# Privacy-preserving Continuous Authentication

**Team**

Stephanie Lew and Jiyi Zhang

# Problem Statement

- Smarthome devices use data collected from sensors extensively for tasks such as identification and authentication

- Nonetheless, users are concerned that their private information is exposed in this process

- We want to show that even with masked data, we can still carry out identification task

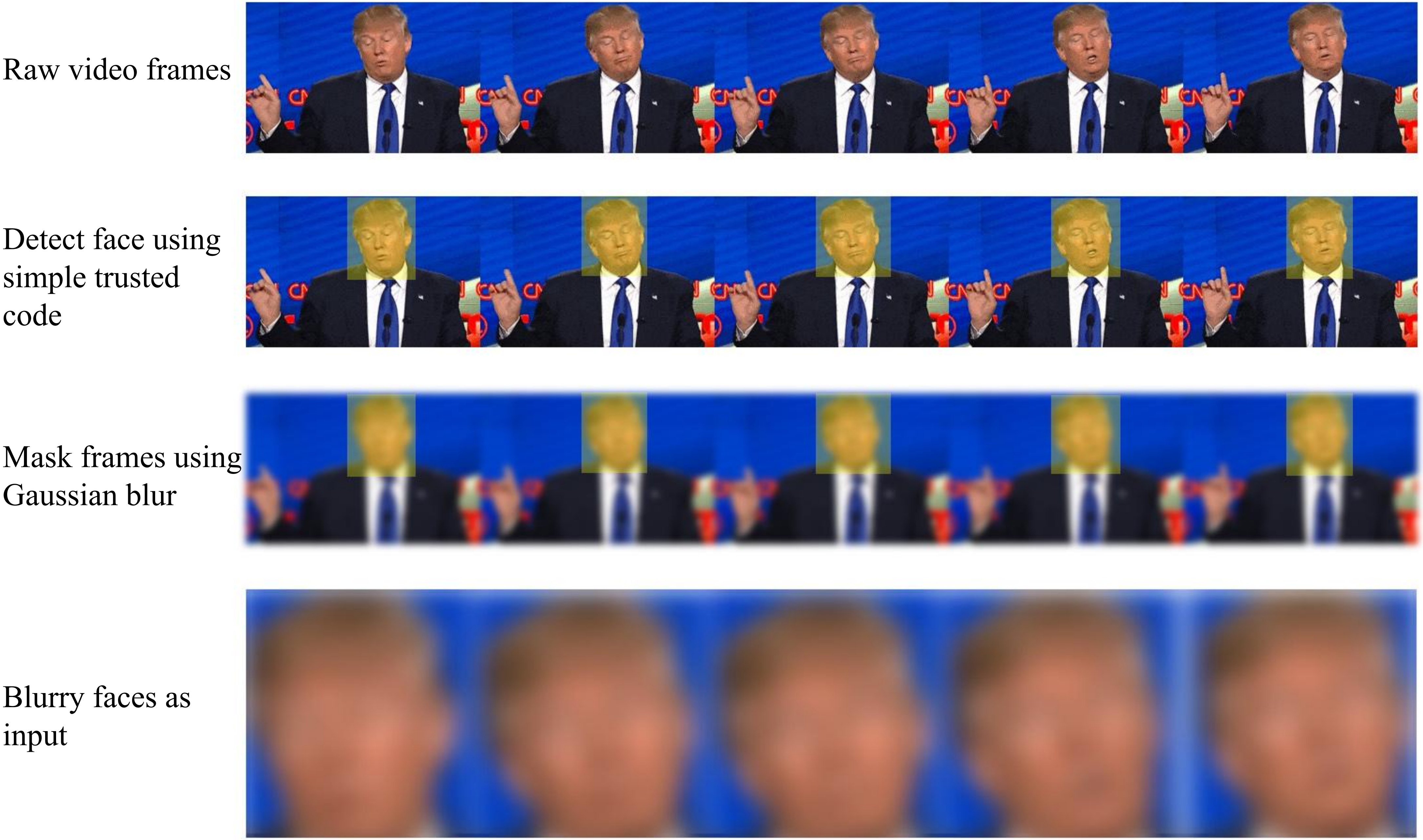
- With the help of continuous data and data from multiple sensors, we can exploit some kinds of information that was not utilized previously (spatio-temporal) to compensate the ‘information loss’ in privacy preserving process and achieve similar or even better performance in above tasks

