Securing Smartphone User Authentication using Teeth Pattern

Sushil Mhetre[1], Dr. Shashikant V. Athawale[2], Latika Kumare[3], Sanket Lipne[4], Sumeet Koli[5]
[2]Associate Professor,
[1]Department of Computer Engineering,
[1]AISSMS College of Engineering, Pune, India

Abstract

In this study, we propose a novel approach to smartphone user authentication that leverages teeth patterns. User authentication is critical for smartphone security and privacy protection. Despite the existence of numerous authentication methods on these devices, ongoing discoveries of security vulnerabilities persist, revealing limitations in traditional methods like PINs, passwords, patterns, and fingerprints. Biometrics utilizing teeth images is additionally expected to achieve reliable and robust individual authentication since teeth are unique to each individual and hardly change during adulthood, thus proving to be a modality for smartphone authentication. In contrast to previous research endeavors employing diverse methods, our work explores a new field by combining an advanced feature regularization system with a deep learning architecture. This novel method seeks to produce extremely unique embeddings, guaranteeing unmatched user authentication accuracy. We foresee the model being trained end-to-end with a limited number of samples, which will effectively minimize the time and energy required for the authentication process. We anticipate the development of an enhanced smartphone authentication method that aims to elevate smartphone security by leveraging individuals' dental patterns and providing a secure, non-intrusive user authentication experience to unlock smartphones and mobile devices.

Index Terms - User authentication, Smartphone, Teeth pattern, Security, Deep Learning

I. INTRODUCTION

In the digital age, where smartphones have become an indispensable part of our lives, safeguarding sensitive personal data has never been more crucial. The widespread usage of smartphones has led to an increased reliance on user authentication methods to protect valuable information. Common methods like passwords, draw patterns, fingerprint recognition, and face recognition, while popular, have shown vulnerabilities – from being compromised to the risk of theft and deception. The vulnerability of traditional methods, such as PINs[10], to theft, forgetfulness, and risk of being peeped or stolen by attackers underscores the necessity for more reliable and user-friendly identification solutions. Biometrics, which authenticates individuals based on unique biological or behavioral traits, presents a promising resolution to this challenge.

This paper advocates for teeth patterns as a superior biometric trait due to their stability, unlike facial features susceptible to alterations, introducing a groundbreaking modality of authentication that leverages this often-overlooked biological characteristic. While fingerprint and face recognition systems are commonly employed, they are susceptible to fraudulent activities. For instance, fingerprint-based authentication has been known to be compromised, and face recognition-based authentication can be tricked by anti-surveillance prosthetic masks[9]. These factors indicate the need for more robust techniques. Striking a balance between security and ease of use, teeth-based authentication emerges as a compelling solution, reshaping smartphone security paradigms.

Teeth patterns are inherently distinctive, difficult to counterfeit, and remarkably resilient to changes over time. This innovation amalgamates cutting-edge hardware and software**,** ensuring a robust and real-time authentication process. Moreover, the utilization of teeth patterns fosters inclusivity, allowing individuals with disabilities or conditions that affect their other biometrics to enjoy secure access. Moreover, dental biometrics, widely used in forensic scenarios, offers high resistance to decomposition, making it an ideal choice for authentication even in challenging conditions.

By utilizing teeth images captured through standard on-device cameras[1], this method provides a seamless and user-friendly alternative to traditional authentication schemes. Our goal is not to replace existing authentication methods but to offer users an intriguing alternative that combines security, reliability, and accessibility to unlock the smartphone. This research contributes to the ongoing efforts to create a safer digital environment for smartphone users, ensuring the protection of their personal data without compromising usability.

II. LITERATURE REVIEW

Dental radiograph alignment and matching were the initial methods of introducing dental biometrics. This work was carried out in 2005 by H. Chen and A. K. Jain [2]. Dental structures are among the last body parts to degrade after death, making them ideal for applications in forensic dentistry [3]. Several studies have delved into dental biometrics, ranging from dental impressions to X-ray images for forensic identification [3]. These methods make use of radiographs, which call for specialized equipment and extremely unpleasant settings for the user.

