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

Shiqing Luo, Anh Nguyen, Chen Song, Feng Lin, Wenyao Zu, and Zhisheng Yan
Georgia State University, San Diego State University, Zhejiang University, SUNY Buffalo

Presenter: Brandon Falk (119033990001)

Accessing Private Data

01 **Background**

Contributions

02 **Oculock**

How it works

03 **Threat Model & Architecture**

Impersonation Attack

Statistical Attack

04 **Experiment**

Impersonation Attack

Statistical Attack

05 **Discussion**

Background 01

Background (1/2)

Using VR Modalities [Remote Controller, Head Navigation] to infer Authentication Input

- Such as PIN, Char Passwords, etc

Head-mounted Display (HMD) - Covers users' eye area

- Exploit Human Visual System (HVS) Biometric Authentication

Previous works used Eye Globe Movements (gaze/stare)

- High error rate, not stable, depends on user condition (i.e. drunk)

This paper considers more than just the eye

- eyelid, extraocular muscles, cells, and surrounding nerves in the HVS

Background (2/3)

This paper presents OcuLock

- HVS-based system for reliable and unobservable VR HMD authentication *(Main Idea of Paper)*

- Using electrooculography (EOG) based HVS sensing framework and a record-comparison driven authentication scheme.
  - Experiments: 70 subjects show that
    - OcuLock is resistant against common types of attacks
      - impersonation attack and statistical attack
        - Equal Error Rates as low as 3.55% and 4.97% respectively.

Background (3/3)

Applications of VR?

- Healthcare, Education, Military, Sensitive Data
  - All can be accessed through (HMD)
    - Examples:
      - Sensitive Data:
        - Credit Card information is stored in HMD to purchase games
      - Hospital
        - CT Scan Models from hospitals is stored in HMD
      - Military
        - Top Secret Aircraft Simulations in VR

Security Weaknesses

- Adversaries have successfully conducted side-channel attacks by observing user input behavior and inferring the virtual input
- Wearing HMD blocks users' real-world visuals and decreases their situation awareness
- The threat of observation-based attacks in VR is significantly higher than that in traditional computing devices

Contributions of Paper

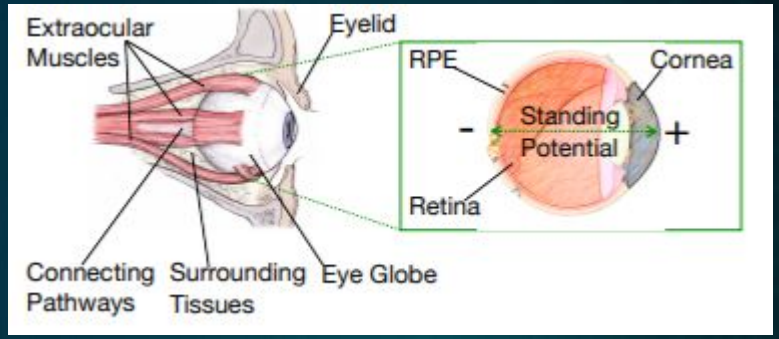
- Propose an EOG-based framework to measure the HVS as a whole for VR authentication, where visual stimuli are designed to trigger the HVS response and EOG is collected to characterize the HVS.

- Design a record-comparison driven authentication scheme, where distinctive behavioral and physiological features are extracted and accurate authentication decisions are made.

- Perform an extensive evaluation of the proposed OcuLock system including reliability performance of the authentication, security analysis against several attacks, and user study of VR HMD authentication.