# Progress Update

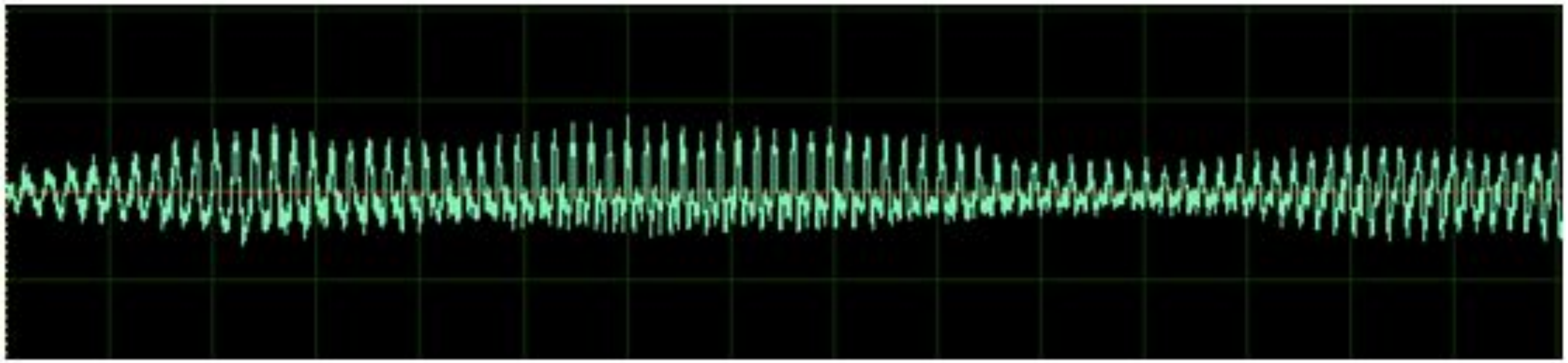
- Refinement of literature survey on PP works in smarthome settings

  - Face identification
  - Speaker recognition

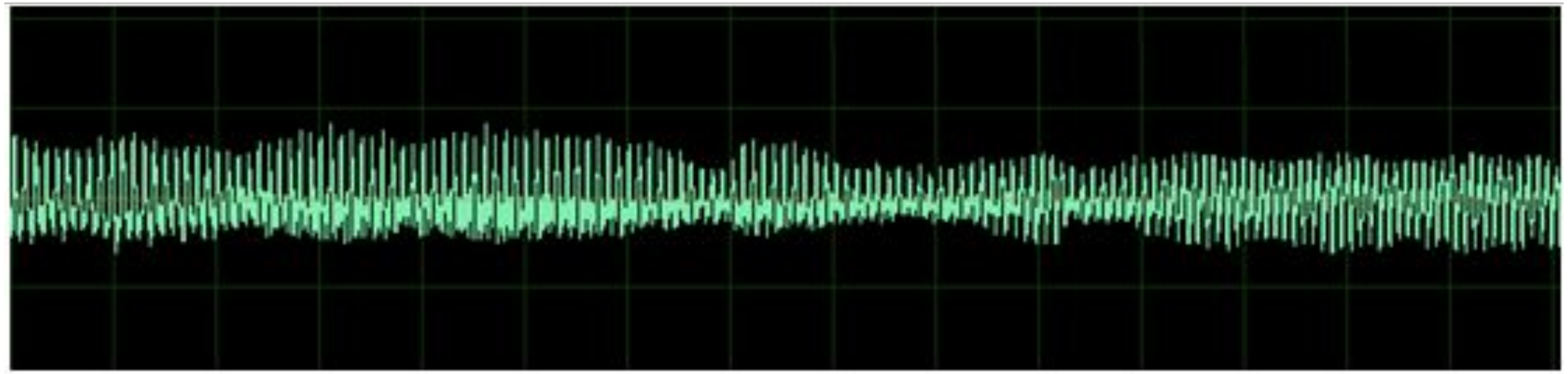
- Definition of experimental setup for both modalities
- We have successfully built a simple testbed for preliminary proof of concept
- We have successfully tested automatic video crawling from YouTube using celebrities' name as query


