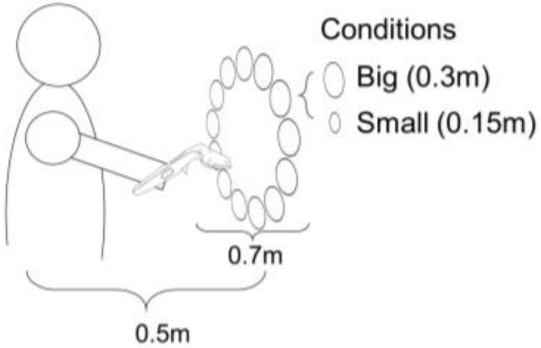


Unlock pattern



Head motion

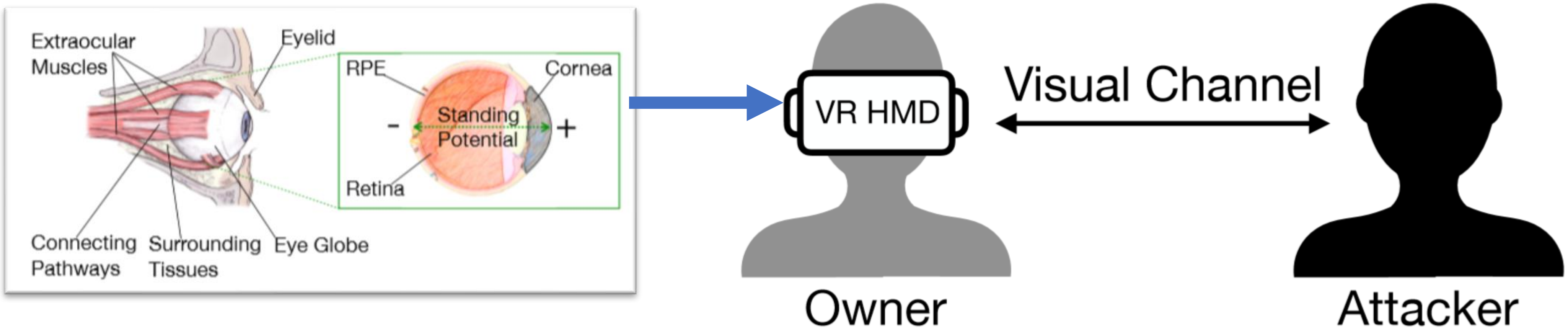
Body motion



*Ling, Zhen, Zupei Li, Chen Chen, Junzhou Luo, Wei Yu, and Xinwen Fu. "I Know What You Enter on Gear VR." In *2019 IEEE Conference on Communications and Network Security (CNS)*, pp. 241-249. IEEE, 2019.

Solution: Human Visual System (HVS) auth.

- An unobservable solution.
- Behavioral and physiological biometric.



Challenge 1: HVS Hard to Measure

- HVS components are hard to measure in VR HMD.
  - Limited space.
  - Dark environment.

Challenges 2: Redundant Training

- Each new user requires a new classifier.

user1 → Sample1, Sample2, …, Sample10 → classifier1

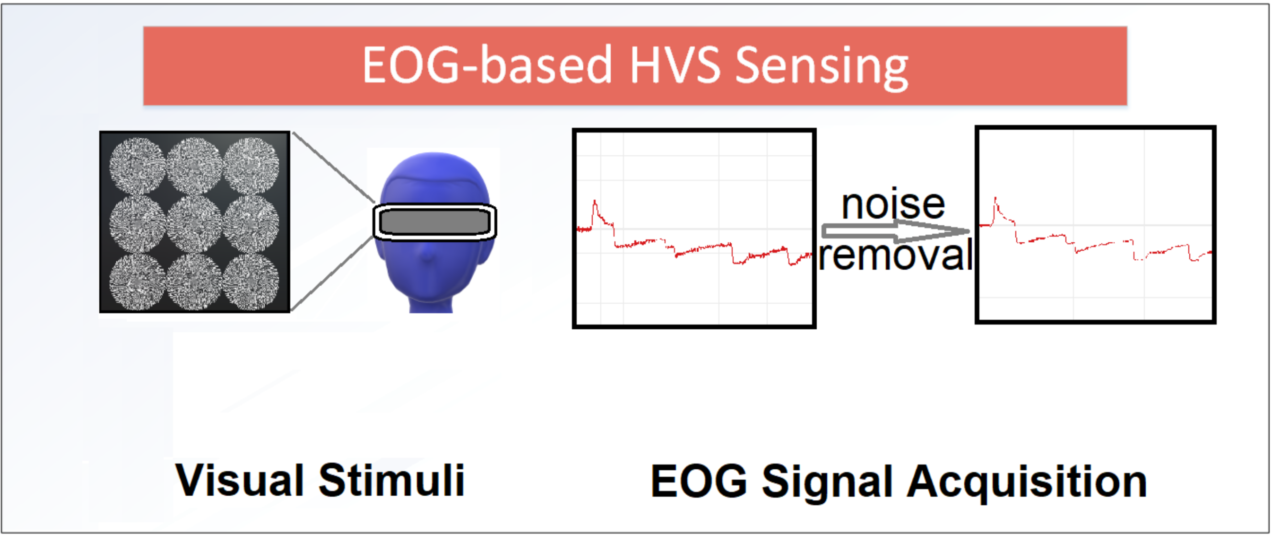
user2 → Sample11, Sample12, …, Sample20 → classifier2

