ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

SECURING SMARTPHONE USER AUTHENTICATION USING TEETH PATTERN

Sushil Mhetre[1], Shashikant V. Athawale[2], Latika Kumare[3], Sanket Lipne[4] and Sumeet Koli[5]
[2]Associate Professor,
[1]Department of Computer Engineering,
[1]AISSMS College of Engineering, Pune, India
[1]sushilmhetre38@gmail.com, [2]svathawale@gmail.com, [3]latikavlk1152@gmail.com, [4]sanketlipne@gmail.com and [5]sumitkoli2002@gmail.com

ABSTRACT

This paper presents a groundbreaking approach to smartphone user authentication by leveraging teeth patterns, addressing challenges posed by traditional methods like PINs and biometrics. Our proposed system integrates a Deep learning (DL) network, a user-friendly mobile app, and mkdt broker notifications. Using mobile phone cameras, deployed with frontal Haar Cascade, the system captures and extracts a 128x128-pixel Region of Interest (ROI) around the mouth, employing preprocessing for enhanced image clarity. The system architecture features a Deep Convolutional Neural Network (CNN) in Python 3.11 with Tensorflow, achieving a robust 98.04% accuracy and EER - 2.5% and CRR -93%, while validation accuracy achieved 99.12% mark for classification purposes. Real-time decision-making during feature matching ensures swift authentication. Comparative analysis indicates promising performance in our system compared to existing methods. Furthermore, the mobile app interface delivers immediate authentication results, enhancing user experience in terms of security and efficiency. This research establishes a foundation for future mobile device security enhancements, providing a practical, innovative solution for immediate implementation. The integration of teeth patterns as a biometric identifier shows promising results, overcoming limitations in traditional authentication methods. The proposed system marks a significant advancement in smartphone security, offering users a reliable and user-friendly authentication experience.

Index Terms - User Authentication, Smartphone Security, Teeth Pattern, Machine Learning, Mobile Biometrics, Image Processing, Convolutional Neural Network (CNN)

I. INTRODUCTION

In our increasingly digital age, smartphones have evolved into indispensable companions, holding a plethora of sensitive personal data. This reality underscores the paramount importance of implementing robust security measures. While widely adopted, popular user authentication methods such as passwords, patterns, fingerprints, and facial recognition are not without vulnerabilities. The susceptibility to theft, forgetfulness, and the potential for deception [10] highlight the pressing need for more reliable and user-friendly identification solutions.

The ease with which attackers can steal PINs, observe drawn patterns, or exploit prosthetics to bypass fingerprint and face recognition systems [9] accentuates the urgency for enhanced security measures. Recognizing this, biometrics emerges as a technology that holds promise for shaping the future of secure identification. This paper advocates for teeth patterns as a superior biometric identifier due to their extraordinary stability, especially when compared to facial features that undergo changes over time. Despite the common usage of fingerprint and face recognition, they remain susceptible to forgery. Instances of compromised fingerprint scanners and the vulnerability of facial recognition to disguises [9] underscore the need for more resilient and foolproof techniques.

Teeth-based authentication presents itself as a compelling solution, effectively striking a balance between security and user convenience. The uniqueness and inherent difficulty in replication of teeth patterns, coupled with their remarkable resilience to changes throughout an individual's life, make them an innovative and robust option for authentication.Additionally, dental biometrics, well-established in forensic applications for its resistance to decomposition, proves to be an ideal choice for authentication even in challenging and adverse environmental conditions.

By harnessing the capabilities of standard smartphone cameras to capture dental images [1], this authentication method provides a user-friendly alternative to traditional schemes. It is important to note that the aim of this proposed approach is not to replace existing options but to furnish users with a secure, reliable, and accessible alternative for unlocking their smartphones. This research aligns with ongoing efforts to create a safer digital environment for smartphone users, ensuring the protection of their personal data without compromising usability.

II. RELATED WORK

Dental biometrics was first introduced through dental radiograph alignment and matching. H. Chen and A. K. Jain completed this work in 2005 [2]. dental architecture are perfect for use in forensic dentistry because they are among the last body parts to decompose after death[3]. Dental biometrics, including X-ray pictures for forensic identification and dental impressions, have been the subject of numerous studies[3]. These techniques rely on radiographs, which require specialized tools and highly uncomfortable conditions for the user.Because of this, our work focuses on a non-invasive method that leverages images of teeth taken using common smartphone cameras and doesn't require a large hardware infrastructure.