Raw video frames
Detect face using simple trusted code
Mask frames using Gaussian blur
Blurry faces as input

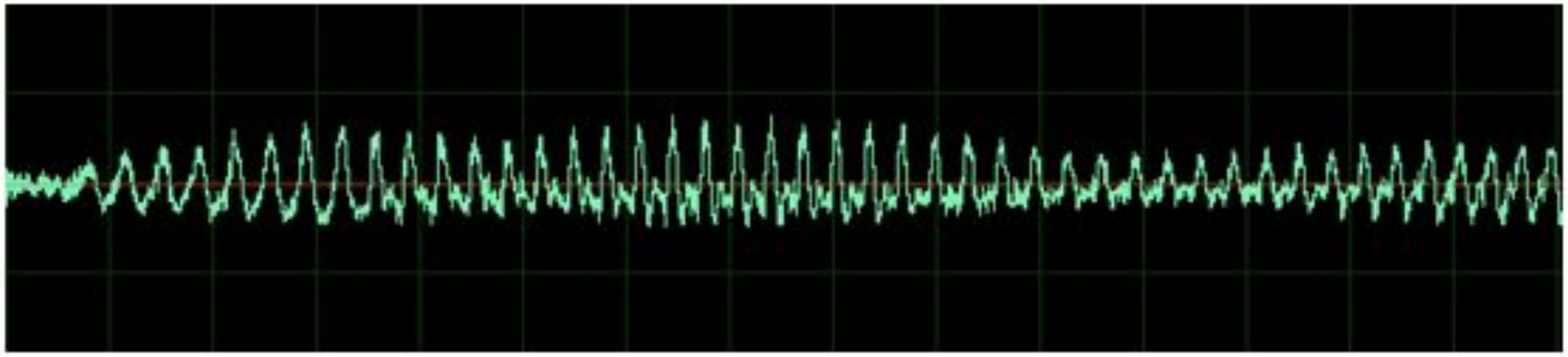
Raw audio

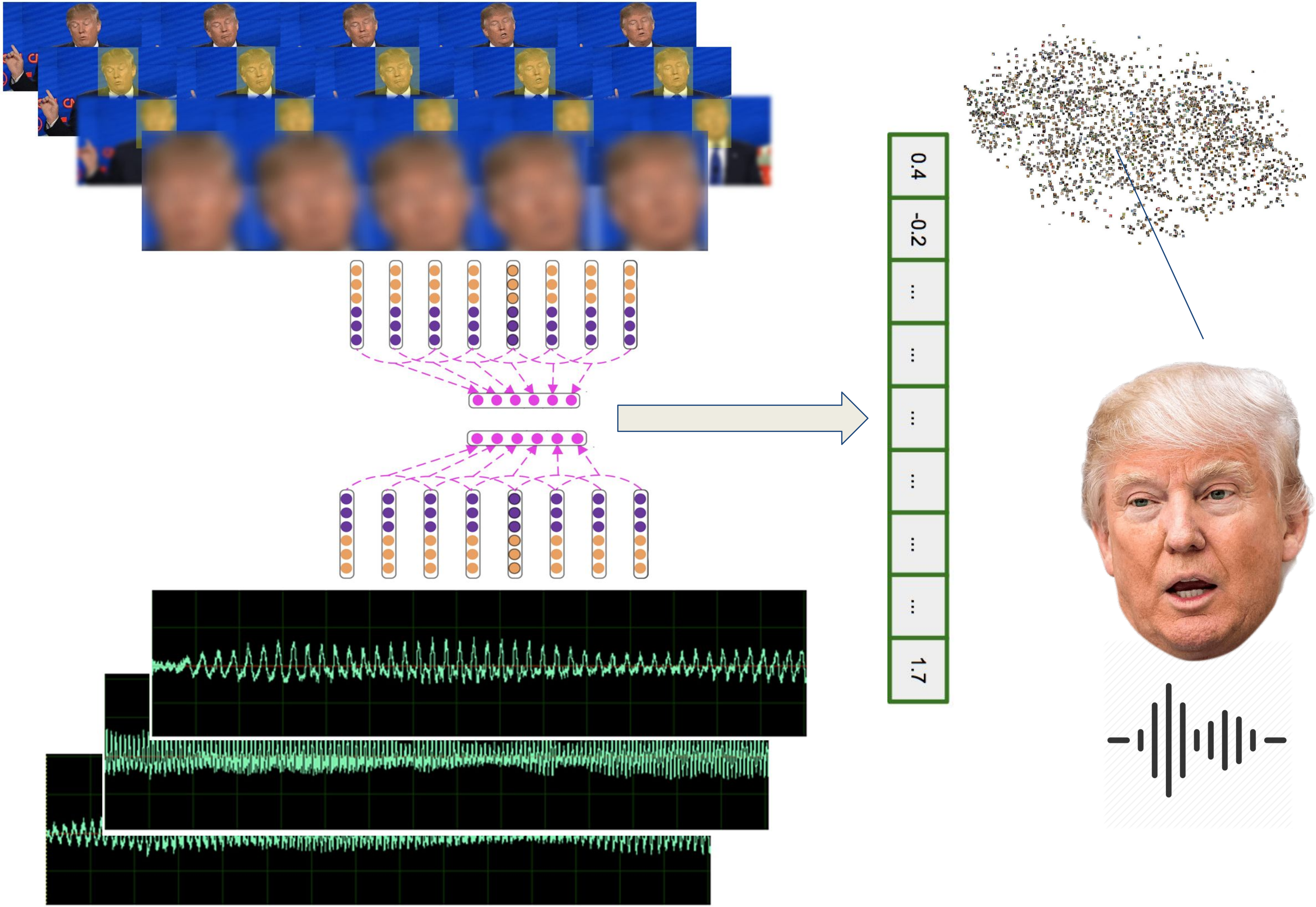


Pitch + 10



Pitch - 10




0.4
-0.2
...
...
...
...
...
...
1.7

# Roadblocks and Challenges

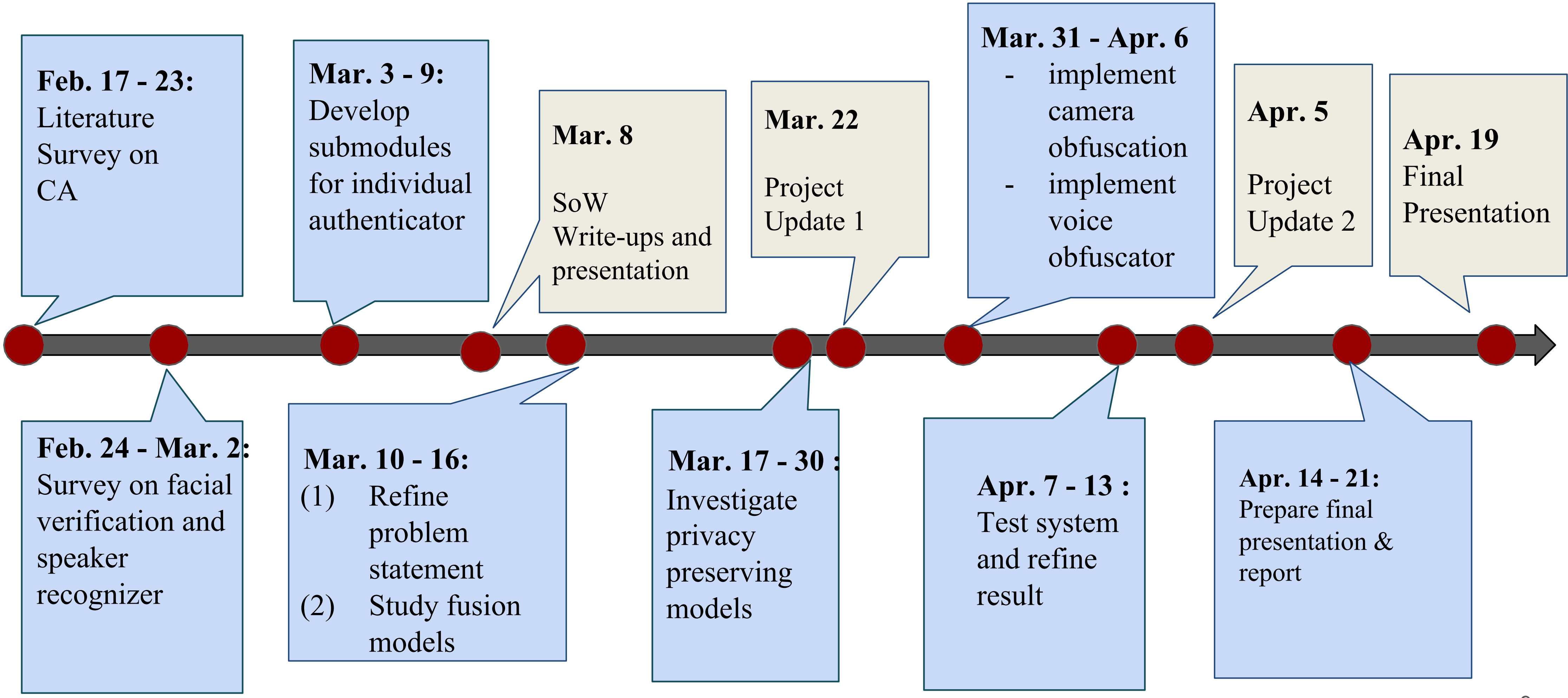
** Privacy Preserving (PP)*

- *PP Facial Identification for smarthomes
    - Identifying people from blurry image is a hard problem
- *PP Speaker verification for smarthomes
    - Few notable *PP voice verification works
    - Requires enrollment phase before verification
        - Need to define what levels of information is adequate for verification without compromising accuracy.
- While there are some promising works in the joint face and voice modality space, there remains little information about how both PP modalities can be fused together for better authentication, while preserving privacy.

