Use of PPG biometrics in identification and authentication

Author: Daniel Saura Lantape daniel.lantape@provadivita.edu.pl

I. Introduction

Biometrics, the measurement and analysis of biological data for identification purposes, has gained significant attention in recent years due to its potential applications in various fields, including security and healthcare. One particular biometric modality that has shown promise is photoplethysmography (PPG), which involves the measurement of blood volume changes in the body through the use of light sensors. PPG technology has been utilized in wearable devices such as smartwatches to monitor health metrics like heart rate and blood oxygen levels. However, its potential for identification and authentication purposes remains largely unexplored. By leveraging the unique physiological characteristics captured by PPG signals, such as heart rate variability, researchers believe that PPG biometrics could offer a secure and convenient method for verifying individuals identities. This research aims to explore the feasibility and effectiveness of using PPG biometrics for identification and authentication in various scenarios.

A. Definition of PPG biometrics

Biometrics, particularly utilizing photoplethysmography (PPG) signals, has emerged as a reliable method for identification and authentication. PPG technology involves measuring blood volume changes through light absorption, offering a unique biometric modality. Research by (J. Přibil et al., p. 7-10) explores the Gaussian mixture models (GMM) classifier for biometric identification using PPG signals from wearable sensors, showing promising results in subject identification accuracy. Additionally, (Yuchen Su et al., p. 726-737) introduces a two-factor authentication scheme, P2Auth, which integrates PIN and keystroke-related PPG measurements on wearables, enhancing authentication accuracy and security. These studies highlight the potential of PPG biometrics in advancing secure and accurate identification methods, leveraging physiological signals for robust user authentication. Through innovative strategies and advancements in PPG technology, biometric identification continues to evolve, addressing vulnerabilities in traditional authentication systems.

B. Importance of identification and authentication in today's digital world

In todays digital world, the importance of identification and authentication cannot be overstated. With the rise of cyber threats and online fraud, it is crucial for individuals and organizations to have robust mechanisms in place to verify identities and grant access to sensitive information. Identification ensures that the right individuals are granted access to specific resources, while authentication confirms that those individuals are who they claim to be. This layered approach helps to protect against unauthorized access and potential breaches of security. In addition, the use of biometric authentication methods, such as PPG biometrics, offers a higher level of security than traditional password-based systems. By utilizing unique physiological characteristics like heart rate variability, PPG biometrics provide a more reliable and secure means of verifying identities in the digital realm . This advanced technology not only enhances security but also improves user experience by simplifying the authentication process and reducing the risk of identity theft (Kim Ho Yeap et al.).

II. Advantages of PPG biometrics in identification

Furthermore, the utilization of PPG biometrics in identification offers numerous advantages over traditional methods. One key benefit is the non-intrusive nature of PPG technology, as it can be seamlessly integrated into existing devices such as smartphones and wearables without requiring any additional hardware. This convenience enhances user experience and reduces the need for multiple authentication methods. Moreover, PPG biometrics provide a high level of accuracy in identifying individuals, with studies showing recognition rates above 95%. This reliability is crucial in security-sensitive applications where precision is paramount. Additionally, PPG signals can be captured in real-time, enabling continuous monitoring for dynamic authentication purposes. This continuous authentication model enhances security by ensuring that the users identity is consistently validated throughout the interaction(Kim Ho Yeap et al.). Overall, the advantages of PPG biometrics demonstrate its efficacy as a promising technology for secure identification processes.

A. Non-intrusive and continuous monitoring

Continuous monitoring in user authentication, particularly through keystroke dynamics biometrics, offers a proactive approach to cybersecurity. By incorporating techniques such as Gaussian Mixture Model with Universal Background Model (GMM-UBM) and deep machine learning, the process becomes more robust and effective (Yunbin Deng et al.). This approach not only eliminates the need for additional hardware but also ensures seamless authentication without

disrupting the users workflow. Furthermore, the integration of user-centric anomaly-based detection with keystroke dynamics biometrics can enhance the security control mechanism, thus complementing traditional static authentication methods. As emphasized in (João Ferreira et al., p. 216-223), the importance of continuous identity verification highlights the potential for extending Intrusion Detection Systems (IDSs) to the user authentication level. By leveraging non-intrusive techniques such as keystroke dynamics analysis, systems can achieve a higher level of security and user identification accuracy in real-time scenarios.

