International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 11 ǁ November 2024 ǁ PP. 130-133

Exploring the Efficiency and Security of Facial Recognition in Managing Personal Information

Save Von M. Villanueva, Rogee Hans S. Nierves
University of San Agustin, General Luna St, Iloilo City Proper, Iloilo City, Iloilo, Philippines
Corresponding Author: Rovilyn Osalla

Abstract
This paper is about the design and implementation of a password manager based on facial recognition for users, aimed at improving security and convenience in accessing digital vaults. The system is further targeted at supporting users with minimum technical knowledge. The study combines facial recognition technology with traditional passwords to provide a more secure means of user authentication that avoids common issues such as forgotten passwords, hacking, or mere inconvenience on the part of the user. The research findings showed that this hybrid solution would improve the user experience because authentication is faster and much more secure. The paper concludes that facial recognition being integrated into password management can effectively solve the increasingly demanding security issues in online management of personal information.

Keywords: *Facial Recognition, Digital Security, Password Management, User Authentication*

Date of Submission: 13-11-2024 Date of acceptance: 26-11-2024

I. INTRODUCTION

As digital technology continues to permeate everyday life, securing online personal information has become an increasingly pressing challenge. Users often face difficulties with traditional password systems, including the frequent forgetting of passwords and the rising threat of hacking attacks [1]. Traditional password management systems are often weak due to convenience-driven choices, such as simple passwords or poor password retention [2]. Furthermore, the growing complexity of user credentials, especially on mobile devices, exacerbates this issue [5]. Given these challenges, facial recognition technology has emerged as a promising solution for user authentication. Unlike traditional password-based systems, facial recognition offers a more secure and user-friendly approach, reducing both security risks and user inconvenience [3]. This study explores the development of a facial recognition-based password manager that not only addresses these security concerns but also ensures accessibility for users with low digital literacy. By leveraging facial recognition alongside traditional password methods, this study aims to propose a hybrid solution that enhances online security and improves user experience.

II. METHODOLOGY

This study employs a quantitative research approach to evaluate the effectiveness and efficiency of a facial recognition-based password manager. The primary objective is to measure the system's performance through various quantitative metrics, including facial recognition accuracy, login time, and security measures such as spoofing resistance and environmental condition adaptability.

The facial recognition algorithms employed in the system include Eigenface, PCA, and Fisherface for feature extraction, optimized to achieve high accuracy and efficiency. Data security is ensured through AES-256 encryption, which protects user data by securely encoding facial features. Technologies such as OpenCV, Dlib, and Face_recognition are utilized for face detection and recognition, while PyCryptodome handles the encryption process.

For data storage, a relational database like SQLite or PostgreSQL is used, ensuring secure management of user information. The user interface is designed with accessibility in mind, built using Tkinter or PyQt, which provides an intuitive platform for non-technical users to interact with the system.

Quantitative data will be gathered from the system's operation, including performance metrics and user feedback obtained through surveys. The analysis will focus on statistical correlations between system features and user experience, providing insights into the potential for facial recognition as an alternative to traditional password management methods.

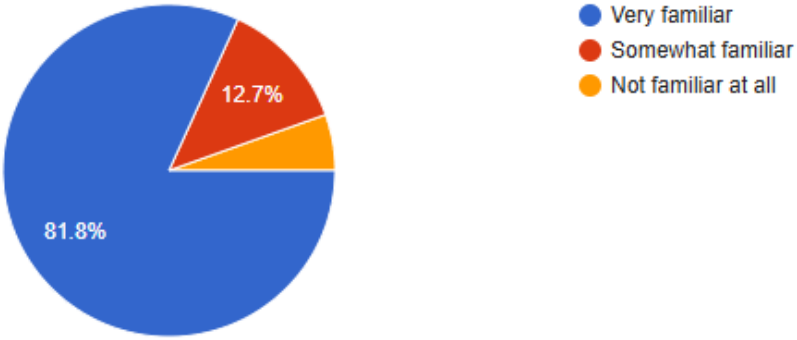
III. RESULTS AND DISCUSSION

The survey results were conducted through google form survey with 55 respondents. The survey indicates a general familiarity with facial recognition technology, with (12.7%) of respondents being somewhat familiar with it and (81.8%) being very familiar. While some of the participants had not yet used facial recognition for security purposes, a significant number (85.4%) had some experience with it. This suggests a growing acceptance of biometric methods, though adoption is still in its early stages for many.