Oculock 02

Oculock



Most devices capture *eye globe movement* (high-level detail)

- Oculock captures low-level detail
  - Trigger Cells and Nerves through immersive VR content
- ***Paper proposes*** an electrooculography (EOG) based HVS sensing framework for VR
  - EOG measures the electrical signals resulted from biological activities in the HVS and can characterize both behavioral and physiological features of the HVS in VR environment
    - Attach thin electrodes within VR headset
    - Design visual stimuli

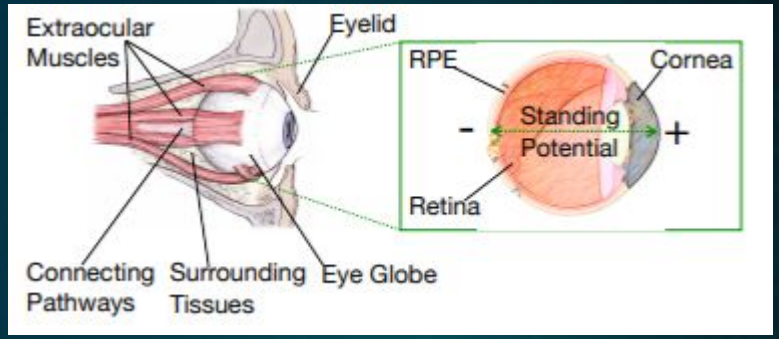
Oculock

Previous works

- Previous biometric systems [29], [19], [7] trained a two-class classifier to differentiate the owner and others, but a new model had to be trained for every new owner.

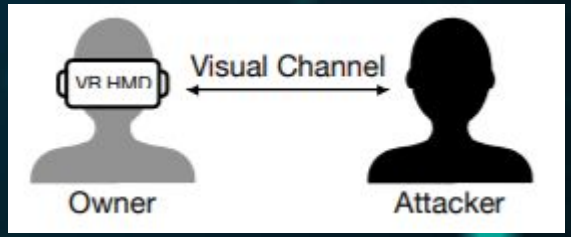
How it works

- size, shape, position, and anatomy of the HVS and their daily interaction present unique features that can distinguish people
- Sympathetic signals transported to the eyes show unique energy patterns dependent on the biostructure of people's sympathetic nerves
- HVS contains unique physiological biostructure and voluntary movement to authenticate VR users



EOG Templates stored in HMD

- Visually, attacker cannot see the face / eyes of the user.



Threat Model & Architecture

03

Threat Model

Objective: Input EOG either directly or indirectly to the VR HMD in order to bypass the authentication. The following were considered

- Enough time and space to do attacks
  - Attacker can steal the device
    - Attacker does not...
      - install malware
      - use external device
        - i.e. attacker using antenna to capture electromagnetic pulses from user
    - Attacker does...
      - Utilize other methods to indirectly obtain information related to user input
        - i.e. statistical attack, impersonation attack