B. High accuracy and reliability in user identification

A key requirement for user identification systems is high accuracy and reliability. Comprehensive user authentication must be built on robust biometric data to prevent unauthorized access. PPG biometrics offer a promising solution due to their unique features such as heart rate variability and blood flow patterns. By analyzing these physiological signals, PPG can achieve high accuracy levels in user identification. Research has shown that PPG-based systems can accurately differentiate individuals with a low error rate . Moreover, the reliability of PPG biometrics is demonstrated by their resistance to spoofing attacks, ensuring the security of the system (Gene Tsudik). Thus, the integration of PPG biometrics in identification and authentication processes can provide a secure and dependable solution for various applications.

III. Challenges and considerations in implementing PPG biometrics for authentication

The integration of photoplethysmography (PPG) biometrics for authentication poses intricate challenges and considerations in the context of advancing cyber-physical security measures. Leveraging the insights from (Oleksandr Kuznetsov et al., p. 9-15), which emphasizes the need for secure biometric authentication systems in the face of quantum computing threats, aligns with the exploration of robust authentication mechanisms. Additionally, (Chia-Wei Lien et al., p. 1-37) sheds light on the evolving landscape of biometric options for securing IoT devices, highlighting the complexity of selecting appropriate biometric modalities. When applied to PPG biometrics, these challenges manifest in the balance between user convenience and security efficacy, sensor reliability, and data stability over time. The strategic integration of PPG biometrics within authentication frameworks necessitates a nuanced understanding of user interaction requirements, computing capabilities, and opportunities presented by new sensor technologies, thereby underscoring the importance of comprehensive research in optimizing authentication protocols for enhanced cyber-physical security.

A. Security and privacy concerns

Amid the increasing adoption of PPG biometrics for identification and authentication purposes, there are growing concerns regarding security and privacy. One major issue is the vulnerability of biometric data to theft or unauthorized access. Unlike passwords or PIN codes, biometric information, once compromised, cannot be changed. This raises significant risks for individuals and organizations relying on PPG biometrics for secure access to systems or facilities. Furthermore, the collection and storage of biometric data raise ethical questions about consent and the potential misuse of personal information. As such, it is imperative for developers and implementers of PPG biometric systems to prioritize robust security measures and transparent privacy policies to mitigate these concerns. Proper encryption, authentication protocols, and regular audits can help safeguard biometric data and ensure trust among users (Richard Jiang et al.).

B. Environmental factors affecting PPG biometric readings

In addition to individual variations in physiology, environmental factors can also influence the accuracy and reliability of PPG biometric readings. For instance, changes in ambient temperature can affect the dilation and constriction of blood vessels, leading to fluctuations in the quality of PPG signals. Similarly, variations in humidity levels can impact the conductivity of the skin and the performance of PPG sensors, potentially leading to errors in biometric measurements. Furthermore, exposure to external light sources, such as sunlight or artificial lighting, can interfere with the detection of PPG signals by introducing noise into the readings. It is essential for researchers and practitioners to take these environmental factors into account when implementing PPG biometric systems to ensure consistent and accurate identification and authentication processes . By understanding and mitigating the impact of these factors, the reliability and effectiveness of PPG biometrics can be enhanced in real-world applications (National Research Council et al.).

IV. Conclusion

In conclusion, the use of PPG biometrics in identification and authentication presents a promising avenue for enhancing security measures in various applications. Through the analysis of individuals unique physiological characteristics, such as heart rate and blood flow patterns, PPG technology offers a sophisticated level of accuracy in verifying identities. This can help prevent unauthorized access to sensitive information and improve overall security protocols. However, like any technology, there are potential limitations and challenges that must be addressed. As further research is conducted in this field, it will be important to consider factors such as usability, scalability, and privacy concerns to ensure the widespread adoption of PPG biometrics. By overcoming these obstacles, PPG technology has the potential to revolutionize the way we approach identification and authentication in the future .