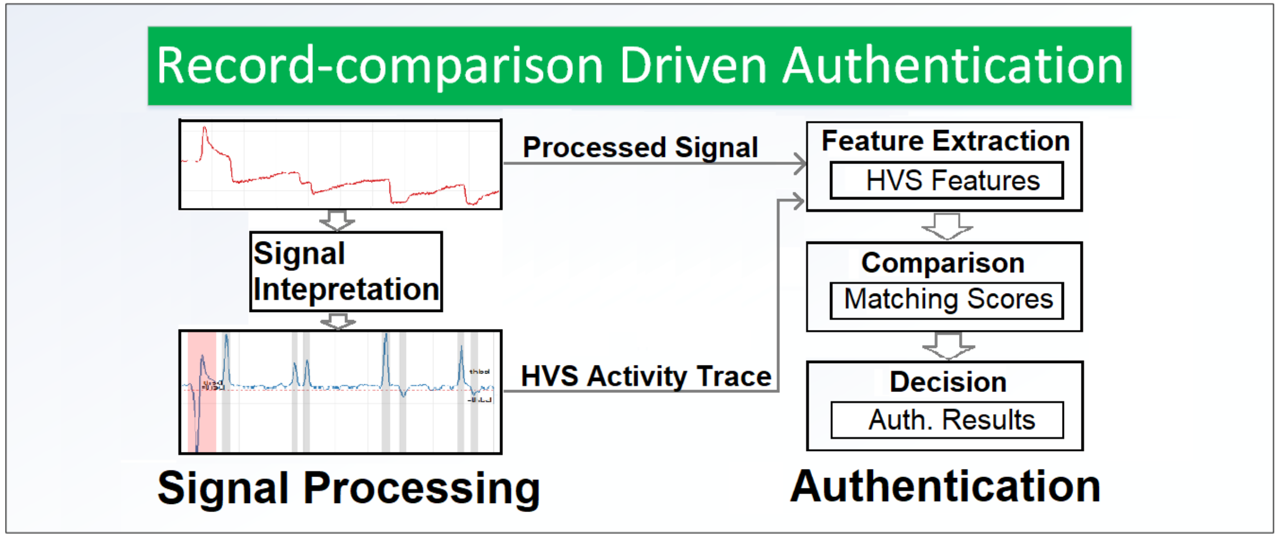
user3 → Sample21, Sample22, …, Sample30 → classifier3

… … …

System Architecture

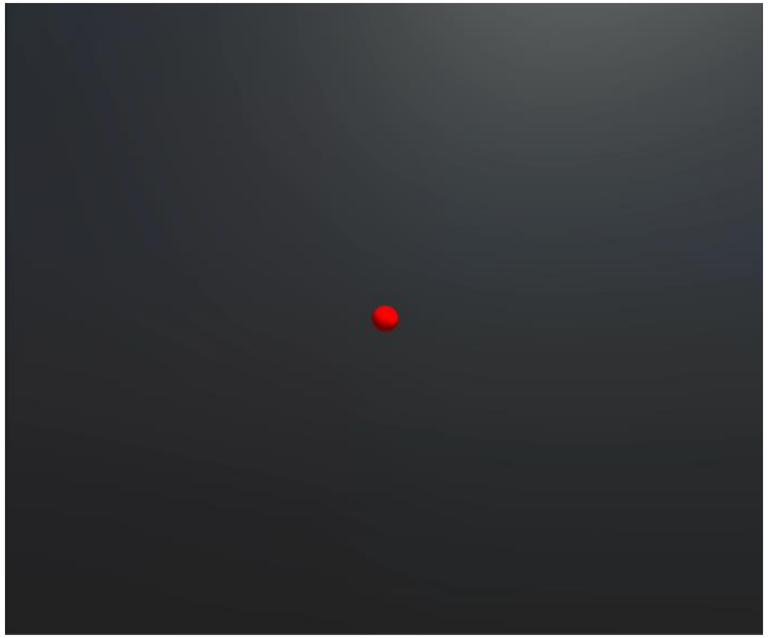
- Module 1: capture the electrical signals from HVS.
- Module 2: authenticate EOG samples based on similarity.





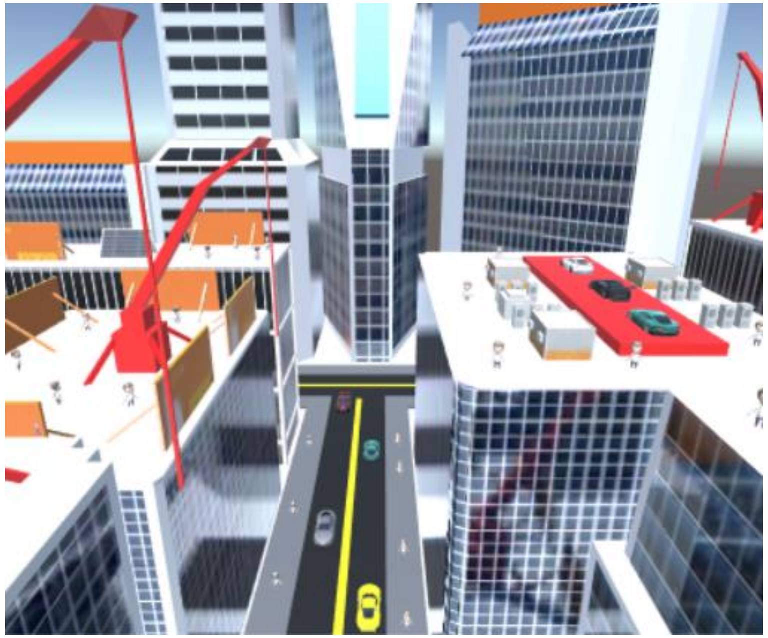
Module 1 - Visual Stimuli

Fixed-Route (FR)



