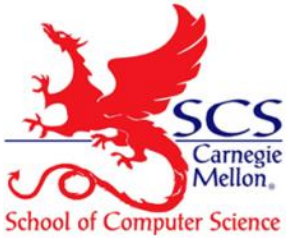
Whose Move is it Anyway? Authenticating Smart Wearable Devices Using Unique Head Movement Patterns

Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu,
Janne Lindqvist, Macro Gruteser

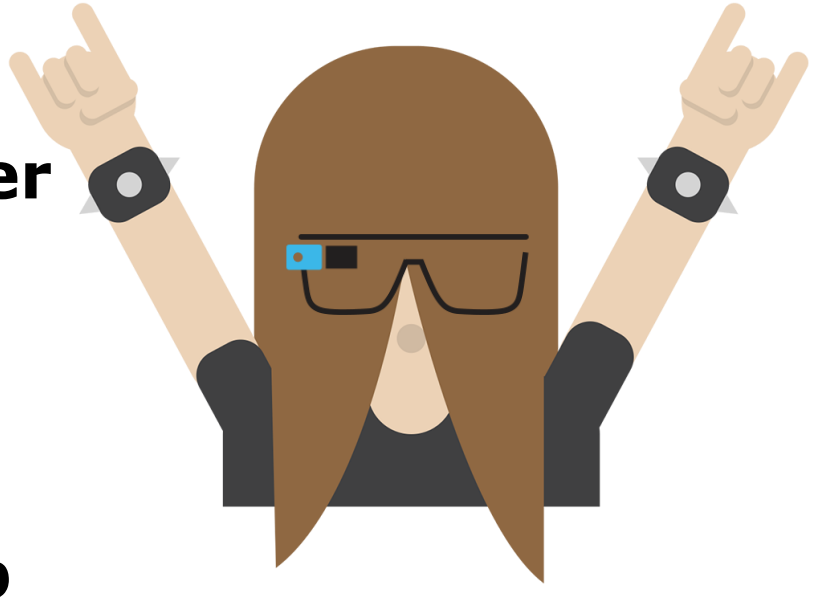
WINLAB

PerCom 2016



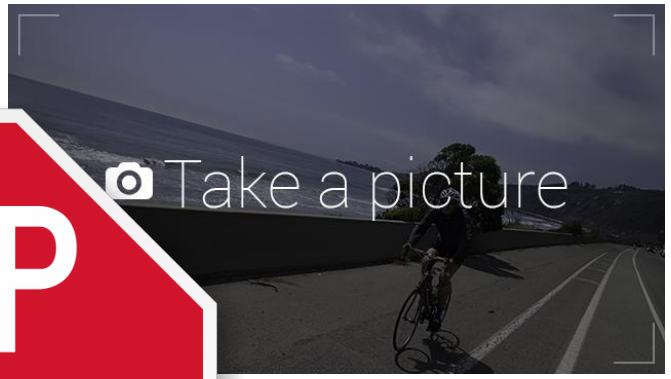
Project Highlights

- **We design HeadBanger**
- **We achieve accurate user authentication**
  - Experiment with 95 subjects
  - High TPR and Low FAR
  - Robust against Attack
- **We build an running app on Google Glass**

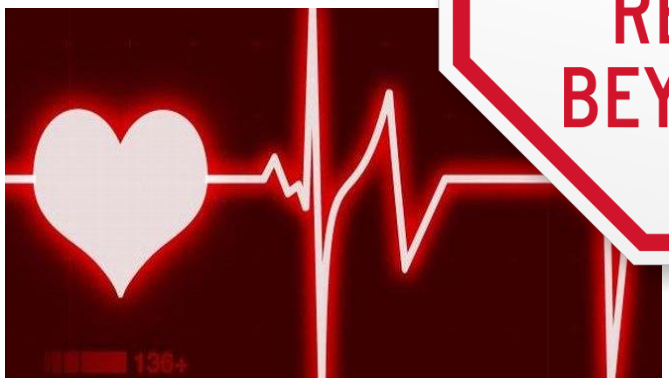


Personal Information Is in Your Wearables !

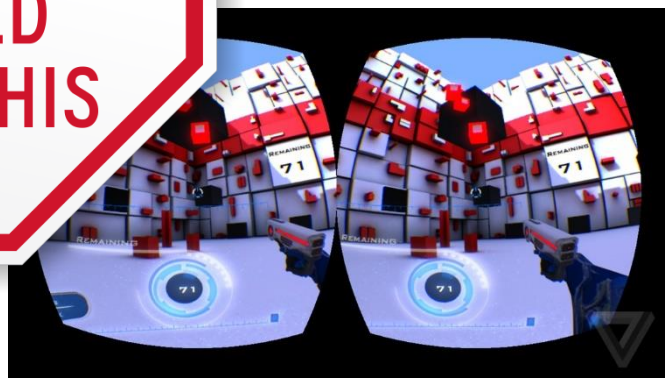
Locati



re & Video



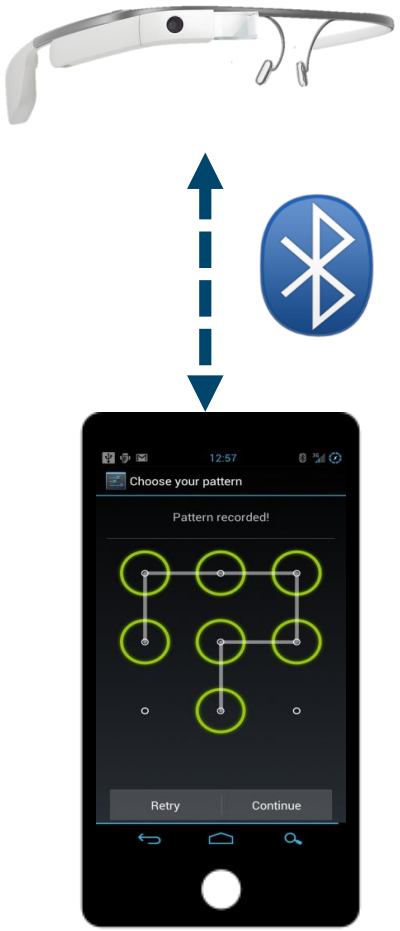
Vital Sign



Gaming Asset

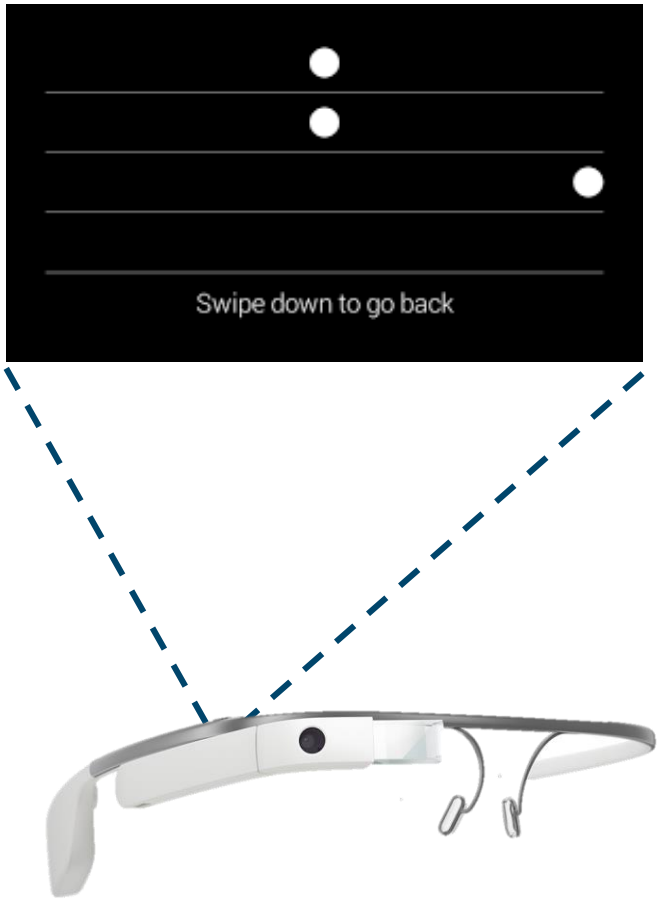
Existing Approaches: Indirect Authentication