A. Summary of the benefits and challenges of using PPG biometrics for identification and authentication

On one hand, the use of PPG biometrics for identification and authentication offers several benefits. Firstly, this technology is non-invasive, making it user-friendly and easily integrated into daily activities. Additionally, PPG signals can be captured remotely, allowing for convenient and contactless authentication processes. Moreover, the uniqueness of individual PPG signals provides a high level of accuracy in identifying users, enhancing security measures. However, there are also challenges associated with the use of PPG biometrics. One significant concern is the potential for spoofing attacks, where adversaries attempt to deceive the system using fake or manipulated PPG signals. Ensuring the robustness of PPG-based authentication methods against such attacks remains a critical area of research . Furthermore, issues related to signal quality and environmental factors can impact the reliability and performance of PPG biometrics systems, emphasizing the need for ongoing technological advancements and improvements (Xiaoxia Yin et al.).

B. Future prospects and potential advancements in PPG biometric technology

Recent advancements in PPG biometric technology have opened up a myriad of possibilities for the future. One exciting prospect is the potential for improved accuracy and reliability in identifying individuals based on their unique physiological signatures. As researchers continue to refine algorithms and hardware, we can expect to see greater authentication security and reduced chances of false positives or negatives. Additionally, the development of wearable devices incorporating PPG sensors could revolutionize the way we approach personal security and access control. These devices could provide continuous monitoring of biometric data, offering a seamless and frictionless user experience while simultaneously enhancing security measures. In the near future, we may even see integration of PPG biometric technology in a wide range of applications beyond traditional identification and authentication, such as in healthcare monitoring and personalized fitness tracking.

References

- J. Přibil, A. Přibilová, I. Frollo, "Experiment with GMM-Based Subject Identification from PPG Signals Acquired by Wearable Sensors", 2023, pp. 7-10
- Yuchen Su, Guoqing Jiang, Yicong Du, Yuefeng Chen, Hongbo Liu, Yanzhi Ren, Huan Dai, Yan Wang, Shuai Li, Yingying Chen, "P2Auth: Two-Factor Authentication Leveraging PIN and Keystroke-Induced PPG Measurements", 2023, pp. 726-737
- Oleksandr Kuznetsov, Yelyzaveta Kuznetsova, Emanuele Frontoni, Yuriy Gorbenko, "Towards Robust Biometric Authentication: Implementing Post-Quantum Cryptography via Code-Based Fuzzy Extractors", 2023, pp. 9-15
- Chia-Wei Lien, Sudip Vhaduri, "Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey", 2023, pp. 1-37
- Yunbin Deng, Yu Zhong, "Keystroke Dynamics User Authentication Using Advanced Machine Learning Methods", 2015
- João Ferreira, H. Santos, "Keystroke Dynamics for Continuous Access Control Enforcement", 2012, pp. 216-223
- Kim Ho Yeap, Chee Theng Chow, Hui Tyen Low, Humaira Nisar, "Enhanced Biometric Identification Using Photoplethysmography Signals", Cambridge Scholars Publishing, 2024-03-25
- Kim Ho Yeap, Chee Theng Chow, Hui Tyen Low, Humaira Nisar, "Enhanced Biometric Identification Using Photoplethysmography Signals", Cambridge Scholars Publishing, 2024-03-25
- Gene Tsudik, "Computer Security – ESORICS 2023", Springer Nature
- Richard Jiang, Somaya Al-maadeed, Ahmed Bouridane, Prof. Danny Crookes, Azeddine Beghdadi, "Biometric Security and Privacy", Springer, 2016-12-21
- National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Whither Biometrics Committee, "Biometric Recognition", National Academies Press, 2010-12-12
- Xiaoxia Yin, Kendall Ho, Daniel Zeng, Uwe Aickelin, Rui Zhou, Hua Wang, "Health Information Science", Springer, 2015-05-05