In the 2008 work by Dong-Ju Kim and Kwang-Seok Hong, a novel multimodal biometric authentication method was presented, using speech and teeth image as characteristics that set mobile device security apart[5]. Utilizing methods from signal analysis, pattern recognition, and image processing, the system showed encouraging outcomes with an Equal Error Rate (EER) of 2.13%.

Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong in 2010 introduced a new multimodal system for authentication in mobile environments using Face, Teeth, and Voice biometric modalities[6], furthering their research in the process. In this work, data from the three modalities were combined using a range of fusion algorithms, including the weighted-summation rule, K-NN, Fisher, and Gaussian classifiers. Having the lowest error rate (1.64%), the weighted-summation method performed better than the other categorization techniques. Notably, when trained alone, single modalities displayed noticeably higher error rates (7.75% for teeth modality). These outcomes demonstrate the benefits and drawbacks of the recommended multimodal approach.

An important step toward practical application was the 2020 study[7] by Jiang, Cao, Liu, Xiong, and Cao, which introduced a unique method for accurate camera angle estimate in the context of smartphone security. Their technique prevented well-known assaults including external force attacks and image/video spoofing by using continuity between images and LBP-based texture attributes. The study extensively evaluated SmileAuth's performance utilizing Random Forest feature selection on a sample of over 300 participants. It showed excellent accuracy (99.74%) and F-score (98.69%) in a range of situations. This technology could be applied to smartphones as a stand-alone or second-layer security authentication method.

In a recent paper[1] from 2021, Pandia, Arora, Jain, Bharadwaj, Bhatia, and Tiwari developed a new biometric authentication approach based on unique tooth patterns. The method incorporated advanced techniques like Large Margin Cosine Loss neural network training, ROI extraction, CLAHE image enhancement, DAM, SAM, and CAM feature extraction. Their method, DeepTeeth, demonstrated with an amazing 97.61% accuracy rate the importance of dental patterns in sample discrimination. The study emphasized how crucial different tooth forms are to enhancing biometric authentication security.

The objective of our study is to develop the Teeth based authentication system, building on the groundwork established by earlier research. We will employ deep learning and neural network-based techniques to practically implement the authentication model using the teeth pattern on smartphones, with an emphasis on enhancing system performance and current efficiency standards.

III. PROPOSED APPROACH

3.1 User Interaction

User interaction is a pivotal component of the image-based authentication system. The mobile application interface allows users to effortlessly capture images using their smartphones' native cameras. This initiates the

authentication pipeline, leading to subsequent stages of image preprocessing, mouth area extraction, and feature matching against the trained Convolutional Neural Network (CNN) model. This user-centric approach prioritizes simplicity and effectiveness, ensuring a straightforward and intuitive experience. The mobile application serves as a central hub for users to engage with the authentication system.

3.1.1 Image Capture

A) Data Collection: During the training phase, the dataset is created by collecting 100 image samples from 50 subjects in two sessions, which accounted for 5000 images as the total dataset for model training and validation ahead. A platform was developed for capturing user images via the smartphone camera, which smoothes the data collection process.