- ✗ **Lack of independency**
- ✗ **Cumbersome**



Existing Approaches: Built-in Authentication

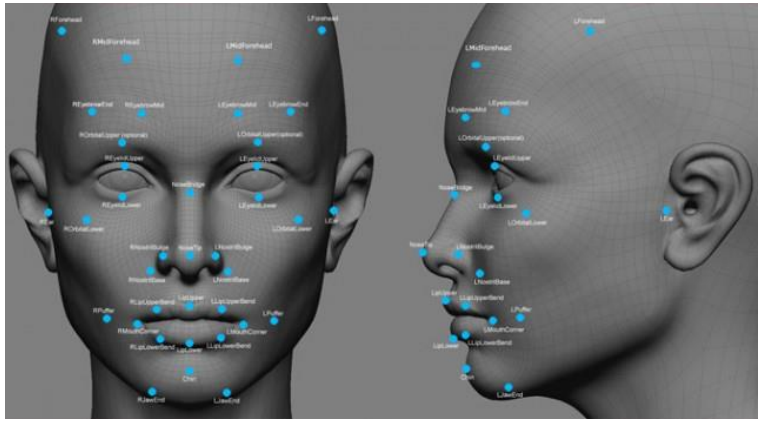
- ✗ **Limited Input Area**
- ✗ **Long Input Period**
- ✗ **Not Intuitive Pattern**



Existing Approaches: Biometrics

Physical Biometrics :

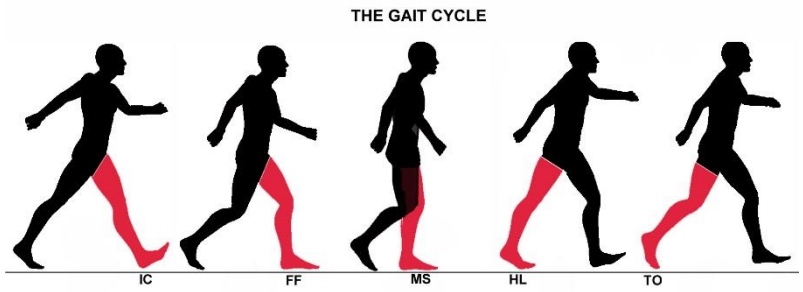
- **Additional Hardware**
- **Not always applicable for head-mounted device**



Existing Approaches: Biometrics

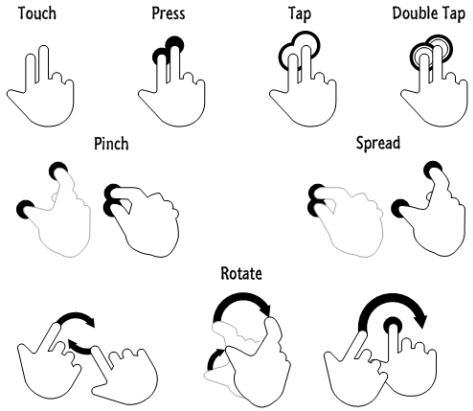
Behavioral Biometrics:

Walking gait, arm swing, finger gesture, etc.

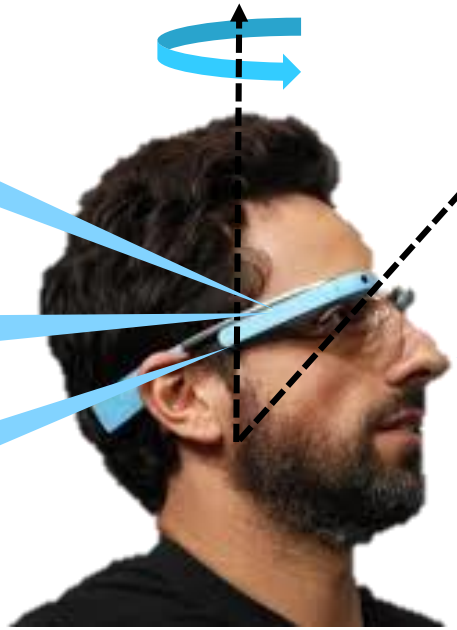


But, for head movements:

- **Hard to collect long-term movement patterns**
- **Do not have high Degree of Freedom**