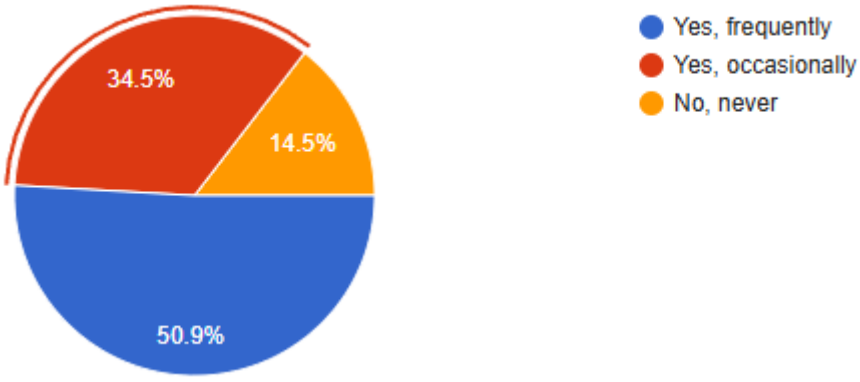
Respondents identified key concerns in traditional password management, with security and forgetting passwords being the most prominent issues. These concerns align with the perceived benefits of facial recognition, particularly in terms of increased security (20%) and faster login processes (18.2%). However, privacy concerns (60%) and the risk of spoofing (38.2%) remain significant barriers to full acceptance, highlighting the need for enhanced encryption and anti-spoofing technologies to increase user confidence.

The findings also reveal a strong willingness to adopt facial recognition for password management, with over half of respondents willing to recommend it to others. Most participants expressed openness to using a facial recognition-based password manager, provided it meets their security and usability expectations. These insights suggest that while facial recognition holds considerable promise for improving online security, addressing user concerns regarding privacy and spoofing will be crucial for broader adoption. Below is the graphical representation of the survey.