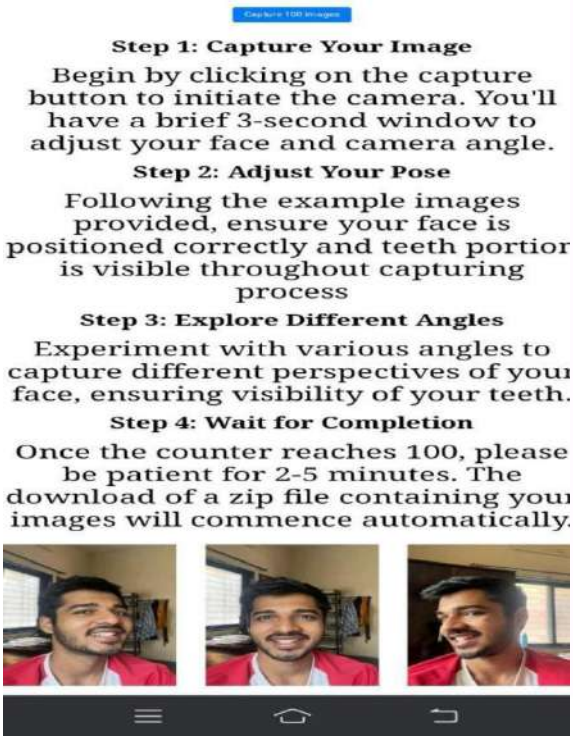

Fig 1. A) Data Collection

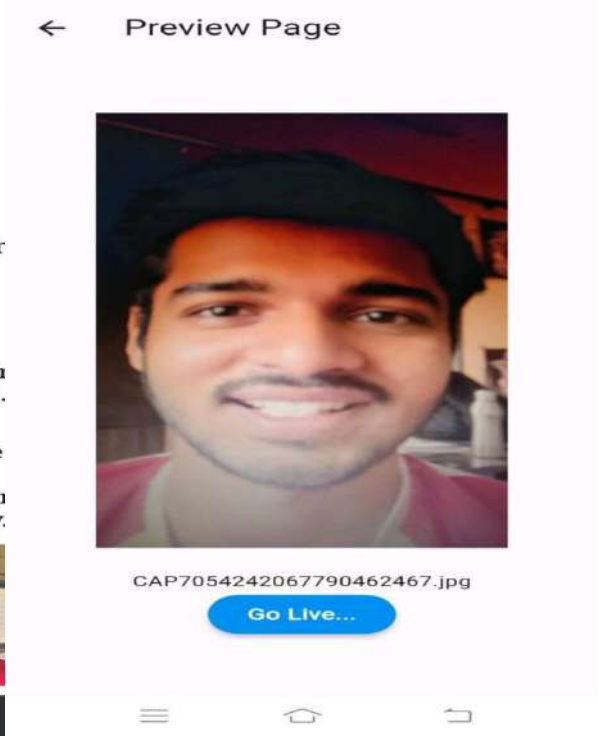

Fig 1. B) Authentication

B) Authentication Process: Images are captured through the mobile application, initiating the authentication process for the user based on the captured dental pattern image. The dataset has been made publicly available for future research purposes.

3.2 Preprocessing

Preprocessing techniques are applied to enhance image quality, preparing it for subsequent analysis. Utilizing, Frontal Haar Cascade, the system consistently extracts a standardized mouth area of 128x128 pixels, focusing on the region of interest for optimal feature extraction. The preprocessing stage involves region-of-interest (ROI) extraction, specifically targeting the mouth area within each facial image. This process is integral to focusing the model on relevant features for teeth recognition. Additionally, data augmentation techniques are applied to enhance the diversity of the training dataset. Techniques such as horizontal and vertical flips, along with rescaling, are implemented to improve model generalization.

3.3 Deep Learning Model: Backbone Network

The deep learning-based convolutional neural network model is a crucial element trained in the backend using Python 3.11 and Tensorflow, Pycharm ID**.** The training dataset comprises mouth area images extracted from user-

captured images. This trained model acts as the backbone for feature extraction and comparison during the authentication process.

CNNs are a class of deep neural networks that are particularly effective for image recognition and classification tasks. They consist of multiple layers, including convolutional layers, pooling layers, and fully connected layers. The key operations in CNNs include convolution, activation, pooling, and fully connected layers.

Mathematical representation for CNN:

$Z^{[l]} = W^{[l]} * A^{[l-1]}+b^{[l]}$

Where , $Z^{[l]}$ is the output of the convolutional layer.

$W^{[l]}$ is the filter weights.

$A^{[l-1]}$ is input to the layer.

$b^{[l]}$ is the bias term.

The proposed CNN architecture consists of multiple convolutional layers followed by pooling layers to extract features from the input images. Dropout layers are included to prevent overfitting, and fully connected layers are used for classification.

Model: “Sequential”

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 128, 128, 64)	1792
max_pooling2d (MaxPooling2D)	(None, 64, 64, 64)	0
conv2d_1 (Conv2D)	(None, 64, 64, 128)	73,856
max_pooling2d_1(MaxPooling2D)	(None, 32, 32, 128)	0
conv2d_2 (Conv2D)	(None, 32, 32, 256)	295,168
max_pooling2d_2(MaxPooling2D)	(None, 16, 16, 256)	0
Flatten (Flatten)	(None, 65536)	0
dense (Dense)	(None, 128)	8,388,736
dropout (Dropout)	(None, 128)	0
dense_1(Dense)	(None, 64)	8,256
dropout_1(Dropout)	(None, 64)	0
Dense_2 (Dense)	(None,50)	1,885

Table 1: Model Summary

Loss Function and Optimization:
To optimize the performance of the CNN model, a loss optimization strategy is employed during training. The model is compiled using the Adam optimizer, and sparse categorical cross-entropy is chosen as the loss function. The training process involves iterative epochs, where the model learns to map input features to the corresponding tooth classes. The evaluation of the model's performance is facilitated through metrics such as accuracy.

3.4 Communication
The MKDT broker facilitates seamless communication between the mobile application and the backend machine learning network. This ensures efficient exchange and processing of captured images, contributing to real-time decision-making.