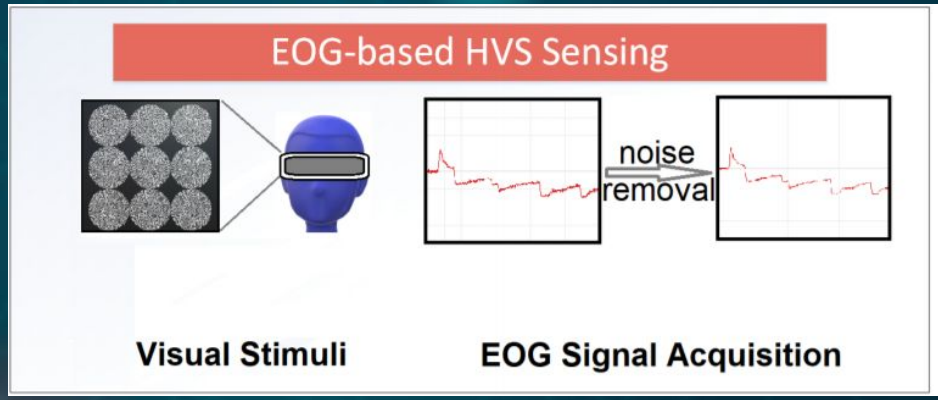
Impersonation Attack

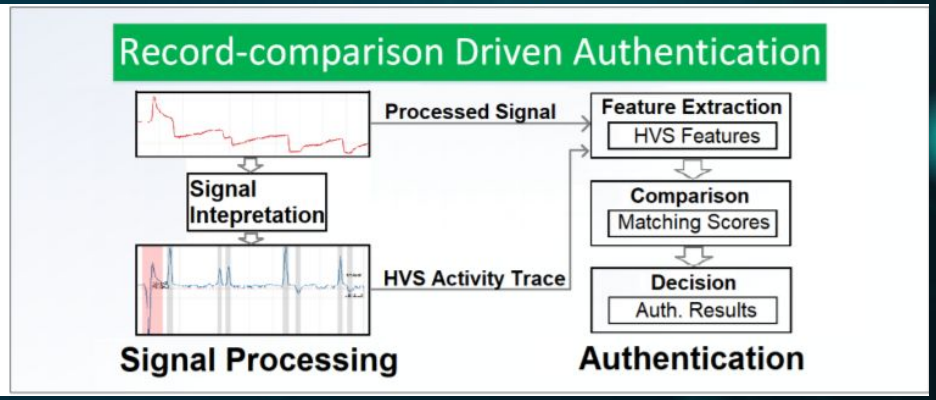
- Observe the victim and attempt to repeat the victim's actions with attacker's own EOG signal.

Statistical Attack

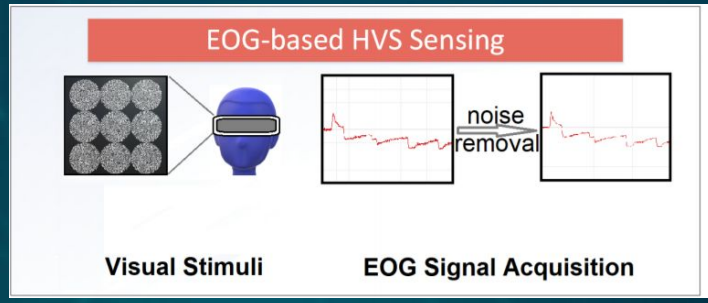
- Acquire EOG records from victim
  - Attacker forges new EOG records based on similarities
    - i.e. Collect college student EOG records for a population of college students using HMD Authentication
  - Use voltage generator or inject signal