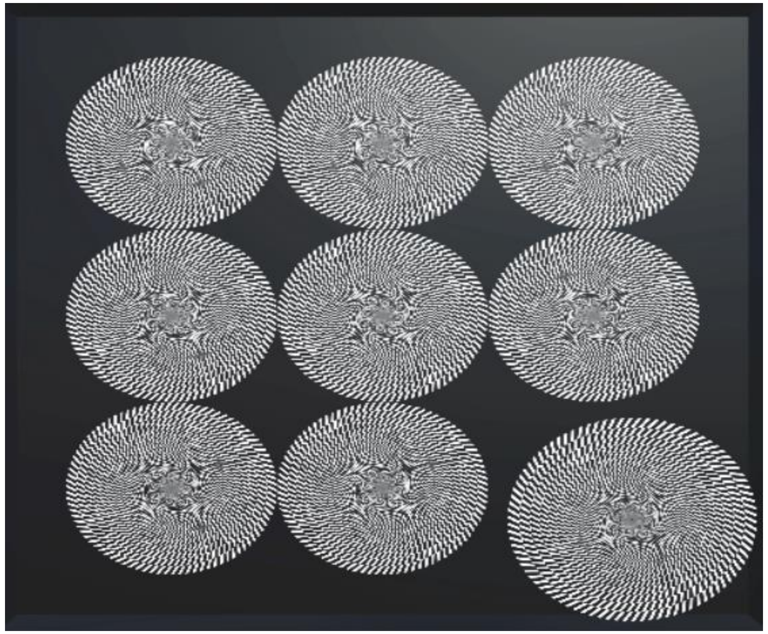
Eye rotation, blinks

City-Street (CS)



Scan path

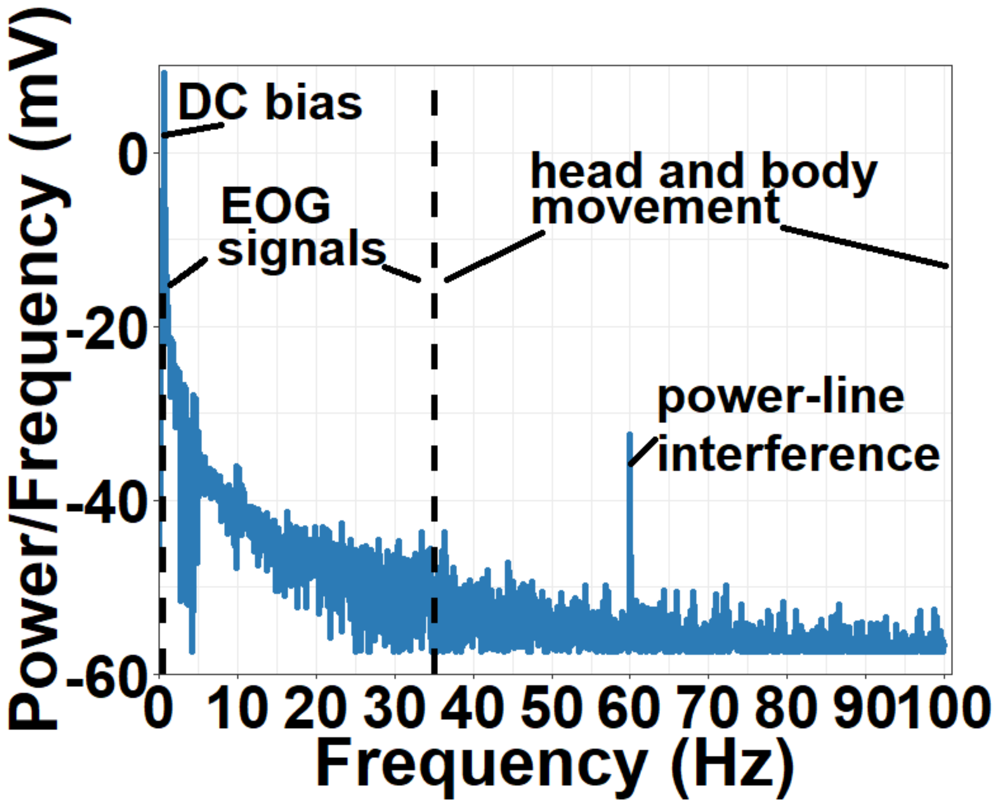
Illusion (IL)



Micro-saccades

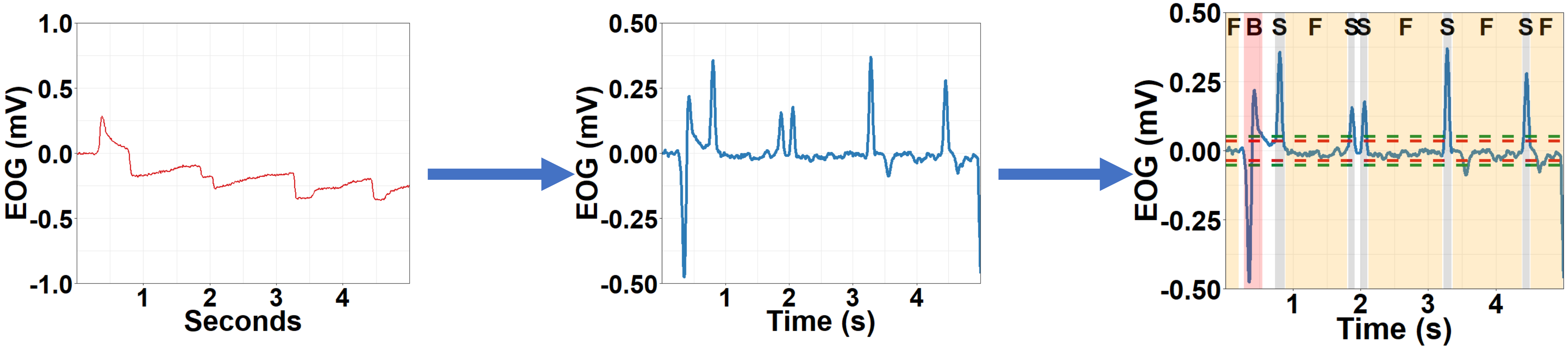
Module 1 - EOG Signal Acquisition

- Remove interference using filters.