Challenges



Limited Input Area

Invisible Input Pattern

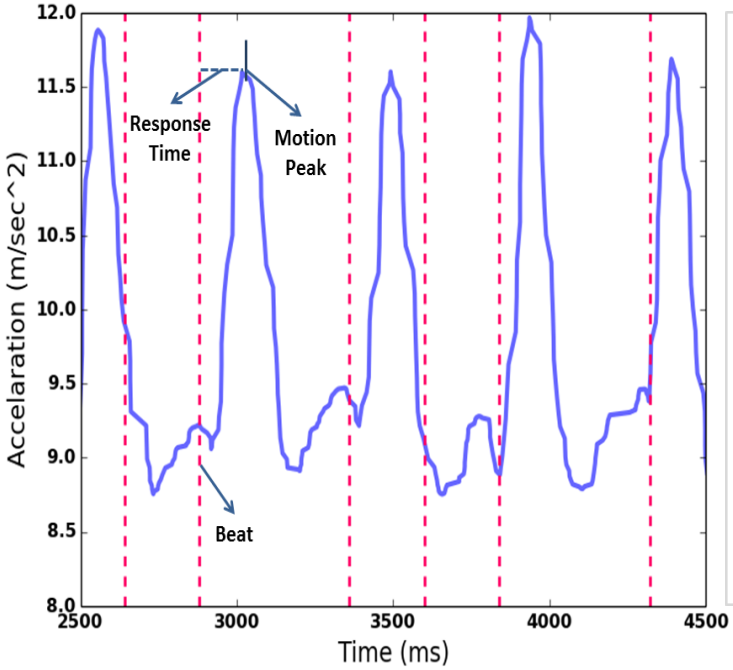
Constrained Recourses

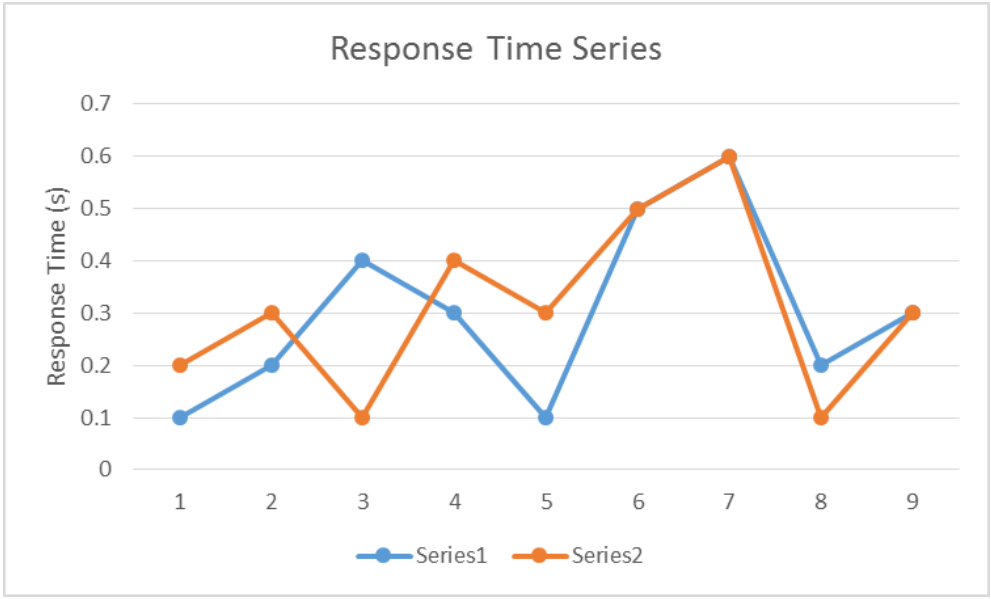
Low Degree of Freedom

Lack of long-term Habit

Music-induced Head Movement

Music-induced Head Movement



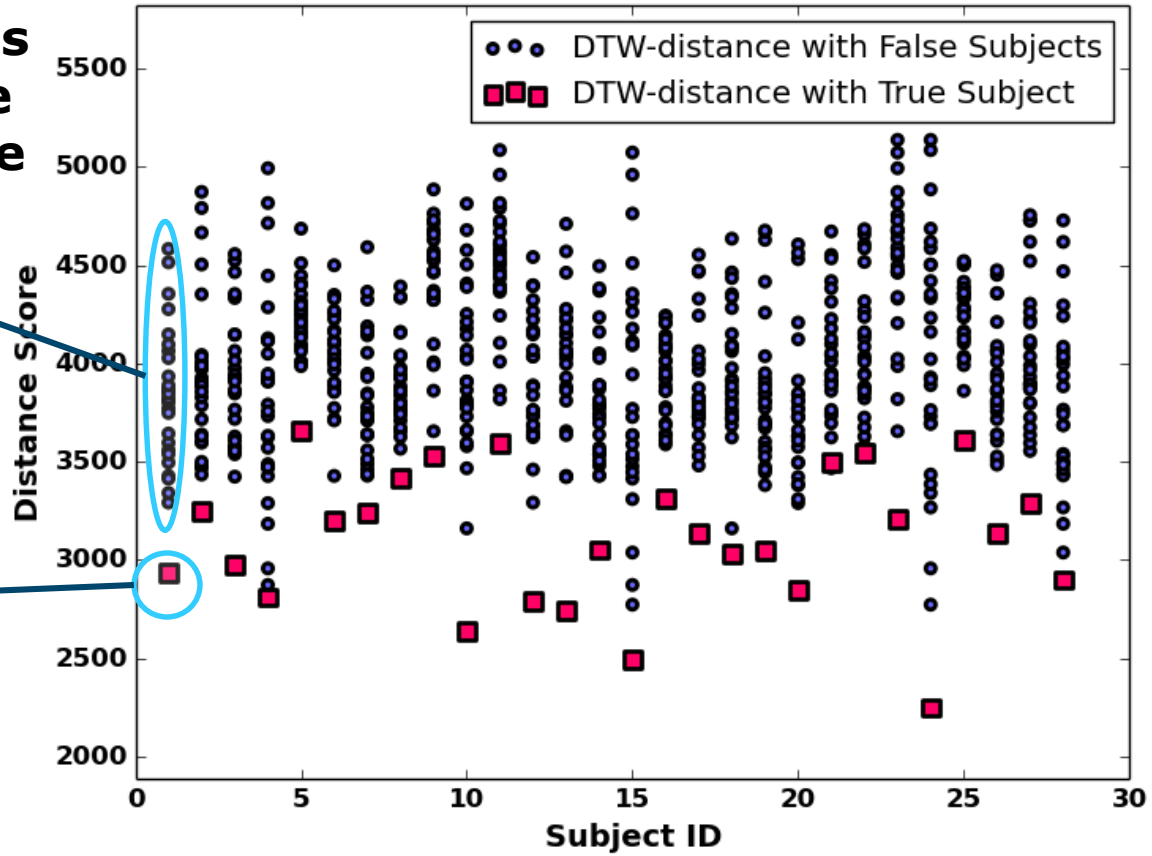


- 30 Subjects
- Same movement and same music 30 times

Response Time Is Not Enough

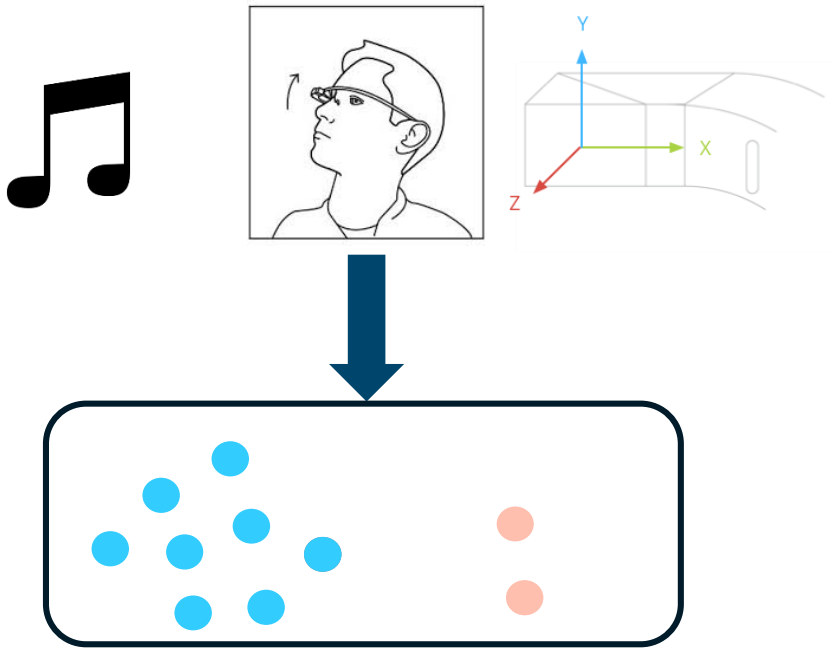
Average Distances between the false users and the true user