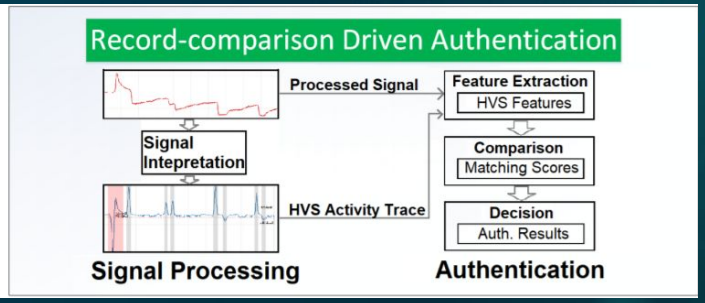
Architecture

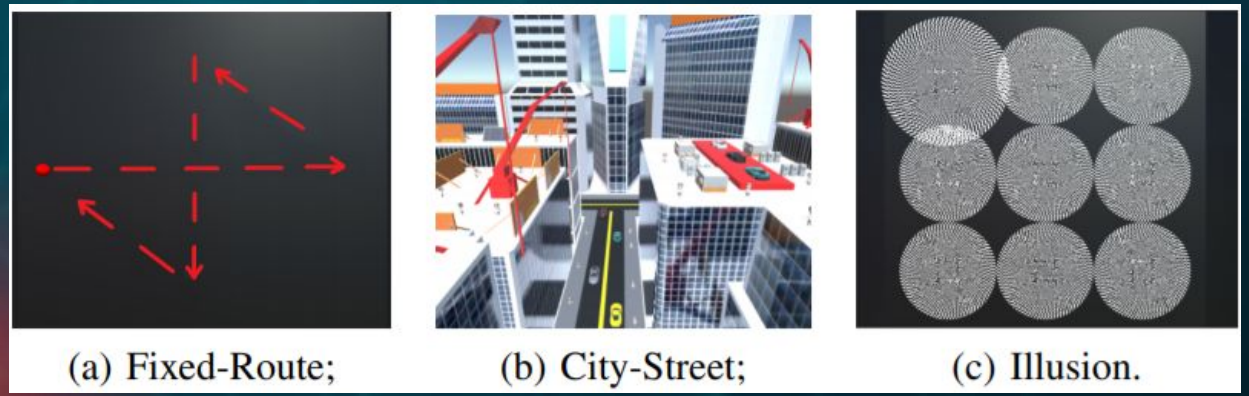




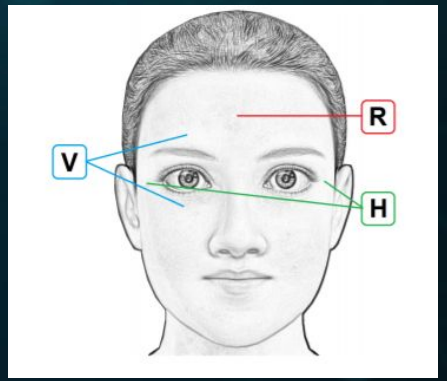
Architecture



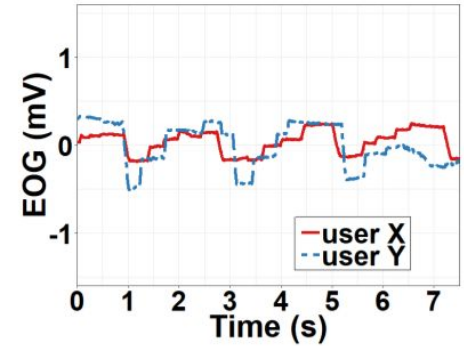




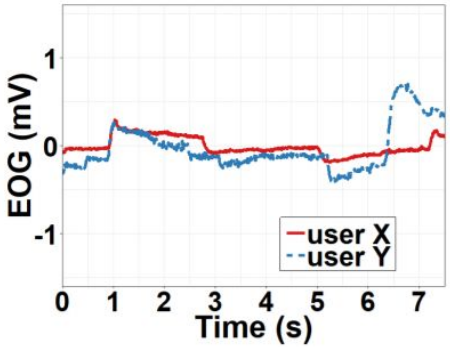
(a) Fixed-Route; (b) City-Street; (c) Illusion.



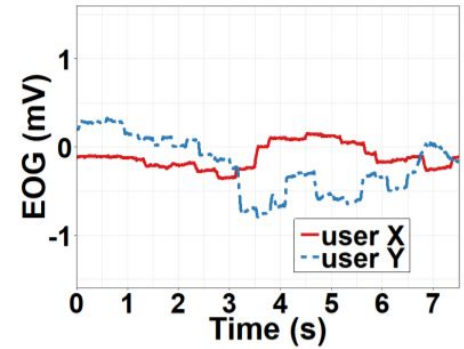
Architecture



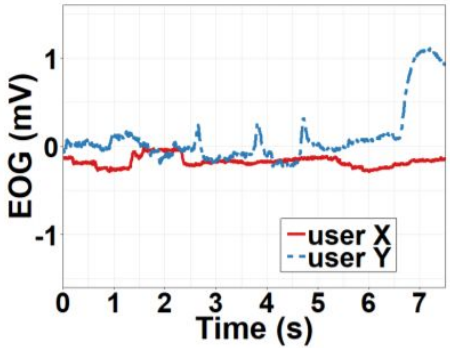
(a) Fixed-Route, EOG_h



(b) Fixed-Route, EOG_v



(c) City-Street, EOG_h



(d) City-Street, EOG_v

Architecture

TABLE I: List of HVS features in OcuLock ("V"=Vertical; "H"=Horizontal).