IV. SYSTEM DESIGN
In this segment, we'll delve into the methodology employed in our teeth-based authentication system, which is centered on utilizing teeth images as the primary biometric trait. Our system is structured into several key subsections: data collection, data processing, feature extraction, comparison, decision-making, and following the

output, the respective action will be taken. A similar architecture has been deployed on laptops as well to secure and authenticate laptops using dental patterns.

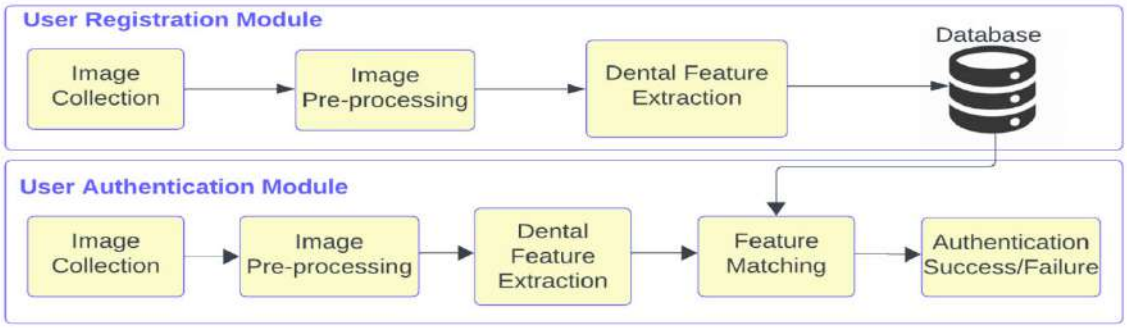

Fig 2: System Architecture

The system's operation is easily understood thanks to the block diagram above. The user's teeth will first be photographed using the smartphone's camera, which is equipped with our application. To fully utilize its attributes, the obtained image will go through preprocessing and augmentation after ROI recognition. Feature extraction, which extracts pertinent features, comes next. If the user is a new one, the extracted data will be retained in the database. The next time the user uses the system after signing up, the data that was entered at that time will be compared with the data stored in the database.If the data from both sides matches and exceeds the threshold value, the user's phone will be notified of successful authentication; if not, the user will be deemed to be an impostor, and the user interface will display the necessary messages.

IV. EXPERIMENTAL EVALUATION

The user authentication module initiates with image capture through the mobile application, followed by preprocessing, feature extraction, and matching against the trained CNN model. Real-time decision-making leads to authentication success or failure, with results communicated to users through the app interface. This proposed approach integrates image acquisition, preprocessing techniques, system architecture, CNN model building, and training strategies to achieve effective teeth recognition. The combination of these components contributes to a robust and accurates ystem for Dental image analysis.

A. Methodology

Experimental Setup: In order to train a Convolutional Neural Network (CNN) model for teeth recognition using the provided code, your system should have a multi-core CPU (ideally with 8GB of RAM) at minimum and optionally an NVIDIA GPU that is compatible with CUDA for quicker computations. TensorFlow, NumPy, scikit-learn, Matplotlib, CMake, and Visual Studio or Jupyter Notebook Build Tools must be installed in order to run the Python code. Make sure there is enough disk space on your computer to hold the dataset, model checkpoints, and additional files. Installing the necessary packages with Pip may require an internet connection. Install the required libraries in a Python environment, then set up the environment and modify the parameters according to the size of the dataset and other requirements.

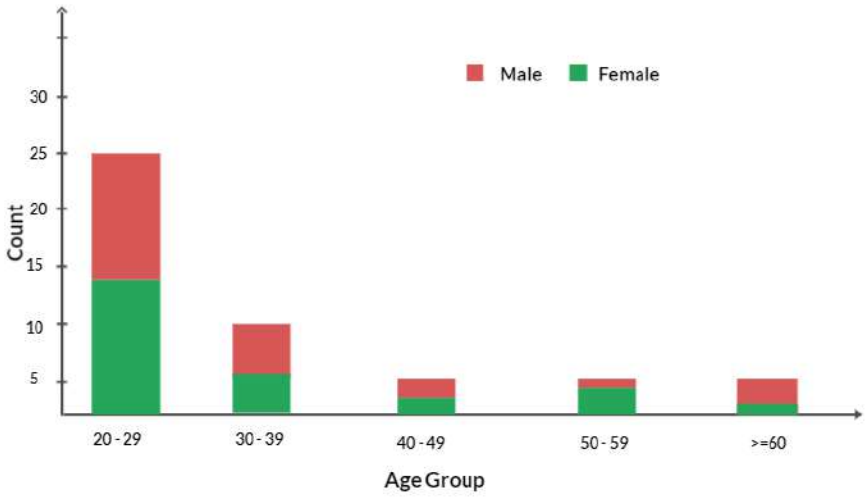

Fig: Demographics of the TeethPhoto database of subjects.