# Changes to the Initial Proposal

- We strengthened our motivation for the project frome multimodal continuous authentication using biometric features by considering the privacy space
- Imbuing privacy into the occupant identification process is a new constraint that we added
- This motivates us to consider the ***tradeoff*** between *securing* a smarthome device and maintain the *privacy* of the occupant

# Project Timeline



**Feb. 17 - 23:**
Literature Survey on CA

**Feb. 24 - Mar. 2:**
Survey on facial verification and speaker recognizer

**Mar. 3 - 9:**
Develop submodules for individual authenticator

**Mar. 8**

SoW Write-ups and presentation

**Mar. 10 - 16:**
(1) Refine problem statement
(2) Study fusion models

**Mar. 17 - 30 :**
Investigate privacy preserving models

**Mar. 22**

Project Update 1

**Mar. 31 - Apr. 6**
- implement camera obfuscation
- implement voice obfuscator

**Apr. 5**

Project Update 2

**Apr. 7 - 13 :**
Test system and refine result

**Apr. 14 - 21:**
Prepare final presentation & report

**Apr. 19**
Final Presentation

# Next Steps

- Stage 1: Conduct control experiments for automatic facial de-identification and re-identification
- Stage 2: Leverage on biometric temporal information to improve the occupant identification performance
  - Conduct experiment on non-obfuscated and obfuscated speaker datasets and compare the results
- Stage 3: Draw conclusions on privacy preserving effects and define privacy framework for passive automatic occupant identification.
- Stage 4: Attempt to fuse stage 1 and stage 2 models, and perform continuous authentication using features from stage 2.

