User-Friendly Authentication on Smart Glasses

Piero Romare

Master's Thesis Proposal

1 Abstract

This proposal focuses on enhancing the security of spatial computing hardware, particularly through biometric authentication and de-authentication systems integrated into smart glasses. By placing non-invasive sensors near the ears, physiological and behavioral data can be collected to capture unique biometric patterns. These data are processed to extract features used by an artificial intelligence model, which determines whether to grant or deny user access to the connected system. The proposed approach will be validated through laboratory experiments and real-world testing, evaluating performance across diverse user conditions.

2 Background

The evolution of personal computing began with the introduction of the microprocessor and the personal computer in the 1970s. Two decades later, in the 1990s, the era of portable computers emerged, bringing the flexibility of mobility. Building on the advantages of portability, the focus shifted towards compactness, resulting in the launch of smartphones in the late 2000s. The latest advancement in personal computing has been wearables, small devices designed to minimize the need for direct commitment with systems and maximize the implicit interaction. Over the past 50 years, technology's impact on human life has not only persisted but has accelerated, driving innovations towards increasingly smooth and non-invasive interactions. The ultimate aim is to integrate technology into daily life without disturbing activities or requiring constant attention to screens. This shift redefines personal computing as "personal space computing", where augmented reality holds immense potential to enhance everyday experiences.

3 Security Aspects

In the context of smart glasses, a large number of sensors are embedded to provide their functionality or additional features. Each sensor can collect data

elicited from the user. The way on how these data are communicated to external system, such as servers that provide services, require security. Under the security terminology, we can find data encryption, securing the data storage again unauthorized access, software vulnerabilities and authentication system.

This project focuses on the field of authentication, which is closely related to identification. While identification seeks to answer the question, *"Who are you?"*, authentication builds on prior knowledge of the user to pose a slightly different challenge: *"Hello, User X. Welcome back! Please prove that you are indeed User X."*

One method of authenticating individuals is through biometrics. Biometrics use unique biological traits (e.g., fingerprints, iris scans, ear canal movements (Carlucci et al., 2020)) or behavioral patterns (e.g., keyboard dynamics, mouse movements). Combining two types of authentication creates two-factor authentication (2FA), while integrating multiple types results in multi-factor authentication (MFA), which are among the most robust methods available today.

Another important topic is de-authentication (Gangwal et al., 2024). De-authentication can mitigate risks such as lunchtime attacks, which occur when a user neglects or forgets to log out after completing an online session. In such cases, maintaining system resistance to unauthorized access becomes critical.

4 Related Work

Recent advancements in ear canal-based biometric systems have explored the use of acoustics and reverberation for authentication. EarEcho(Gao et al., 2019) exemplifies this approach by using the acoustic properties of the ear canal for continuous user authentication. Its prototype demonstrated high recall and precision rates under diverse conditions, highlighting its robustness. Building on similar principles, EarDynamic(Wang et al., 2021a, 2021b) employs acoustic sensing to monitor ear canal deformations during speech, enabled by sensors embedded in earphones. Similarly, EarPrint (Zou et al., 2024) integrates passive authentication through a combination of physiological and behavioral acoustics. Its real-time prototype achieves low false acceptance and equal error rates, demonstrating its effectiveness.

While previous studies have primarily focused on authentication methods using earphones, there is a notable gap in research specifically utilizing the ear as a source of biometric characteristics for user authentication in smart glasses. To the best of our knowledge, authentication methods for smart glasses have primarily relied on gestures, visual movements, or various general tasks, without considering the ear. These methods apply the potential of embedded sensors in wearable devices to capture user-related signals passively, making them more user-friendly. For instance, in (Boutros et al., 2020), a fusion approach using iris and periocular characteristics was introduced for user authentication, employing a Convolutional Neural Network (CNN). Similarly, iris recognition using an infrared sensor was demonstrated in (Y.-H. Li & Huang, 2017), where features

were extracted for authentication. Eye movements in response to visual stimuli, captured by a camera, were also shown to serve as a continuous authentication method for VR headsets in (Zhang et al., 2018). Additionally, SonicID employs ultrasonic acoustic waves to authenticate users by scanning their faces, where two speakers send encoded signals to eight microphones that feed a CNN for user authentication (K. Li et al., 2024). In (Isobe & Murao, 2023), a speaker embedded in the nose pad emits a signal that propagates through the nose and is captured by a microphone. This acoustic signal is represented as a 20,000-dimensional vector, which is compared against a dataset of reference vectors from other users, with authentication based on the Euclidean distance between the user's vector and the dataset. Furthermore, acoustic signals from teeth clicks have shown potential for use in authentication procedures (Mohapatra et al., 2024). Gaze patterns, measured via electrooculogram, have also been demonstrated as a viable authentication characteristic (Findling et al., 2020; Ragozin et al., 2022). Regarding gestures, GlassGuard (Peng et al., 2017) combines touch gestures and voice commands to provide continuous authentication using a Support Vector Machine (SVM). Likewise, in (Chauhan et al., 2016), four gesture commands were used as actions for continuous authentication. Another approach involves measuring skin deformation during blinking, using a photoreflector mounted on smart glasses to detect and authenticate based on blinks (Kawasaki & Sugiura, 2022).