Index	Name	EOG-based Calculation	Category	Component
1	Eyelid Close Speed	Slope of EOG signal during blink close phase.	Physiological	V
2	Eyelid Open Speed	Slope of EOG signal during blink open phase.	Physiological	V
3	Eyelid Stretch Extent	Amplitude of EOG signal during blink close phase.	Physiological	V
4 & 5	Metabolism Intensity	Arden Ratio (AR).	Physiological	H & V
6	Extent of Right Rota. Dist.	Max amplitude of positive EOG/AR.	Physiological	H
7	Extent of Left Rota. Dist.	Max amplitude of negative EOG/AR.	Physiological	H
8	Extent of Up Rota. Dist.	Max amplitude of positive EOG/AR.	Physiological	V
9	Extent of Down Rota. Dist.	Max amplitude of negative EOG/AR.	Physiological	V
10 & 11	Sympathetic Energy	Wavelet transform amplitude from 0.05 to 0.5 Hz.	Physiological	H & V
12 & 13	Fixation Start Time	Start time of fixation.	Behavioral	H & V
14 & 15	Fixation Duration	Duration of fixation.	Behavioral	H & V
16 & 17	Fixation Centroid	Average EOG amplitude during a fixation.	Behavioral	H & V
18 & 19	Saccade Start Time	Start time of saccade.	Behavioral	H & V
20 & 21	Saccade Duration	Duration of saccade.	Behavioral	H & V
22 & 23	Saccade Location	5-point sampling of saccade path.	Behavioral	H & V

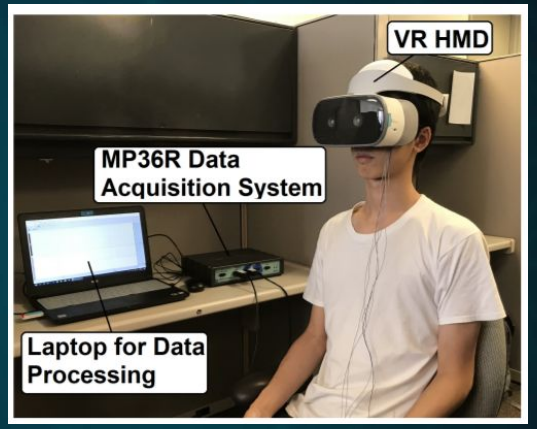
Experiment & Conclusion

04

Experiment

70 individuals tested

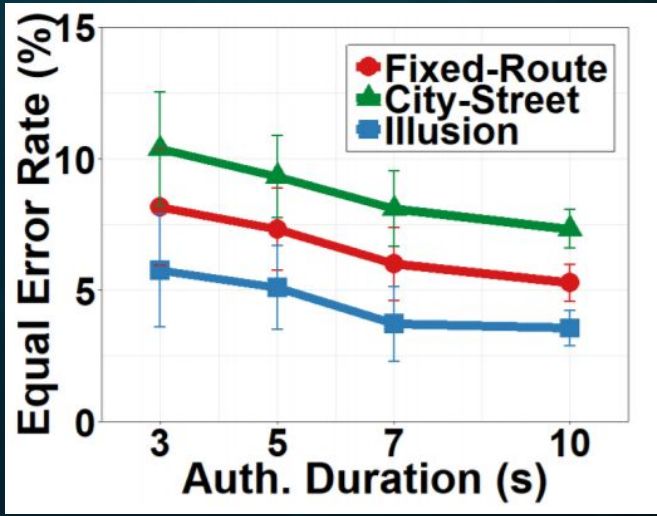
- **700 EOG Records per person, shown visual stimuli**