Description of the Dataset: We constructed an internal database containing 5000 photos from 50 subjects, each of whom provided 100 samples, for our dataset. These images functioned as the training set for our model, which was designed to be applied to a particular task such as classification or image recognition. After being trained on such a dataset, a model can gain the ability to identify patterns and features in the photos, which will enhance its feature extraction process and its capacity to categorize and forecast data in the future. The robustness and efficiency of the trained model in completing the intended task are influenced by the quantity and diversity of the dataset.

Fig: Teeth Dataset

Evaluation Metrics: Our model demonstrated good performance, with a 93% Correct Recognition Rate (CRR) and an Equal Error Rate (EER) of 2.5%. By highlighting the point at which the false acceptance rate and the false rejection rate equal, the EER offers an assessment of the model's overall performance in a classification task. A lower EER is indicative of superior performance. Meanwhile, the percentage of accurately detected cases among all the instances in the collection is displayed by the CRR. With a 93% confidence rate in correctly identifying occurrences across all groups or categories, our model performs well. Together, these metrics suggest that the model performs brilliantly in the task for which it was created, exhibiting high recognition accuracy and low mistake rates.

Final Decision: An experimentally determined threshold is always the basis for the decision on whether or not the two samples represent the same individual. A threshold limit is imposed; if the accuracy is higher than the threshold, the user is considered authenticated; if not, they are classified as unknown.

V. RESULT AND DISCUSSION

The model's performance metrics paint a picture of remarkable achievement across various evaluation criteria. With an exceptional validation accuracy of 99.05%, the model demonstrates its proficiency in learning relevant patterns from the data. The impressively low validation loss further solidifies its effectiveness.In terms of distinguishing between genuine and impostor samples, the Equal Error Rate (EER) of 2.56, along with a Correct Rejection Rate (CRR) of 92%, showcases commendable performance. While there's room for improvement in this aspect, the overall performance remains commendable.

The classification report reveals a nuanced understanding of the model's success, where precision, recall, and F1-score may vary across classes. However, the model's ability to correctly identify several classes with high precision and recall indicates its efficacy in capturing distinguishing features. Moving forward, augmenting the dataset, fine-tuning the model architecture, optimizing hyperparameters, and potentially incorporating ensemble learning or domain-specific knowledge can further enhance the model's capabilities, ensuring continued success in diverse scenarios.

During the evaluation, anomalies like outliers and class imbalances may arise, affecting model performance. Outliers, often due to data errors or rare events, can skew results. Techniques such as robust statistical methods or outlier removal can mitigate their impact. Class imbalances, where some classes have fewer samples, can bias predictions. Oversampling, undersampling, or class-weighting methods help address this issue. Future research could explore advanced anomaly detection techniques like unsupervised learning with autoencoders or GANs, and deep learning architectures such as graph neural networks.By addressing these anomalies and pursuing future research directions, anomaly detection systems can become more effective and applicable in real-world scenarios.

Our work does not aim to replace the existing authentication schemes but would like to provide users an interesting alternative. We believe there is no single best biometrics for authentication in terms of accuracy, robustness and accessibility. The proposed system can be easily integrated with existing schemes to add another layer of protection. The proposed system can be combined with facial recognition to enable multi-modal authentication.We plan, in future works, to enhance the processing time in the mobile environment through improved algorithms or optimization processes.

IV. CONCLUSION

In the modern world where technology is advancing rapidly , the threats and security concerns related to them are also increasing. It is both user-friendly and meets the demand for enhanced security. The proposed Teeth pattern based authentication system combines deep learning and neural network techniques, making it a promising solution for enhancing smartphone security in a user-centric manner. This article presents a cutting-edge smartphone authentication system, utilizing teeth patterns for heightened security. Through advanced deep learning methodologies like Convolutional Neural Networks (CNNs), the Teeth pattern based authentication system achieves impressive accuracy and user-centric usability. With a 92% Correct Recognition Rate (CRR) and a 2.5% Equal Error Rate (EER) for tiny RoI image of 128×128 size, it offers robust authentication while ensuring user convenience and privacy. By combining technological innovation with user-focused design, the system addresses evolving security challenges, promising a safer and more secure digital experience for smartphone users.

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.