5 Conclusion

In conclusion, this research explores the potential for integrating ear-related biometric systems into smart glasses, an area that has yet to be fully explored in existing literature. By utilizing the unique acoustic and physiological properties of the ear, it may be possible to enhance the authentication process, creating a user-friendly and secure user experience. A key challenge remains in optimizing the integration of multiple biometric modalities—such as acoustic, optical, and motion sensors—within smart glasses to achieve comprehensive, multi-layered authentication. Additionally, protecting sensitive activities and data from vulnerabilities like lunchtime attacks remains critical, and de-authentication strategies could play a key role in mitigating such risks. Ensuring that biometric systems maintain high accuracy under various real-world conditions—such as noise, user motion, and varying indoor/outdoor environments—while remaining unobtrusive and comfortable for the user, is crucial for their extensive adoption. Addressing these challenges will be crucial in developing robust and user-friendly authentication systems for smart glasses, creating the way for their secure and practical integration into daily life.

The scope of this project would answer one or more the following questions:

- How can existing ear-related biometric systems be integrated into smart glasses?
- What are optimal strategies for integrating multiple biometric modalities

(e.g., acoustic, optical, motion sensors) in smart glasses for comprehensive and robust authentication?

- Which methods have been explored to protect sensitive activities and data to prevent lunchtime attacks?
- How can biometric systems for smart glasses maintain high accuracy under various real-world conditions, such as noise, user motion, and in indoor/outdoor settings under comfortable and not intrusive settings?

6 Skills

- Hardware prototyping skills (Arduino or Raspberry PI)
- Conducting interviews and analyzing response data
- Programming skills

References

Boutros, F., Damer, N., Raja, K., Ramachandra, R., Kirchbuchner, F., & Kuijper, A. (2020). Fusing iris and periocular region for user verification in head mounted displays. *2020 IEEE 23rd International Conference on Information Fusion (FUSION)*, 1–8. https://doi.org/10.23919/FUSION45008.2020.9190282

Carlucci, M., Cecconello, S., Conti, M., & Romare, P. (2020). Eathentication: A chewing-based authentication method. *2020 IEEE Conference on Communications and Network Security (CNS)*, 1–9. https://doi.org/10.1109/CNS48642.2020.9162343

Chauhan, J., Asghar, H. J., Mahanti, A., & Kaafar, M. A. (2016). Gesture-based continuous authentication for wearable devices: The smart glasses use case. In M. Manulis, A.-R. Sadeghi, & S. Schneider (Eds.), *Applied cryptography and network security* (pp. 648–665). Springer International Publishing.

Findling, R. D., Quddus, T., & Sigg, S. (2020). Hide my gaze with eog! towards closed-eye gaze gesture passwords that resist observation-attacks with electrooculography in smart glasses. *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, 107–116. https://doi.org/10.1145/3365921.3365922

Gangwal, A., Paliwal, A., & Conti, M. (2024). De-authentication using ambient light sensor. *IEEE Access*, *12*, 28225–28234. https://doi.org/10.1109/ACCESS.2024.3367607

Gao, Y., Wang, W., Phoha, V. V., Sun, W., & Jin, Z. (2019). Earecho: Using ear canal echo for wearable authentication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, *3*(3). https://doi.org/10.1145/3351239

Isobe, K., & Murao, K. (2023). Personal identification method using active acoustic sensing applied to the nose pad of eyeglasses. *Adjunct Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing and the 2022 ACM International Symposium on Wearable Computers*, 345–348. https://doi.org/10.1145/3544793.3560400

Kawasaki, Y., & Sugiura, Y. (2022). Personal identification and authentication using blink with smart glasses. *2022 61st Annual Conference of the Society of Instrument and Control Engineers (SICE)*, 1251–1256. https://doi.org/10.23919/SICE56594.2022.9905842

Li, K., Agarwal, D., Zhang, R., Gunda, V., Mo, T., Mahmud, S., Chen, B., Guimbretiere, F., & Zhang, C. (2024, June). Sonicid: User identification on smart glasses with acoustic sensing. https://doi.org/10.48550/arXiv.2406.08273

Li, Y.-H., & Huang, P.-J. (2017). An accurate and efficient user authentication mechanism on smart glasses based on iris recognition. *Mobile Information Systems*, *2017*(1), 1281020. https://doi.org/https://doi.org/10.1155/2017/1281020

Mohapatra, P., Aroudi, A., Kumar, A., & Khaleghimeybodi, M. (2024). Non-verbal hands-free control for smart glasses using teeth clicks. https://arxiv.org/abs/2408.11346

Peng, G., Zhou, G., Nguyen, D. T., Qi, X., Yang, Q., & Wang, S. (2017). Continuous authentication with touch behavioral biometrics and voice on wearable glasses. *IEEE Transactions on Human-Machine Systems*, *47*(3), 404–416. https://doi.org/10.1109/THMS.2016.2623562

Ragozin, K., Marky, K., Lu, J., & Kunze, K. (2022). Eyemove - towards mobile authentication using eog glasses. *Proceedings of the Augmented Humans International Conference 2022*, 10–14. https://doi.org/10.1145/3519391.3519411

Wang, Z., Tan, S., Zhang, L., Ren, Y., Wang, Z., & Yang, J. (2021a). An ear canal deformation based continuous user authentication using earables. *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 819–821. https://doi.org/10.1145/3447993.3482858

Wang, Z., Tan, S., Zhang, L., Ren, Y., Wang, Z., & Yang, J. (2021b). Eardynamic: An ear canal deformation based continuous user authentication using in-ear wearables. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, *5*(1). https://doi.org/10.1145/3448098

Zhang, Y., Hu, W., Xu, W., Chou, C. T., & Hu, J. (2018). Continuous authentication using eye movement response of implicit visual stimuli. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, *1*(4). https://doi.org/10.1145/3161410

Zou, Y., Weng, J.-C., Lei, H., Wang, D., Leung, V., & Wu, K. (2024). Earprint: Earphone-based implicit user authentication with behavioral and physiological acoustics. *IEEE Internet of Things Journal*, *11*, 31128–31143. https://doi.org/10.1109/JIOT.2024.3417622