Average distance between the true user and itself

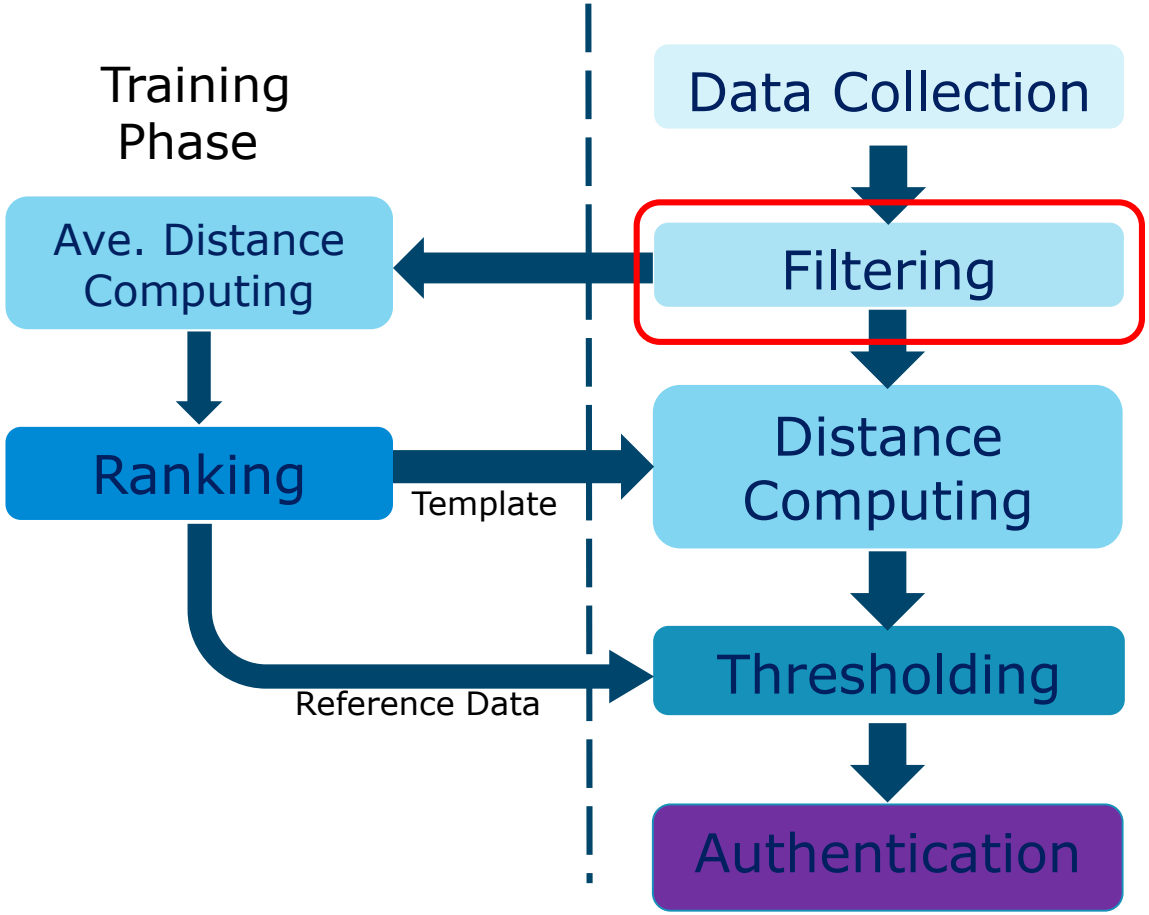


Headbanger Rationales

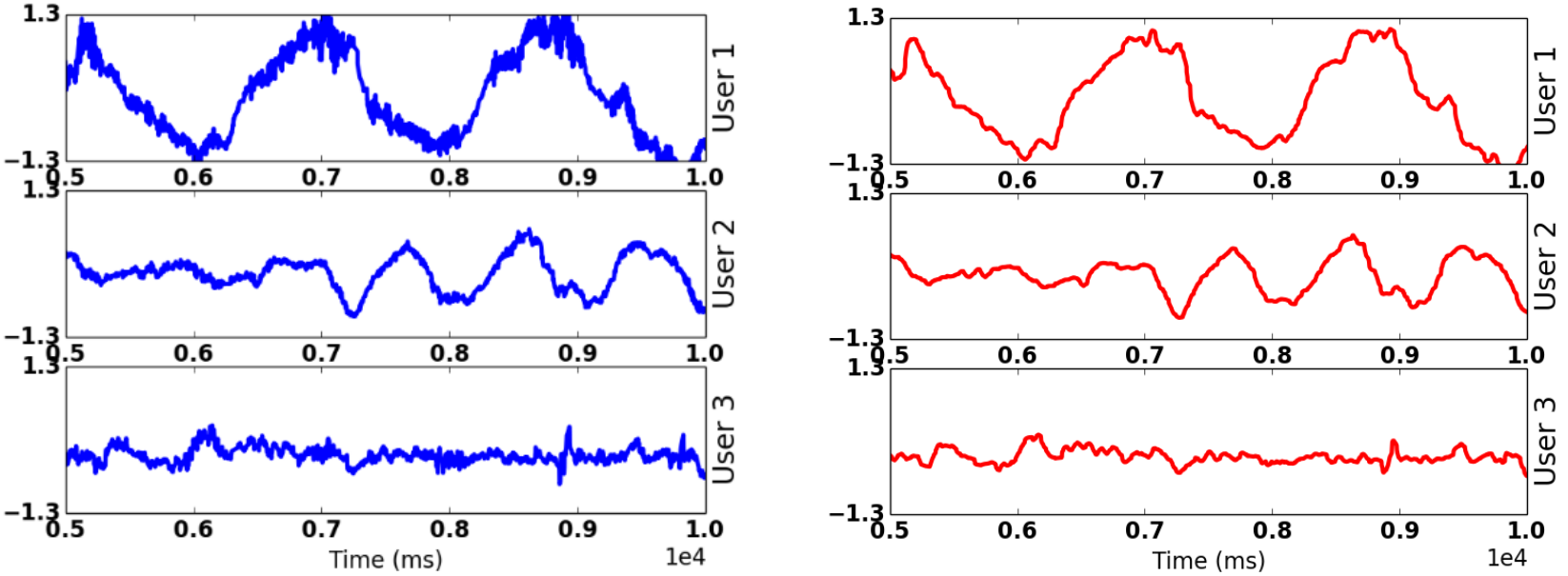
Dist. Of the Same User
<<
Dist. Of Two Users



Headbanger Overview

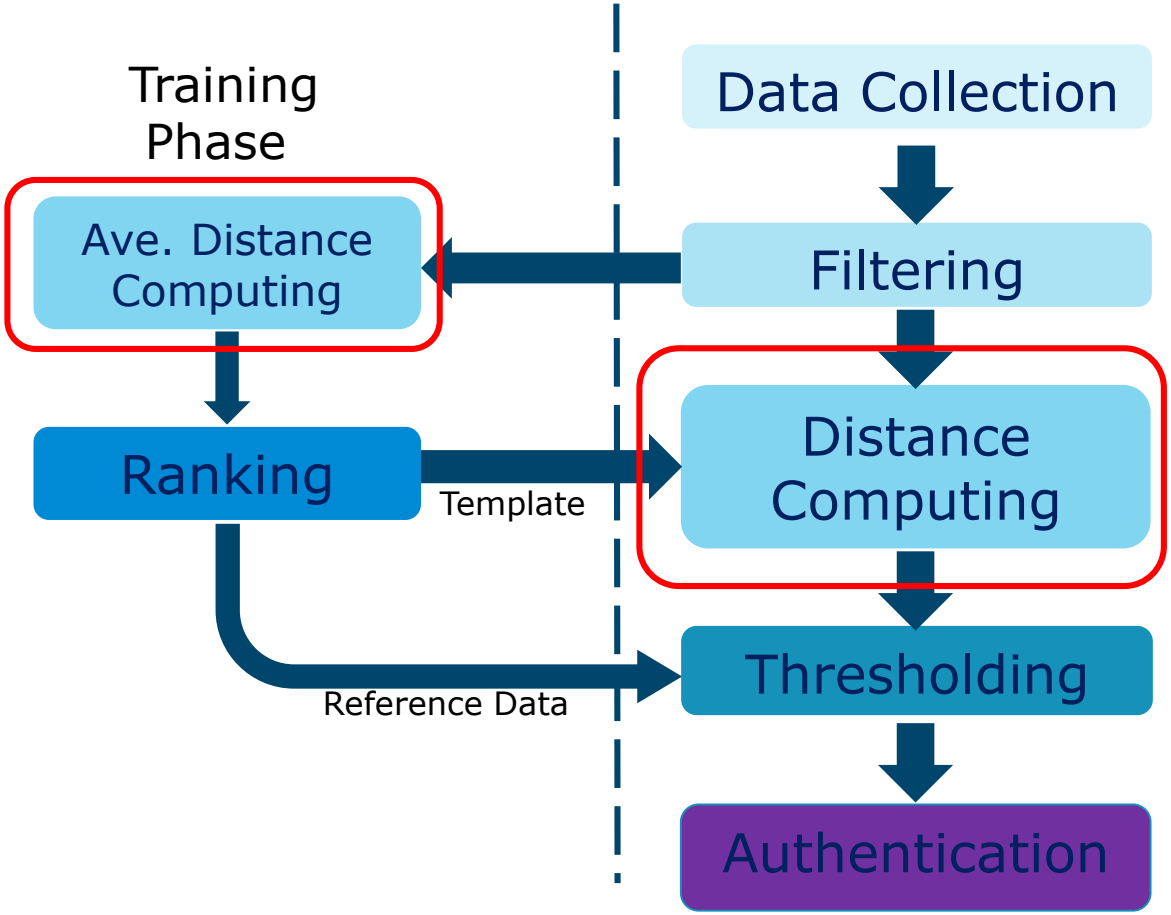


Data Filtering



- Accelerometer Contains High Frequency Noise
- Head Movement is at Low Frequency (< 5 Hz)

Headbanger Overview



Dynamic Time Warping

Time-normalized distance between A and B :