1. How familiar are you with facial recognition technology?

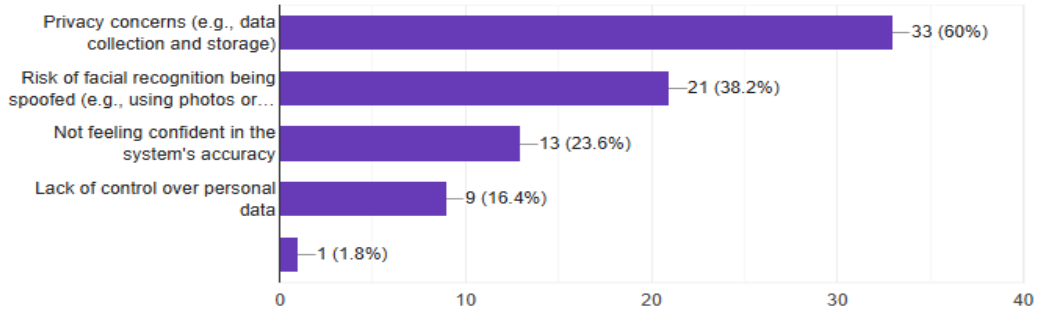


2. Have you ever used a facial recognition system for security or authentication purposes?

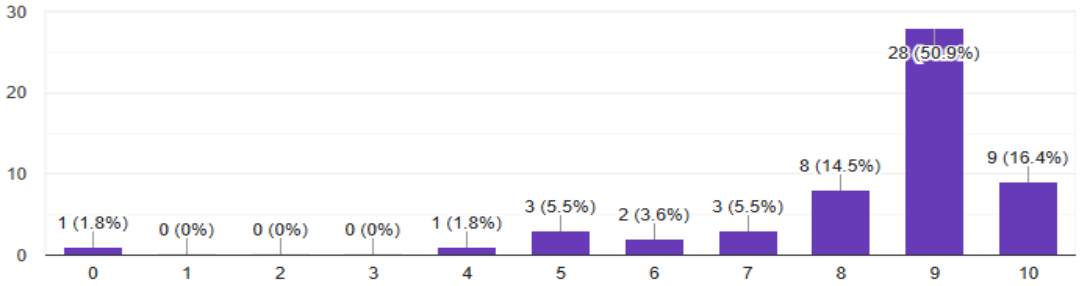


3. What do you expect to be the main benefit of using facial recognition to manage passwords?

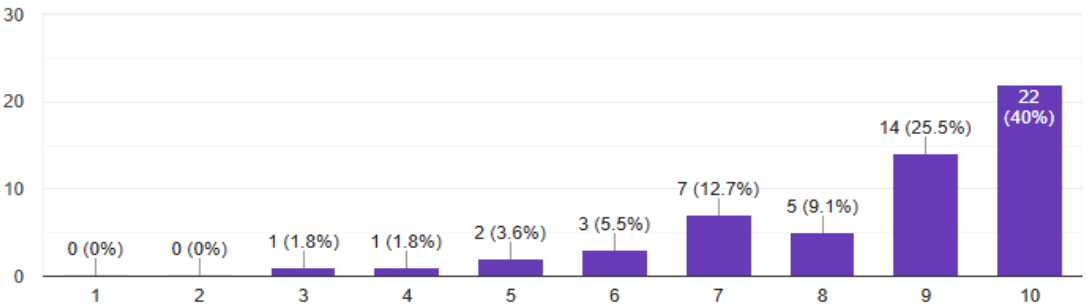
4. What is your biggest concern about using facial recognition for password management? (Select all that apply)



5. If you had the option, would you recommend using facial recognition as a password management solution to others?



6. How open are you to using biometric technologies (such as facial recognition) to manage your digital security?



Future work will include researching applications under different settings to ensure it is robust against most possible security attacks. This includes testing whether the system works as expected under different lighting conditions and other user scenarios with its resilience against all attempts to spoof the images or even videos of the user [10]. Continual improvement of the facial recognition algorithms would be paramount to continue holding at such high accuracy security levels. Other methods of multi-factor authentications, combining

facial recognition with other biometric modalities, would also boost security across the application [11]. This is intended to incorporate facial recognition technology into password management systems as one step toward stronger digital security. This application, therefore, will have the main objective of making it easier for users to perform improved and more accessible operations whenever the traditional password managing methods become hard to control. This would be much more significant in preventing the rising challenges in the digital security world as new protection strategies are found, one of which includes facial recognition to operate a password application.

IV. CONCLUSION

This study demonstrates that integrating facial recognition technology into password management systems offers a significant improvement in both security and user accessibility. By reducing reliance on traditional password systems, the facial recognition-based manager not only addresses common security vulnerabilities but also makes the authentication process more user-friendly, particularly for those less familiar with technology. While the current implementation shows promising results, future improvements to algorithm accuracy, anti-spoofing measures, and multi-factor authentication will further enhance the system's security and robustness, offering a more secure alternative to traditional password management solutions.we can improve user experience while addressing common security challenges.

REFERENCES

[1]. Liu & Cheung National Institute of Standards and Technology. "Face Recognition Vendor Test (FRVT)." used: foundational reference for facial recognition technology.
[2]. Mohialden Jain, A. K., et al. "An Introduction to Biometric Recognition." IEEE Transactions on Circuits and Systems for Video Technology. used: provides insight into biometric recognition systems.
[3]. Lin et al. Chen, Y. and Ross, A. "Score Normalization in Multimodal Biometric Systems." Pattern Recognition. used: discusses password issues and user challenges.
[4]. Morosan Kumar, A. and Zhang, D. "Personal Authentication Using Multiple Palmprint Representations." Pattern Recognition. used: addresses user inconvenience and password retention issues.
[5]. Raghavendra Gao, X., et al. "Forgetting of Passwords: Ecological Theory and Data." Rutgers University; Aalto University. used: highlights the psychological burdens associated with remembering multiple passwords.
[6]. Olanrewaju et al. Alshareef et al. "A Study of Gender Bias in Face Presentation Attack and Its Mitigation." Future Internet. used: discusses biases in facial recognition technology.
[7]. Zhou et al. Zawar "Real-Time Face Liveness Detection and Face Anti-spoofing Using Deep Learning." used: addresses the need for robust facial recognition systems.
[8]. Srinivas et al. Raghavendra "AuthNet: A Deep Learning based Authentication Mechanism using Temporal Facial Feature Movements." used: explores advanced authentication mechanisms and their implications.
[9]. Khan et al. Gupta "Smart Attendance System Using Face Recognition: A Machine Learning Approach." International Journal of Research Publication and Reviews. used: discusses the integration of facial recognition with other technologies.
[10]. Tang et al. Liu "Enhancing Deepfake Detection With Diversified Self-Blending Images and `Residuals." IEEE Access. used: addresses the challenges of spoofing in facial recognition.
[11]. Boonroungrut et al. Porras et al. "Development and evaluation of a machine learning-based point-of-care screening tool for genetic syndromes in children." The Lancet Digital Health. used: highlights the potential of machine learning in facial recognition applications.