Module 2 - Signal Processing

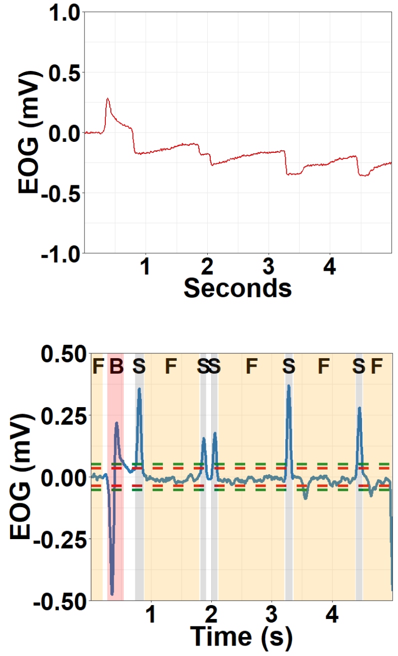
- Recognize saccades (S), fixations(F) and blinks(B).
  - Continuous wavelet transform algorithm*.



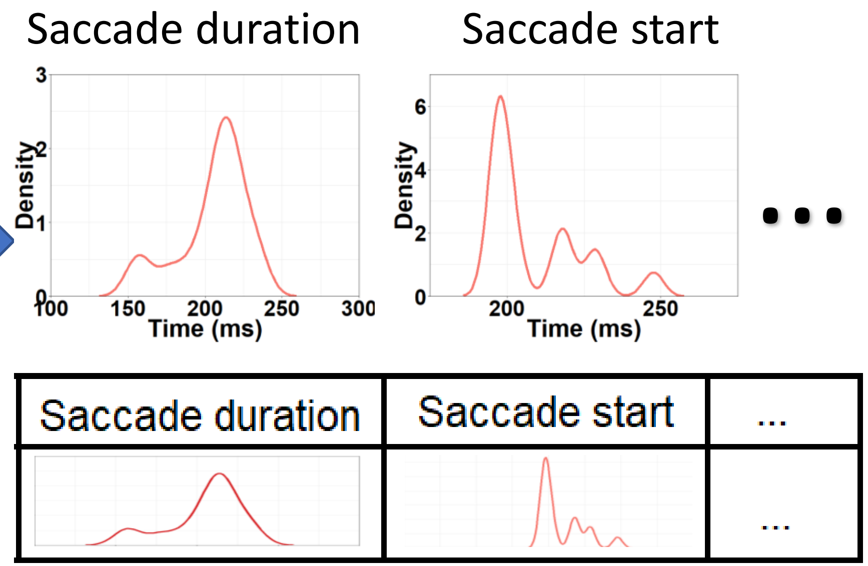
*A. Bulling, J. A. Ward, H. Gellersen, and G. Troster, "Eye movement analysis for activity recognition using electrooculography," IEEE transactions on pattern analysis and machine intelligence, 2010.

Module 2 - Authentication

- Extracts behavioral and physiological features from the EOG signal.

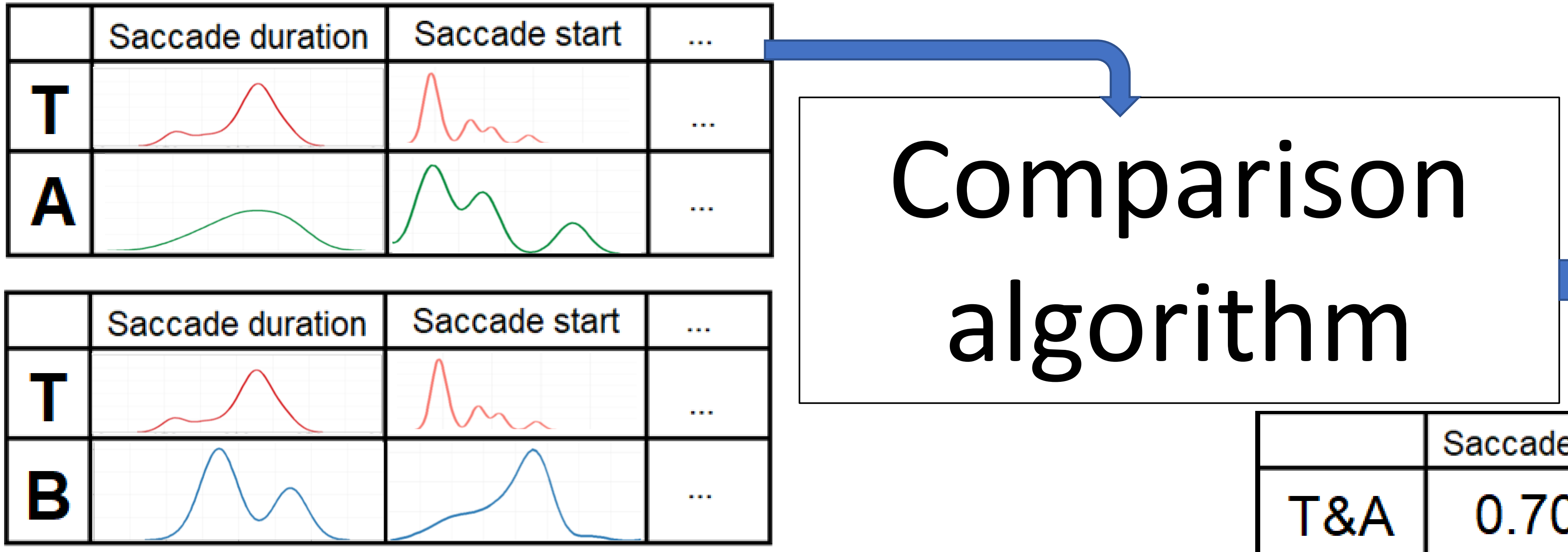


Behavioral features:
Saccade: duration, start time, location.
Fixation: duration, start time, centroid.
Physiological features:
Eyelid: close speed, open speed, stretch extent.
Metabolism intensity.
Rotation extent: right, left, up, down.