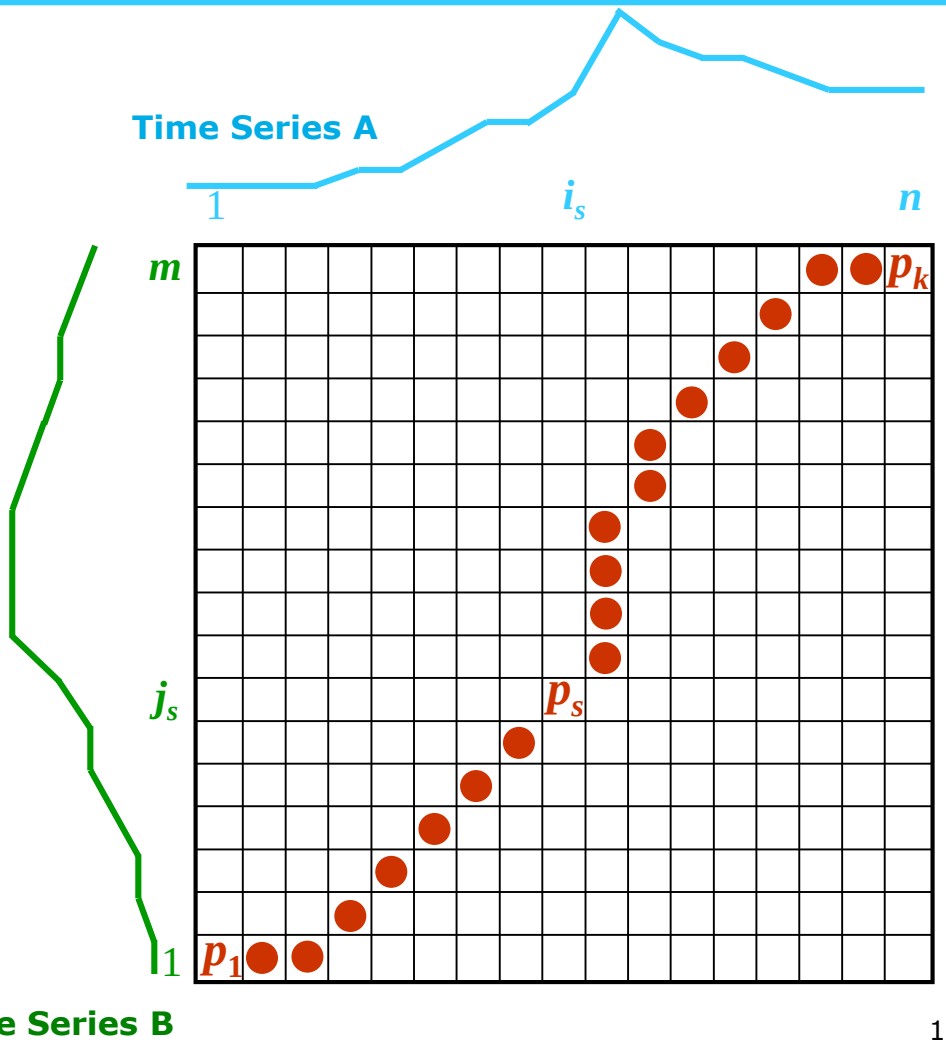
$$D(\mathbf{A}, \mathbf{B}) = \left[\frac{\sum_{s=1}^{k} d(p_s) \cdot w_s}{\sum_{s=1}^{k} w_s} \right]$$

$d(p_s)$: distance between i_s and j_s

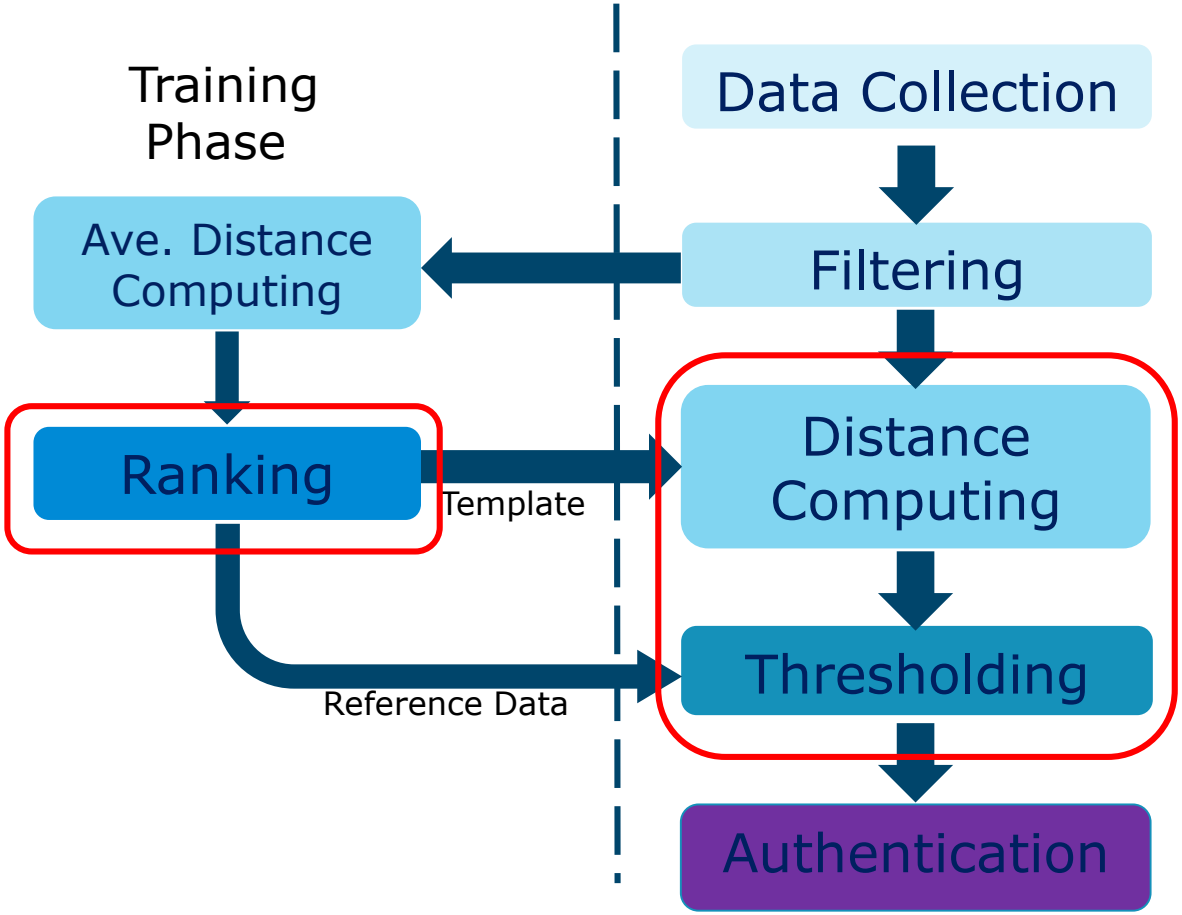
$w_s > 0$: weighting coefficient.

Best alignment path between **A** and **B** :

$P_1 = \arg\min_P (D(\mathbf{A}, \mathbf{B}))$.