Hence, our work focuses on a non-invasive approach using teeth photos captured by standard smartphone cameras without requiring extensive hardware infrastructure.

In the study conducted by Dong-Ju Kim and Kwang-Seok Hong, a pioneering multimodal biometric authentication approach was introduced in 2008, employing teeth image and voice as distinguishing traits for mobile device security [5]. Leveraging techniques from image processing, signal analysis, and pattern recognition, the system demonstrated promising results with an Equal Error Rate (EER) of 2.13%.

While extending their study ahead, Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong in 2010 presented a new multimodal system for authentication in mobile environments using Face, Teeth, and Voice biometric modalities [6]. A variety of fusion strategies were used in this study to combine data from the three modalities, such as the weighted-summation rule, K-NN, Fisher, and Gaussian classifiers. The weighted summation method outperformed other classification strategies with the lowest error rate (1.64%). Notably, single modalities showed considerably higher error rates (7.75% for teeth modality) when trained independently. These results highlight the advantages and disadvantages of the suggested multimodal strategy.

The 2020 study [7] by Jiang, Cao, Liu, Xiong, and Cao presented a novel approach for precise camera angle estimation in the context of smartphone security, an essential step toward actual use. Using continuity between pictures and LBP-based texture properties, their method prevented prominent attacks such as external force attacks and image/video spoofing. Using more than 300 participants, the study carefully assessed SmileAuth's performance using Random Forest feature selection. It demonstrated superior precision (99.74%) and F-score (98.69%) across a variety of circumstances. This system could be used as a standalone or second layer of security authentication mechanism in smartphones.

A new biometric authentication method based on distinctive teeth patterns was described by Pandia, Arora, Jain, Bharadwaj, Bhatia, and Tiwari in a recent paper [1] from 2021. Advanced techniques such as ROI extraction, CLAHE image enhancement, DAM, SAM, and CAM feature extraction, and Large Margin Cosine Loss neural network training were all included in the method. Their technique, DeepTeeth, proved the value of dental patterns in sample discrimination with an astounding 97.61% accuracy rate. The study stressed how important distinct tooth patterns are for improving the security of biometric authentication.

Building on the foundation laid by previous research, we aim to develop the Teeth Lock system which will focus on improving the system performance and current efficiency standards as we practically implement the authentication model using the teeth pattern on smartphones by utilizing deep learning and Neural network-based techniques.

III. SYSTEM DESIGN

In this segment, we'll delve into the methodology employed in our Teeth Lock system, which is centered on utilizing teeth images as the primary biometric trait. Our system is structured into several key subsections: Data Collection, Data Preprocessing, Feature Extraction, Comparison, Decision Making, and following the output respective action will be taken.