Module 2 - Authentication

- Compare sample A and B with template sample T.

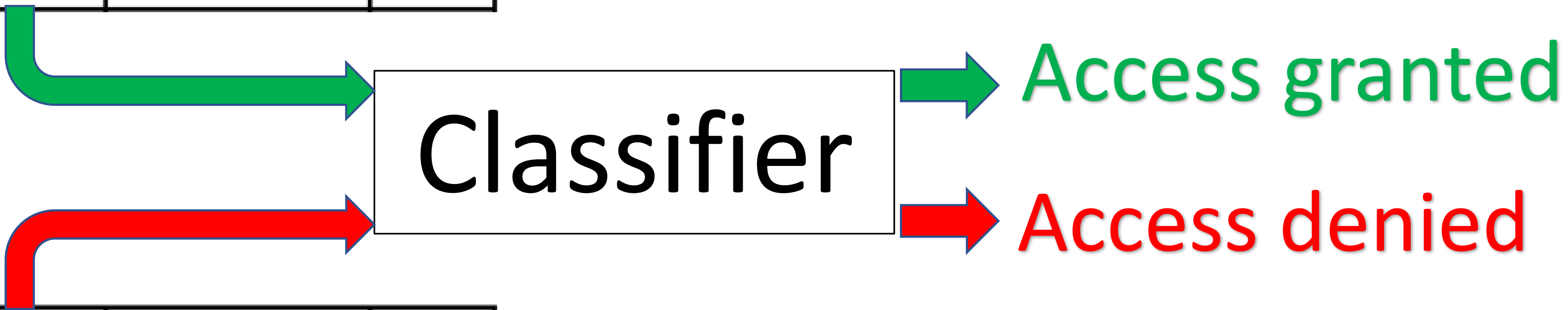


	Saccade duration	Saccade start	...
T&A	0.7067	0.8681	...
T&B	0.0908	0.1167	...

Module 2 - Authentication

- Are A and B the same as template?

	Saccade duration	Saccade start	...
T&A	0.7067	0.8681	...

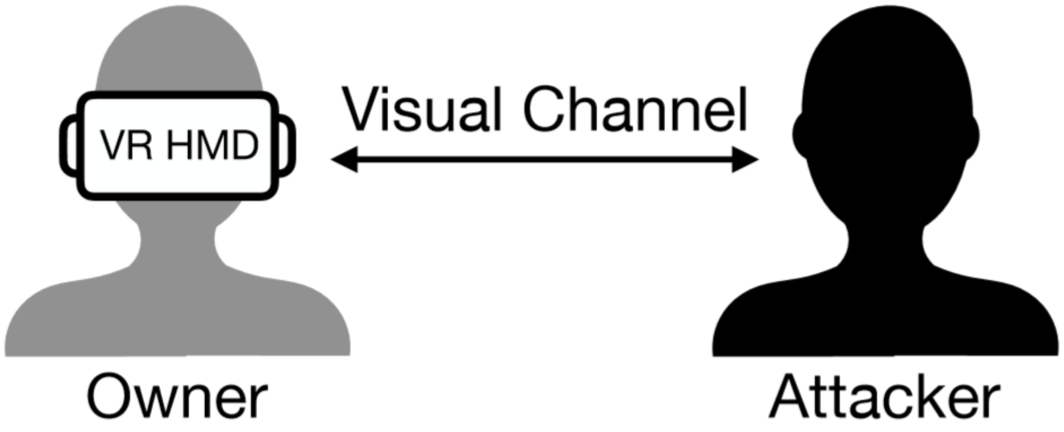


	Saccade duration	Saccade start	...
T&B	0.0908	0.1167	...

No need to re-train the classifier.

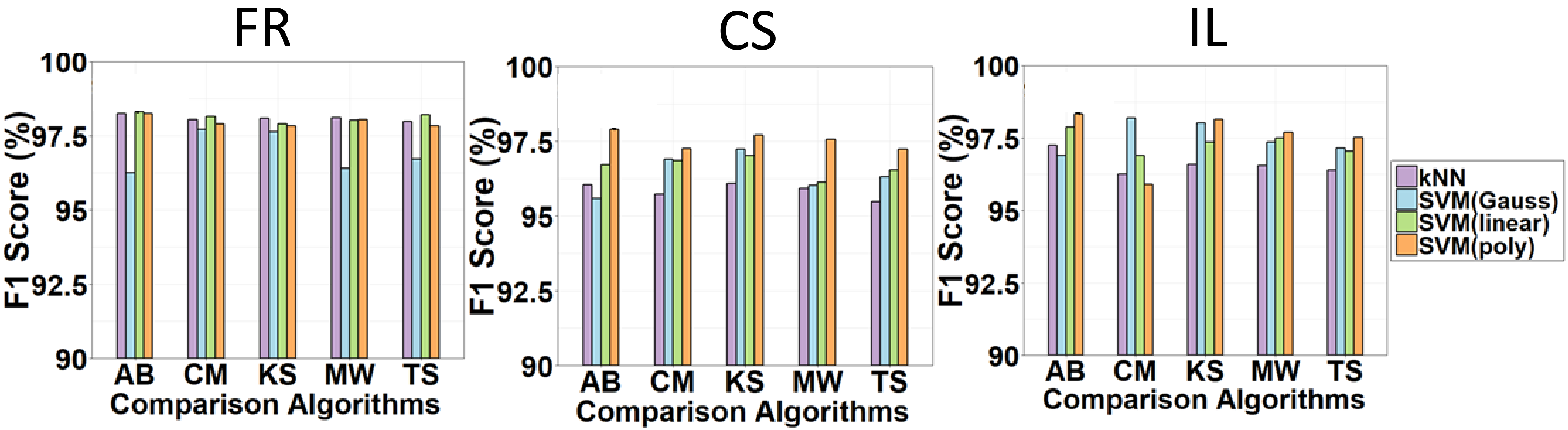
Experiment - Impersonation Attack

- 70 participants.
  - Each provides 10 records.
- Records are partitioned into training and testing sets.
  - 1:1, by subject.
  - In each set, 61075 comparison results (1575 positive, 59500 negative).