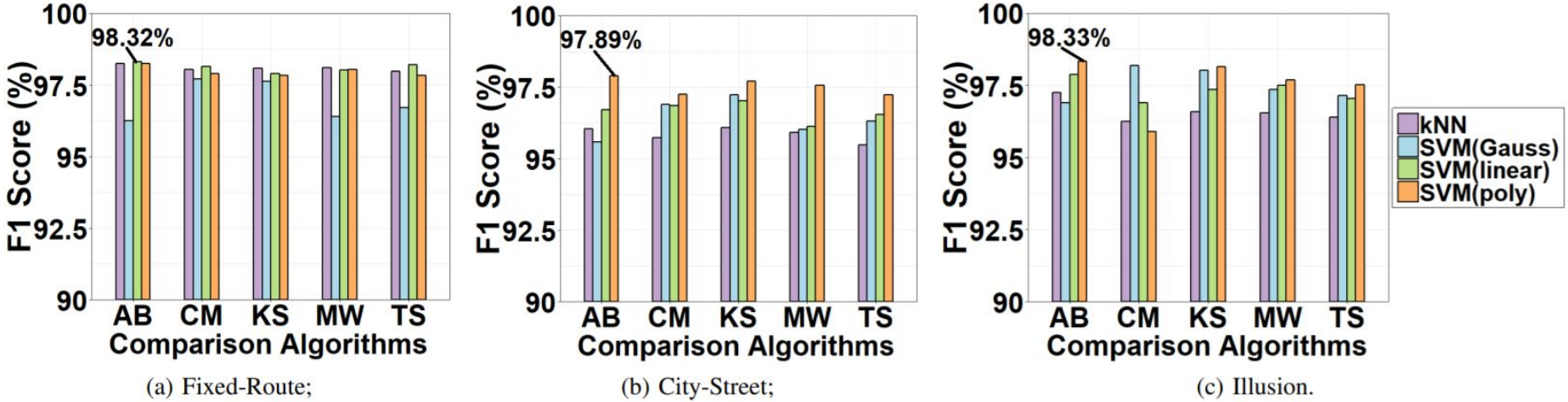
(Shown on Next Slide) To prove uniqueness in the values

Different comparator models including

- **k-nearest neighbors algorithm (kNN), a Support Vector Machine (SVM) using the Gaussian radial basis function as the kernel, an SVM using a linear kernel, and an SVM using a polynomial (poly) kernel.**
- **Multiple comparison algorithms including Ansari-Bradley Test (AB), Two-Sample Cramer-von Mises Test (CM), Two-Sample Kolmogorov-Smirnov Test (KS), Mann-Whitney U-Test(MW), and Two-Sample t-test (TS) [20] are also tested**



Experiment



(a) Fixed-Route; (b) City-Street; (c) Illusion.

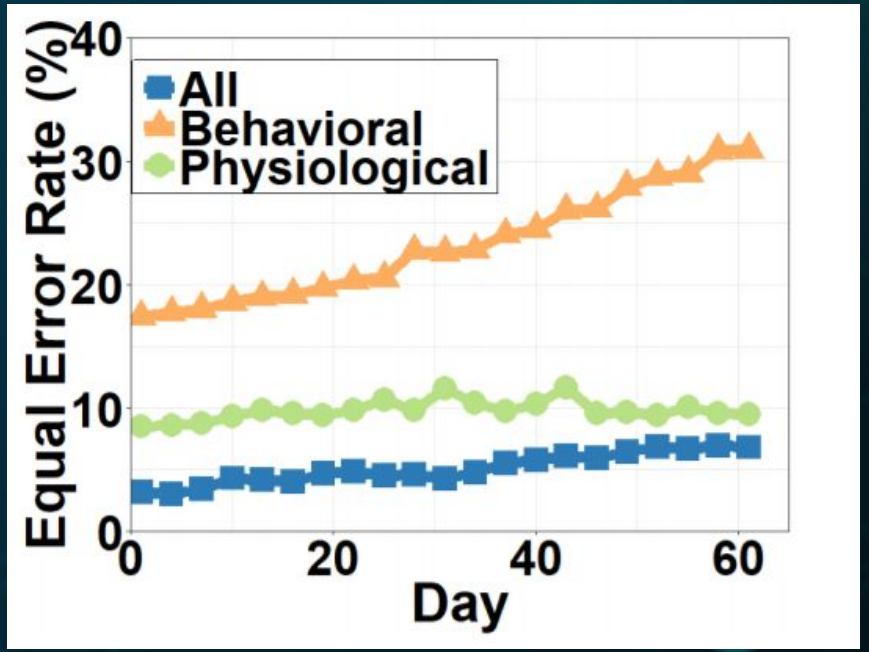
Fig. 11: F1 scores for three stimuli using different comparison algorithms and comparator models.