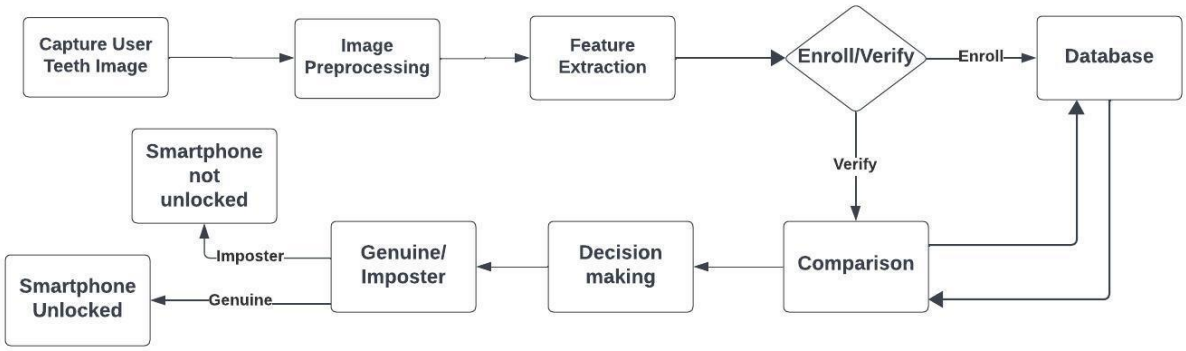

Fig. System Architecture

The block diagram above makes it simple to understand how the system operates. Initially, the user's teeth image will be taken with the camera of the smartphone device that has our application installed. The application will employ a rectangular block to guide the user in capturing the teeth image from the entire image. Following ROI recognition, the acquired image will undergo preprocessing and enhancement to make the best use of its features. This is followed by feature extraction, which extracts relevant features. The extracted data will be kept in the database if the user is a new one. The information that was recorded at that time will be compared with the information kept in the database the next time the user utilizes the system after enrolling in it. The user's phone will be unlocked if the data from both sides matches and is more than the threshold value; otherwise, the user will be considered to be an impostor and the phone will stay locked.

IV. CONCLUSION

In the modern world where technology is advancing rapidly, the threats and security concerns related to them are also increasing. This article offers a novel and secure approach to smartphone user authentication by using teeth patterns to provide a new and safe method of authenticating smartphone users. It is both user-friendly and meets the demand for enhanced security. The proposed Teeth Lock system combines deep learning and neural network techniques, making it a promising solution for enhancing smartphone security in a user-centric manner. By protecting smartphone users' personal information, the research helps to create a safer online environment.

V. REFERENCES

[1] A. Pandia, G. Arora, A. Jain, R. Bharadwaj, A. Bhatia and K. Tiwari, "DTeeth: Teeth-photo Based Human Authentication for Mobile Devices," 2022 IEEE International Joint Conference on Biometrics (IJCB), Abu Dhabi, United Arab Emirates, 2022, pp. 1-8, doi: 10.1109/IJCB54206.2022.10007983.

[2] H. Chen and A. K. Jain. Dental biometrics: Alignment and matching of dental radiographs. *IEEE transactions on pattern analysis and machine intelligence*, 27(8):1319–1326, 2005.

[3] P. Pittayapat, R. Jacobs, E. De Valck, D. Vandermeulen, and G. Willems. Forensic odontology in the disaster victim identification process. The Journal of forensic odontostomatology, 30(1):1, 201

[4] Tae-Woo KIM, Tae-Kyung CHO, "Teeth Image Recognition for Biometrics", IEICE Transactions on Information and Systems, vol. E89- D, no. 3, pp.1309-1313, 2006

[5] Dong-Su Kim and Kwang-Seok Hong. Multimodal biometric authentication using teeth image and voice in a mobile environment. 2008. IEEE Transactions on Consumer Electronics. IEEE, 54:1790–1797, 2008.

[6] Dong-Su Kim, Kwang-Woo Chung and Kwang-Seok Hong. Person authentication using face, teeth and voice modalities for mobile device security. 2010. IEEE Trans. Consumer Electron. IEEE, 56(4):2678–2685, 2010.

[7] H. Jiang, H. Cao, D. Liu, J. Xiong, and Z. Cao. Smileauth: Using dental edge biometrics for user authentication on Smartphones. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(3):1–24, 2020.

[8] G. Koch, R. Zemel, and R. Salakhutdinov. Siamese neural networks for one-shot image recognition. In *ICML deep learning workshop*, volume 2. Lille, 2015.

[9] Nesli Erdogmus and Sébastien Marcel. Spoofing face recognition with 3d masks. 2014. IEEE Trans. Information Forensics and Security, IEEE, 9(7):1084–1097, 2014

[10] Dingyi Fang Xiaojiang Chen Kwang In Kim Ben Taylor Guixin Ye, Zhanyong Tang and Zheng Wang. Cracking android pattern lock in five attempts. 2017. 24th Annual Network and Distributed System Security Symposium (NDSS), 2017.