# Bibliography

## Team Daemons: Stephanie Lew and Jiyi Zhang

[1] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens.” Woot, vol. 10, pp. 1–7, 2010.

[2] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, “Measuring user confidence in smartphone se- curity and privacy,” in Proceedings of the eighth symposium on usable privacy and security. ACM, 2012, p. 1.

[3] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, “Touch me once and i know it’s you!: implicit authentication based on touch screen patterns,” in proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2012, pp. 987–996.

[4] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, “Touchalytics: On the applica- bility of touchscreen input as a behavioral biometric for continuous authentication,” IEEE transactions on information forensics and security, vol. 8, no. 1, pp. 136–148, 2013.

[5] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, “Continuous user authentication on mobile devices: Recent progress and remaining challenges,” IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49–61, 2016.

[6] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, “Surveying the development of biometric user authentication on mobile phones,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268–1293, 2015.

[7] I. C. Stylios, O. Thanou, I. Androulidakis, and E. Zaitseva, “A review of continuous au- thentication using behavioral biometrics,” in Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference. ACM, 2016, pp. 72–79.

[8] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, “Design and implementation of a contextual-based continuous authentication framework for smart homes,” Applied System Innovation, vol. 2, no. 1, p. 4, 2019.

[9] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, “Continuous and trans- parent multimodal authentication: reviewing the state of the art,” Cluster Computing, vol. 19, no. 1, pp. 455–474, 2016.

[10] V. Radha and D. H. Reddy, “A survey on single sign-on techniques,” Procedia Technology, vol. 4, pp. 134–139, 2012.

[11] F. Aloul, S. Zahidi, and W. El-Hajj, “Two factor authentication using mobile phones,” in 2009 IEEE/ACS International Conference on Computer Systems and Applications. IEEE, 2009, pp. 641–644.

# Bibliography

## Team Daemons: Stephanie Lew and Jiyi Zhang

[12] I. Nakanishi, “Unconscious biometrics for continuous user verification,” in Proceedings of the 8th International Conference on Signal Processing Systems, ser. ICSPS 2016. New York, NY, USA: ACM, 2016, pp. 20–25. [Online]. Available: http: //doi.acm.org/10.1145/3015166.3015180

[13] K. Sitara and B. Mehtre, “Digital video tampering detection,” Digit. Investig., vol. 18, no. C, pp. 8–22, Sep. 2016. [Online]. Available: https://doi.org/10.1016/j.diin.2016.06.003

6

[14] M. Carrillo, Cassandra, “Continuous biometric authentication for authorized aircraft personnel : a proposed design,” 2003. [Online]. Available: https://calhoun.nps.edu/ handle/10945/1011

[15] R. Janakiraman, S. Kumar, S. Zhang, and T. Sim, “Using continuous face verification to improve desktop security,” in Proceedings of the Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION’05) - Volume 1 - Volume 01, ser. WACV-MOTION ’05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 501–507. [Online]. Available: http://dx.doi.org/10.1109/ACVMOT.2005.120

[16] G. Chetty and M. Wagner, “Multi-level liveness verification for face-voice biometric au- thentication,” in Proceedings of 2006 Biometrics Symposium, L. Williams, Ed. United States: IEEE, Institute of Electrical and Electronics Engineers, 2006, pp. 1–6.

[17] D.-J. Kim, K.-W. Chung, and K.-S. Hong, “Person authentication using face, teeth and voice modalities for mobile device security,” IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2678–2685, 2010.

[18] H. Saevanee, N. L. Clarke, and S. M. Furnell, “Multi-modal behavioural biometric au- thentication for mobile devices,” in IFIP International Information Security Conference. Springer, 2012, pp. 465–474.

[19] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, “Implicit authentication through learning user behavior,” in International Conference on Information Security. Springer, 2010, pp. 99–113.

[20] X. Wang, T. Yu, O. Mengshoel, and P. Tague, “Towards continuous and passive authentica- tion across mobile devices: an empirical study,” in Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2017, pp. 35–45.