Experiment - Impersonation Attack

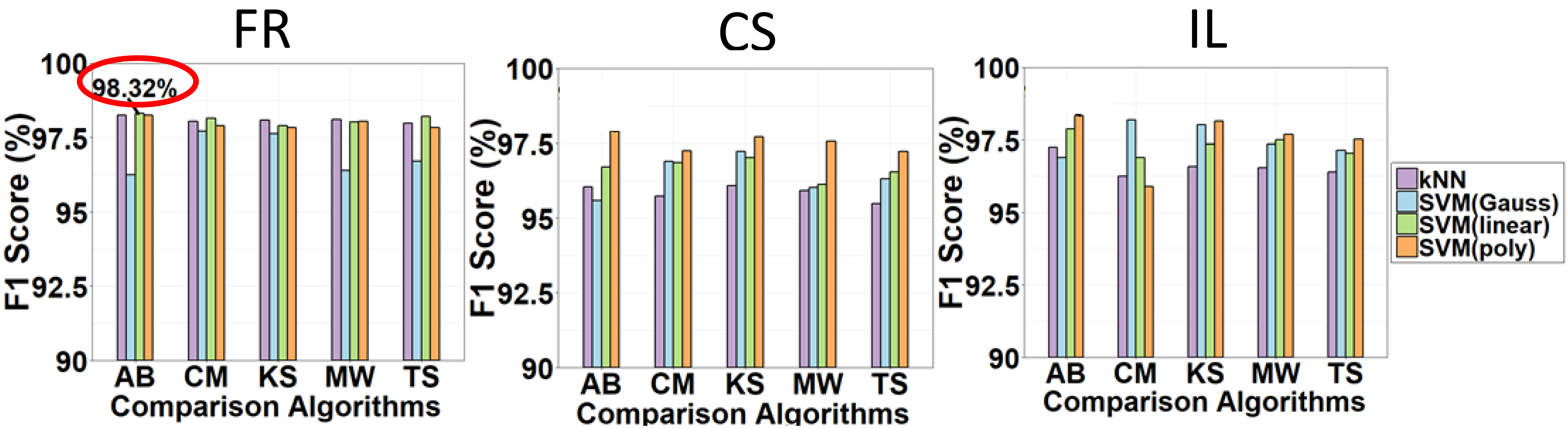
- F1 scores of all combinations of matching algorithm and classifiers.



Matching algorithms:
Ansari-Bradley test (AB); Mann-Whitney u-test (MW); Two-sample Kolmogorov-Smirnov test (KS); Two-sample Cramer-von Mises test (CM); Two-sample t-test (TS).

Experiment - Impersonation Attack

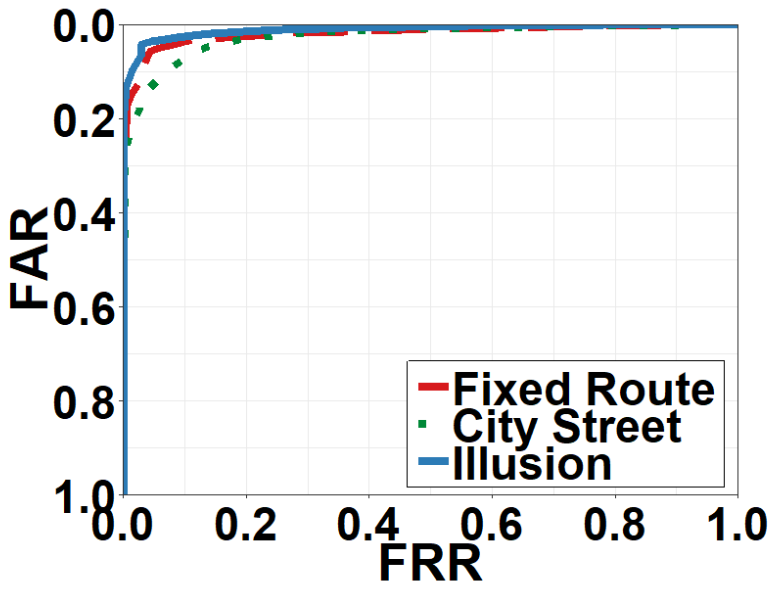
- Best F1 score using AB Test and SVM (linear).