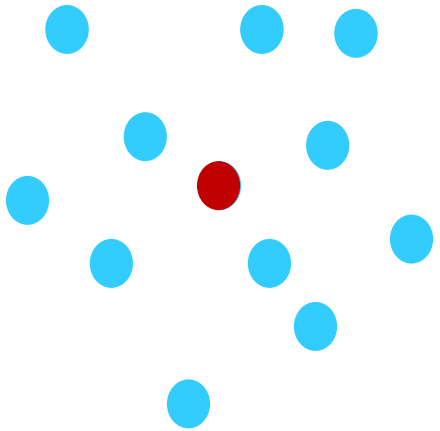
Headbanger Overview



Reduce the Computing Overhead

- **Choose Representative Samples**
  - Compute the average distance to other samples
  - Rank the samples based on their average distance
  - Threshold can be expressed as:

$$Threshold = \overline{d_k} + \mathrm{n} \times \sigma_k$$



Repeatability & Similarity Experiment

Objectives:

- True user can login with high probability
- Different user do different movement
- Low computing cost

Setup:

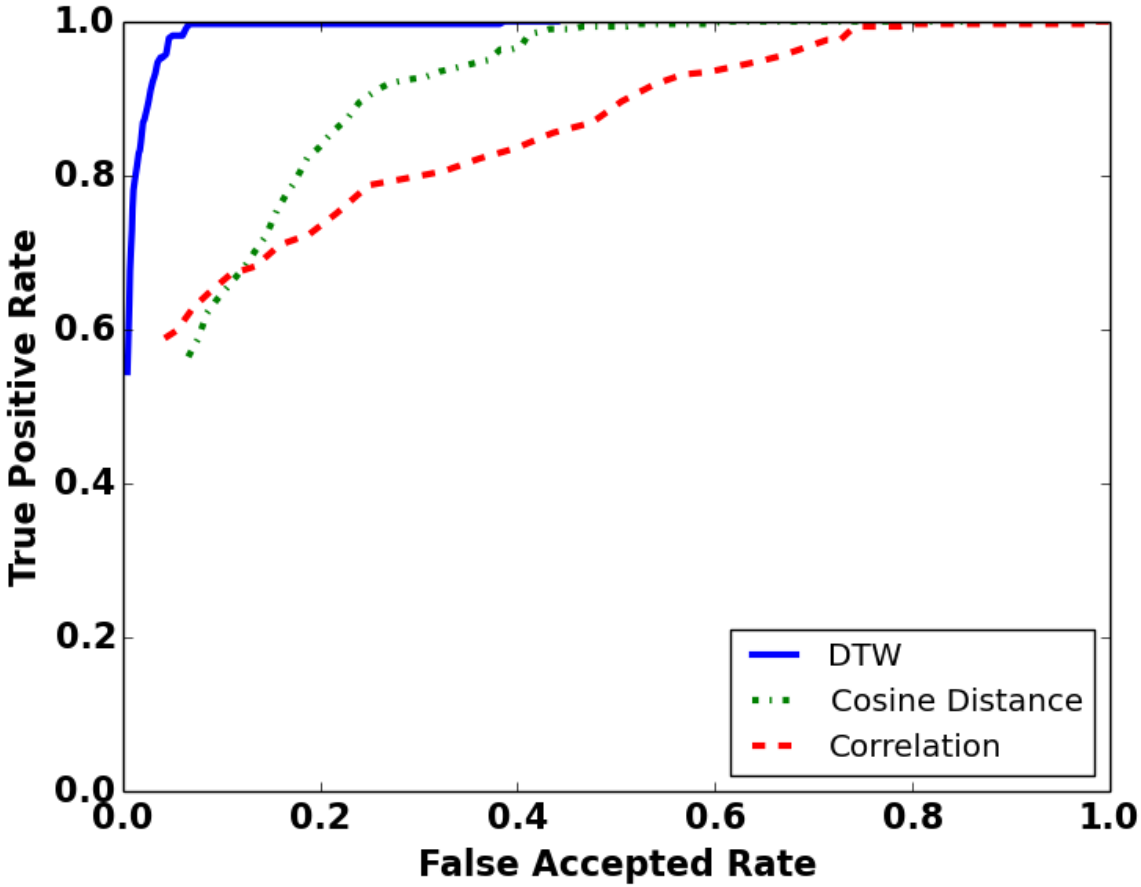
- 30 subjects are involved
- Each of them design its own pattern
- Each of them performs it 40 times

Evaluation Metrics

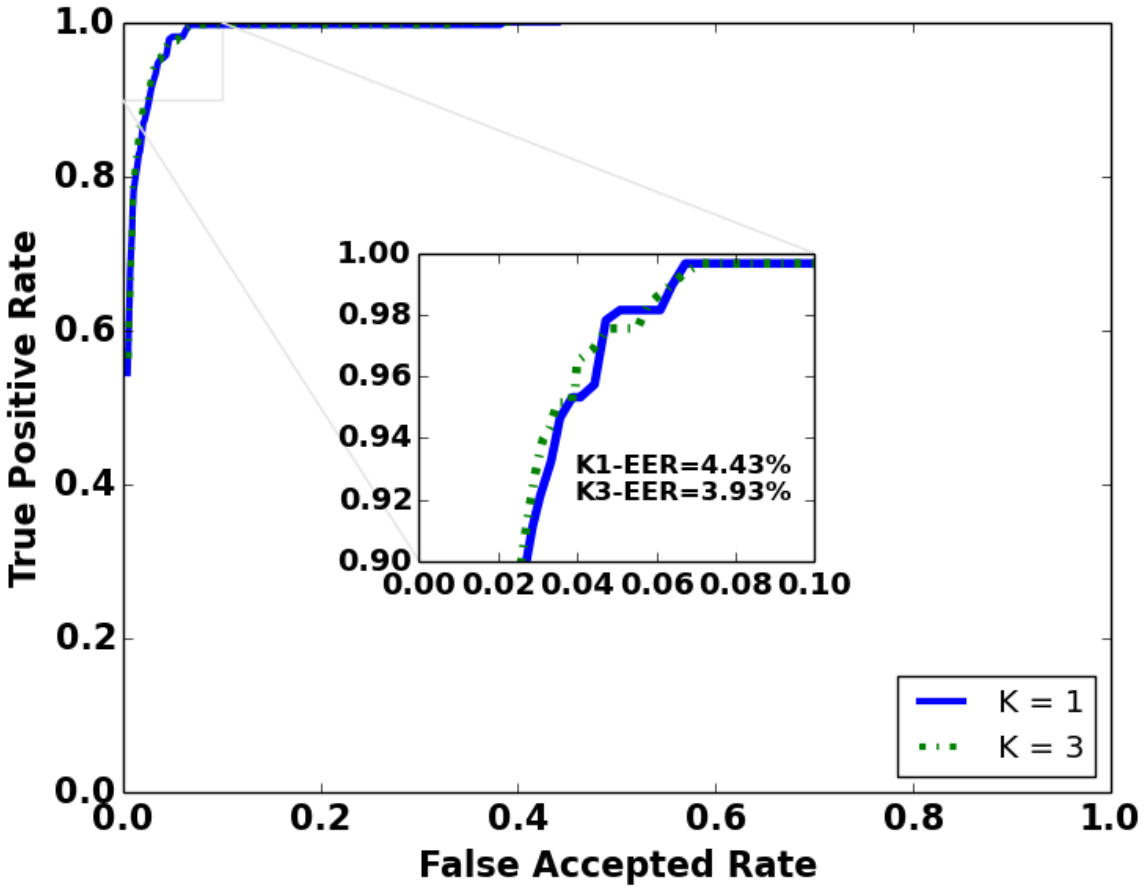
- True Positive Rate
- False Accepted Rate
- Equal Error Rate

EER = TRR(n) = FAR(n)