- **The F1 scores reach ~ 98% due to the unique and comprehensive features considered in OcuLock. AB Test also achieves better performance. This is because many proposed features are distributions rather than scalar numbers**

Experiment Interesting Observation

Physiological more reliable than Behavioral

- **EOG more reliable than staring**
  - **No fluctuations meaning eye tiredness or mood does not affect results**
  - **Low-level features can be triggered by VR immersion effectively**

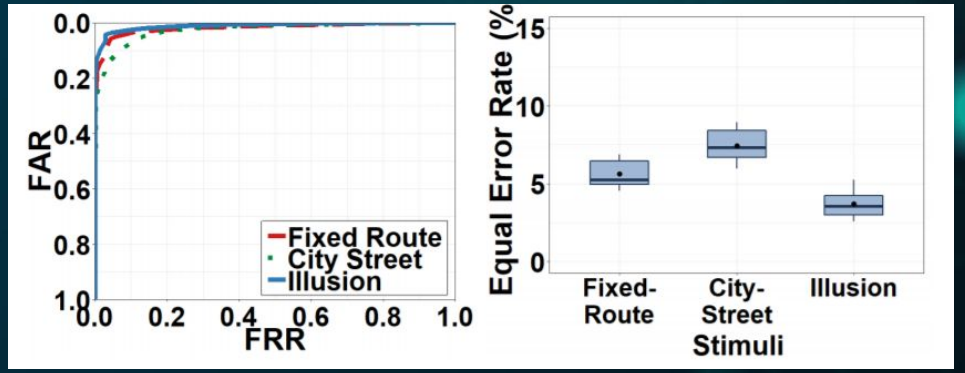


Experiment Impersonation Attack

AUC values for ROC curves 97.62%, 96.08% and 98.31% accuracy in distinguishing uniqueness between the user and attacker

Low-level HVS information more accurate if

- More / constant stimuli presented
  - Tracking
- City-street Stimuli had limited tracking
  - Higher EER

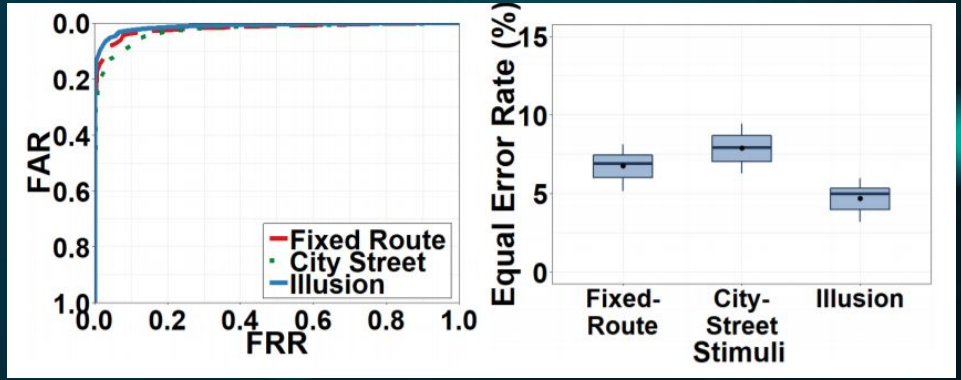


Experiment
Statistical Attack

First - All 70 participant records were compared together, only 45 positive samples. / 70,000

Second - Forged EOG attack - 3,000 Positive samples, 105,000 negative samples

AUC values for ROC curves 96.11%, 94.78% and 96.23% accuracy in distinguishing uniqueness between the user and attacker



- The AUC score for statistical attack is lower than impersonation attack by a small amount suggesting this type of attack is stronger but does not severely affect the model performance

Discussion

05

Discussion

- Related Works
  - Focus on AR, Gestures, Graphical Passwords, Remote Input
    - Suffer from high error rates
      - Oculink improves on this tremendously
  - Eye-based Authentication
    - Staring, Scanning, Patterns (High-Level)
      - Oculink focuses on (Low-Level)
  - EOG Patterns
    - Oculink is first to implement this
- Advanced Attacks
  - Replay Attack - Claims highly unlikely due to HMD preventing attacker from replaying their expressions
    - Obtain EOG Template - Use voltage generator produce exact same EOG
      - Proposes to adopt sensors to prevent this
      - Attacker builds Artificial Eye contain all HVS functionality. Out-of-reach with current tech.