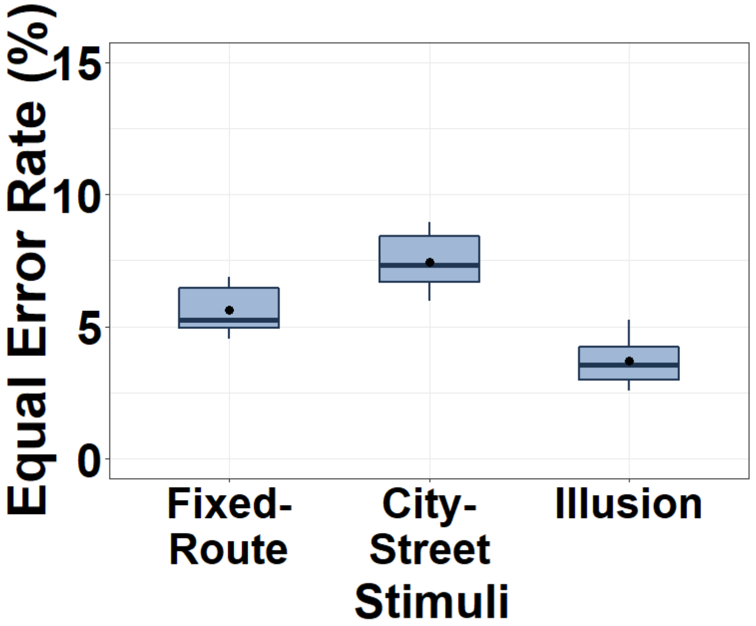
Matching algorithms:
Ansari-Bradley test (AB); Mann-Whitney u-test (MW); Two-sample Kolmogorov-Smirnov test (KS); Two-sample Cramer-von Mises test (CM); Two-sample t-test (TS).

Experiment - Impersonation Attack

- Low equal error rate: EER(FR)=5.27%; EER(CS)=7.32%; EER(IL)=3.55%.



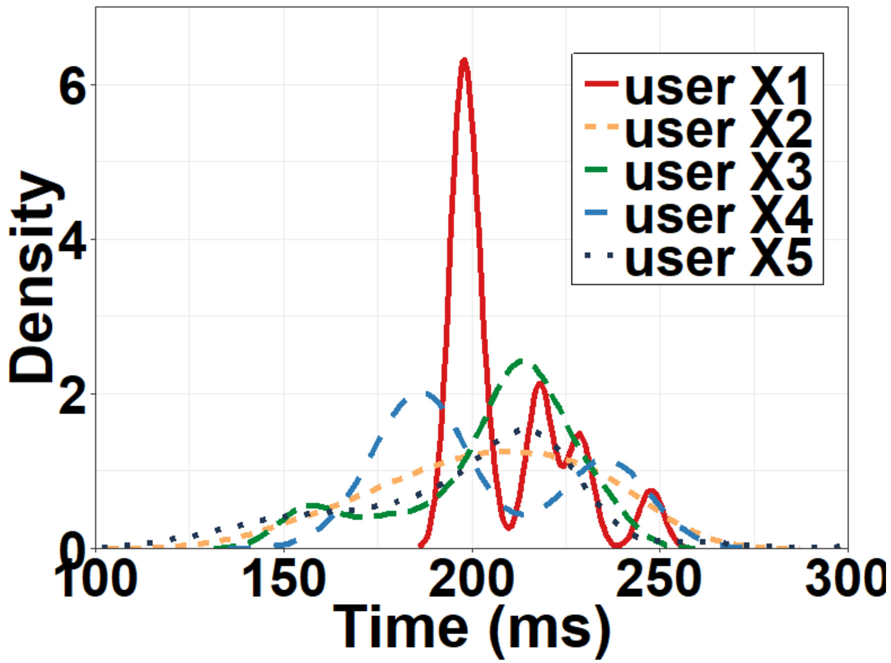
Receiver Operating Characteristic (ROC)



Equal Error Rate (EER)

Experiment - Statistical Attack

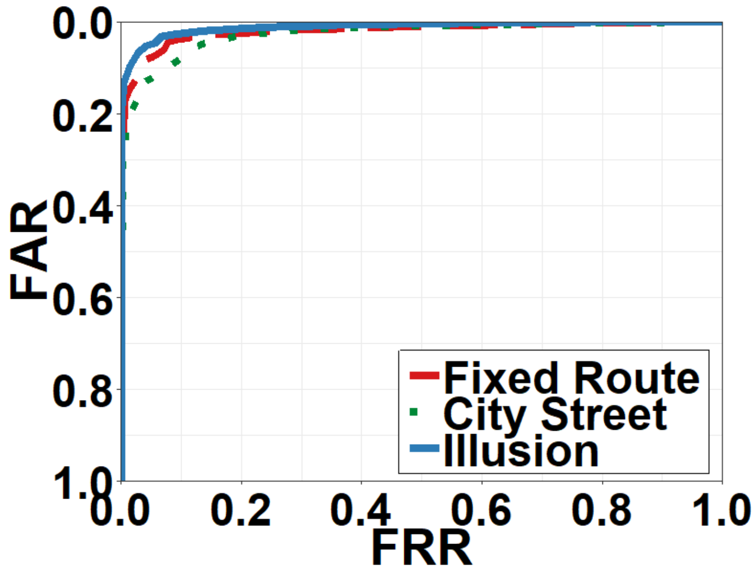
- The attacker calculates the PDF of features from users, then uses the most probable feature values to generate the forgery.



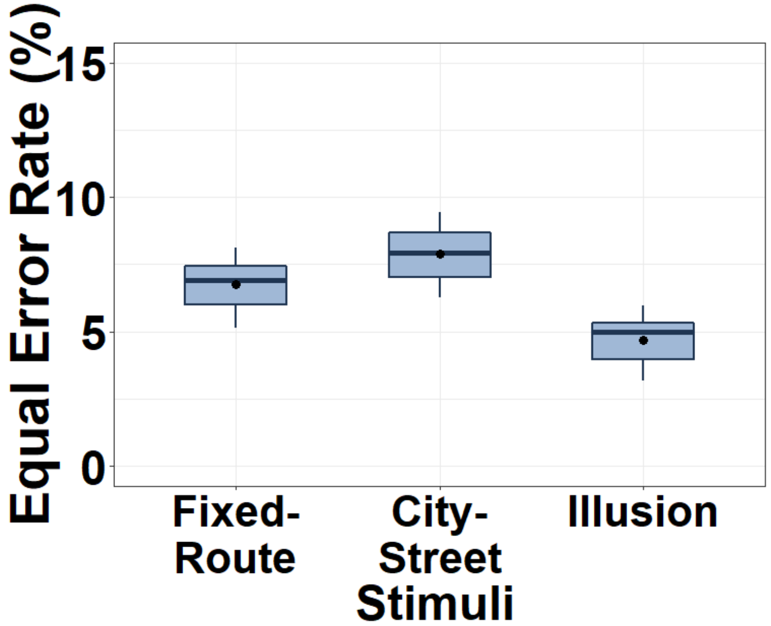
...