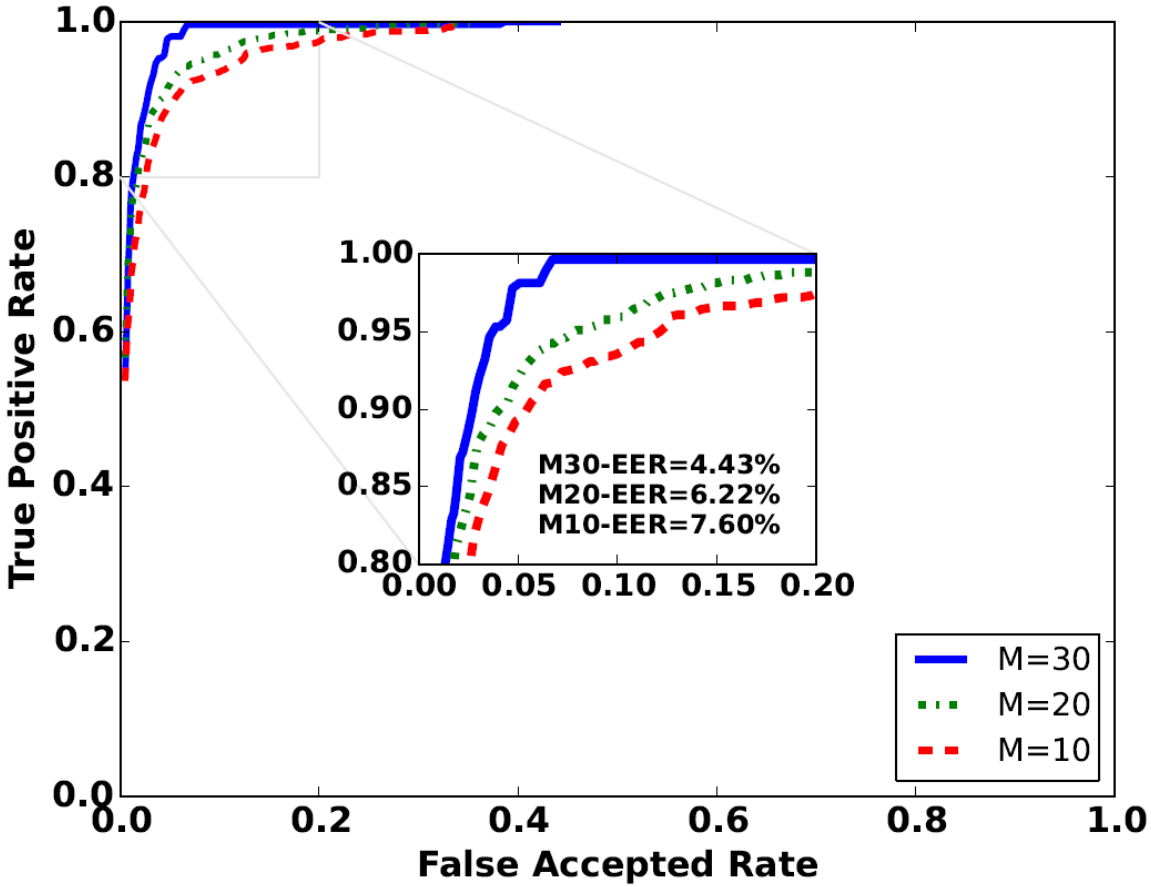
Impact of Distance Algorithm



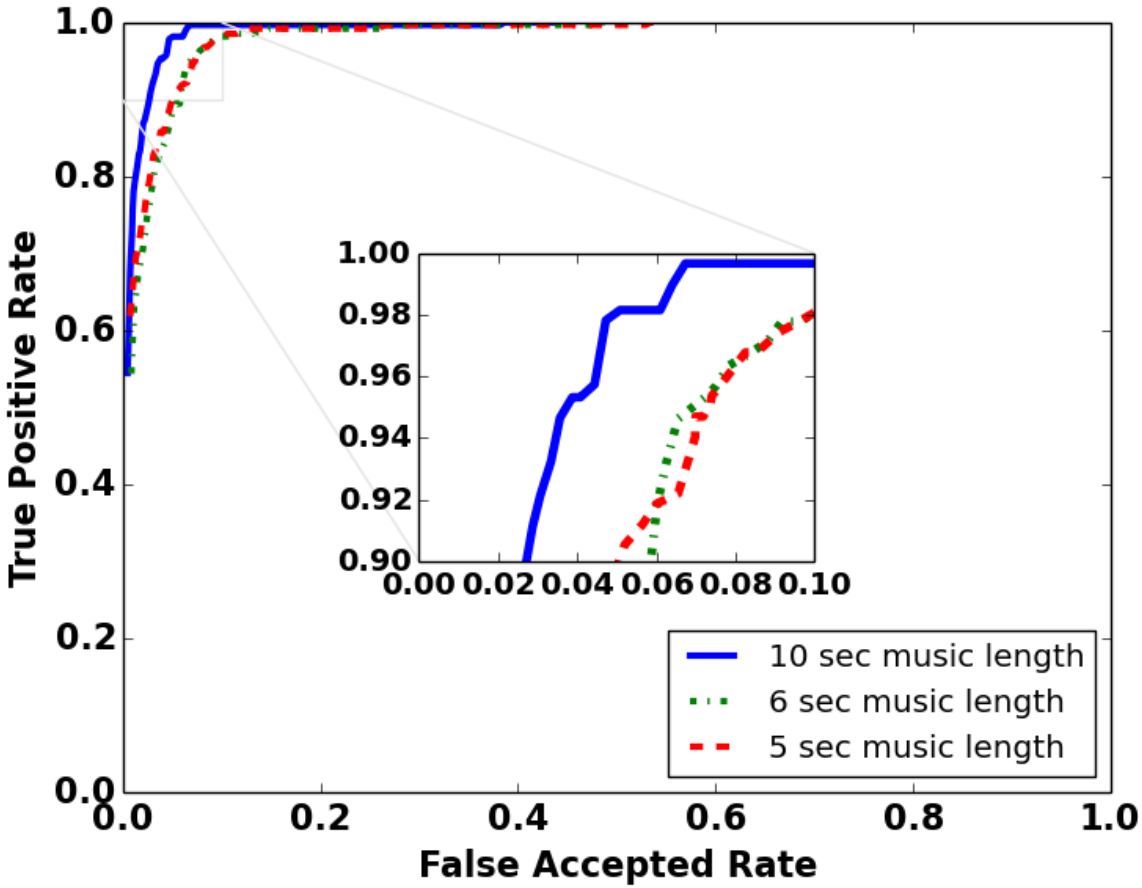
Impact of Voting Scheme



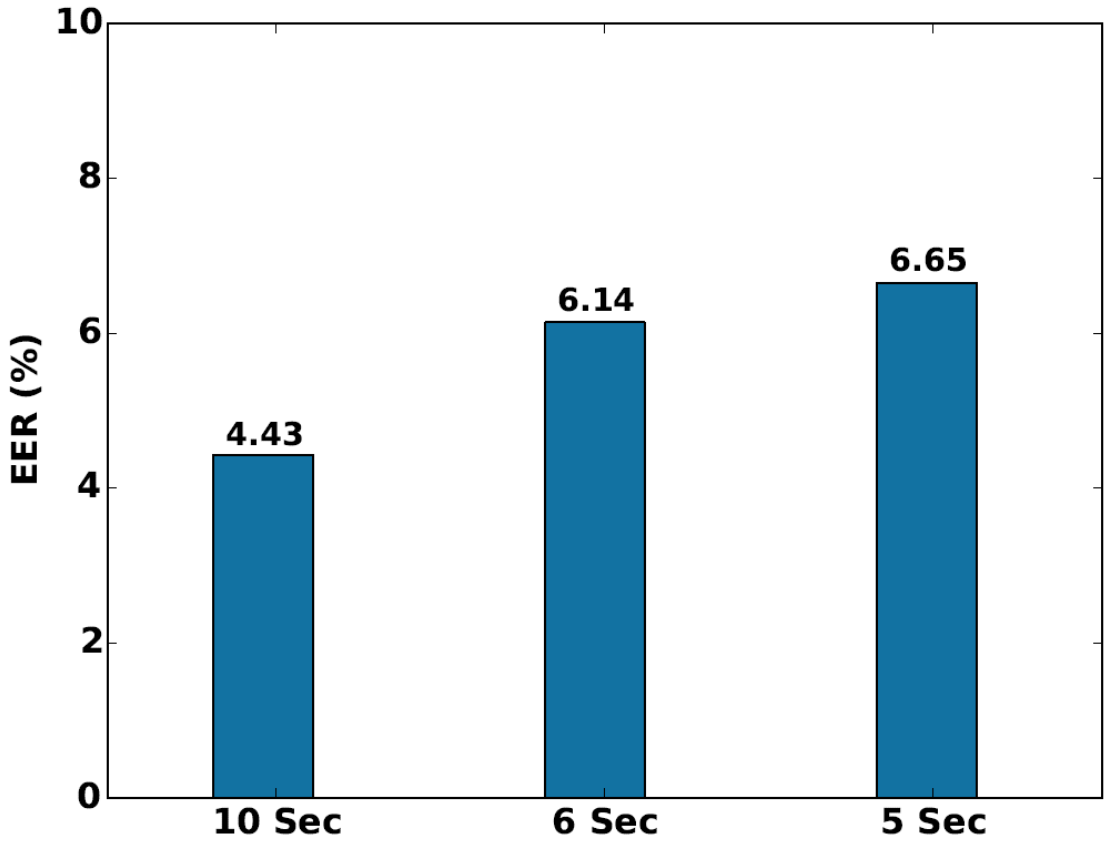
Impact of Training Size



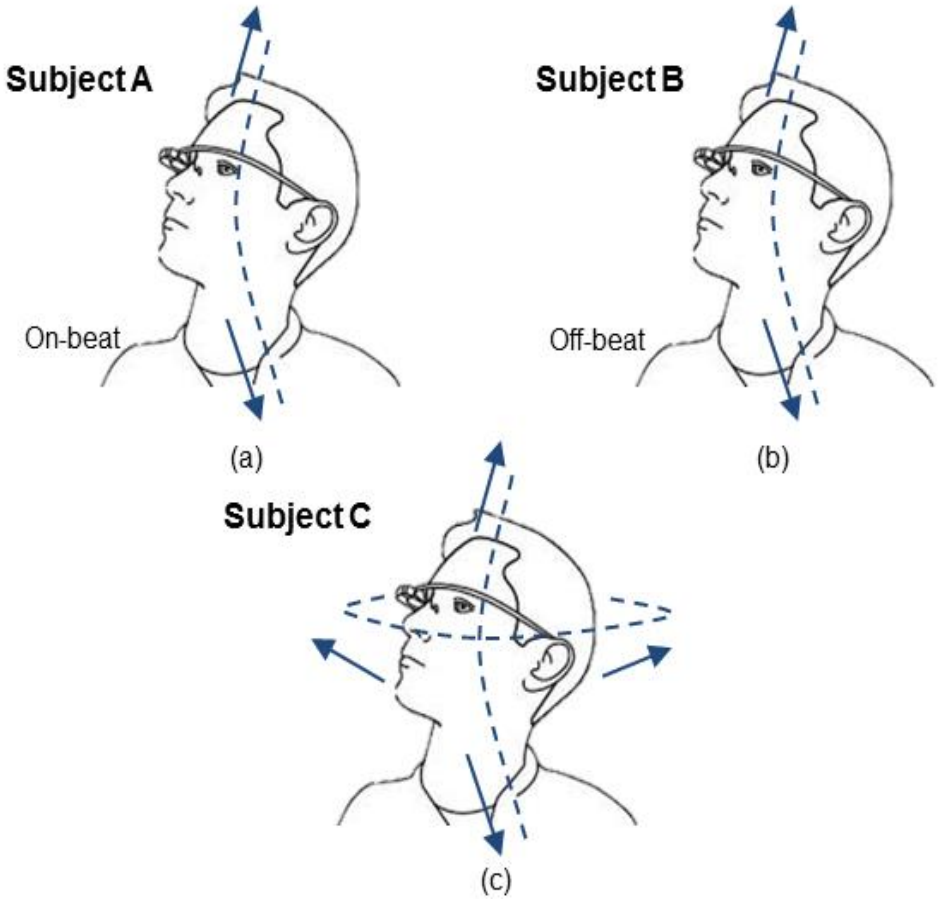
Impact of Music Duration



Overall



Let's Attack it!

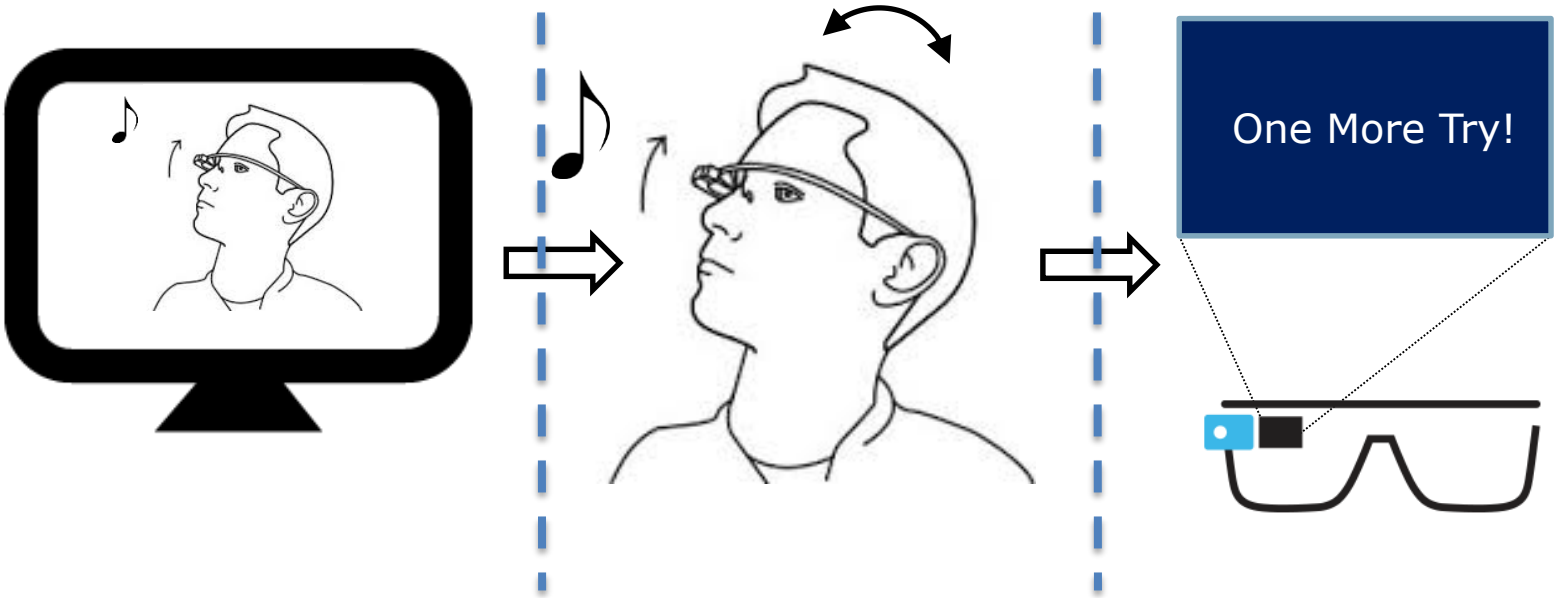


Let's Attack It!

1. Watch the user's movement video

2. Mimic the user's movement

3. Headbanger displays the authentication result



Attack Results

Target	# of Attackers	# of Successful Attackers	Average # of Trials before 1st Successful Attack	FAR (%)
A	12	7	10	15.83
B	13	3	14	2.77
C	12	3	17	2.72
Overall	38	13	13	6.94

Prototyping

- Google Glass Development Kit
- Java Speech Tool Kit
- Fast DTW: $O(n^2) \rightarrow O(n)$
- Task pipelining

Music Cue Duration (s)	Data processing latency (s)
10	1.93
6	1.15
5	0.88

Conclusion

- We design Headbanger
- We Conduct Intensive Experiment
  - Repeatability, Robustness
- We develop a running App on Google Glass

Thank you! Questions?