Experiment - Statistical Attack

- Low impact at equal error rate: EER(FR)=6.93%; EER(CS)=7.93%; EER(IL)=4.97%.



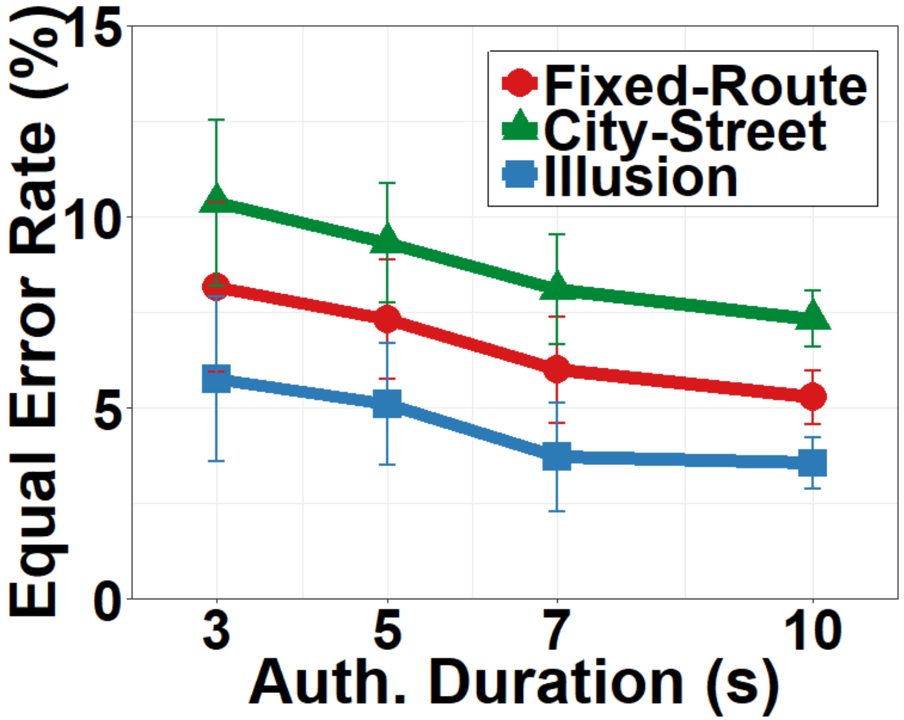
ROC



EER

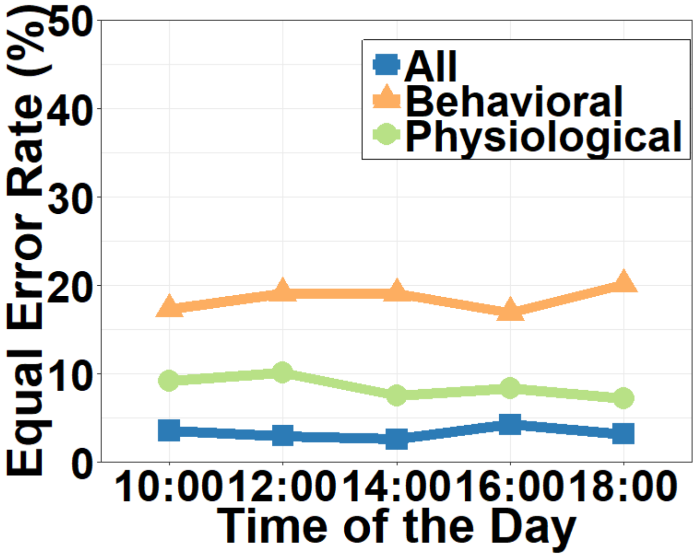
Experiment - Time Efficiency

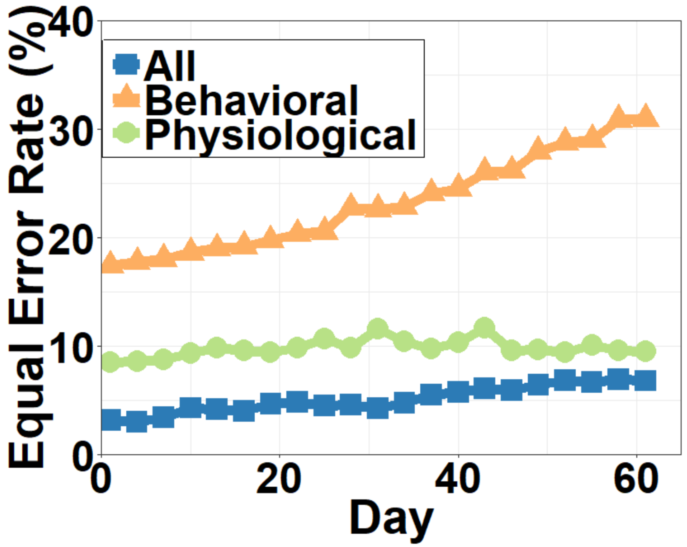
- Trade-off between security and convenience.



Experiment - Temporal Stability

- 5 participants.
- The accuracy is stable.





Conclusion

- We propose an EOG-based framework to measure the HVS as a whole for VR authentication.
- We design a record-comparison driven authentication scheme.
- We perform an extensive evaluation of the proposed OcuLock system.

Thank you