GAA Use Only
Proposal Number: _____

University of Dayton
Graduate
Academic Affairs

GRADUATE STUDENT SUMMER FELLOWSHIP APPLICATION COVER SHEET

Student Name (Last, First, MI): Jadhav Ishwar S
Student ID Number: 1017360500 Student Email Address: jadhavi1@udayton.edu
Department: Computer Science +4 Zip Code: 45469

Degree Program: ☑Master's ☐Doctoral
Program Name (e.g., M.S. in Biology): M.S. in Computer Science
Program Start Date (Month/Year): August/2022
Expected Graduation Date (Month/Year): May/2024

Proposed Project:
Have you received prior GSSF awards? ☑No ☐Yes If yes, list years: _____
GSSF Application Number: ☑M1 ☐M2 ☐DOC1 ☐DOC2 ☐DOC3
Faculty Sponsor's Name: Prof. Tam Nguyen
Where will the work be conducted? Department of Computer Science

Does the project involve: (Check all that apply.)
☐Human Subjects ☐Animal Subjects
☐Other Students ☐Other Faculty

If any of the boxes above are checked, explain in your proposal.

Student: *Sign below to certify that you have read and understand the GSSF Guidelines & Instructions, and that you meet all eligibility criteria as stated, including those for financial support.*

Student Signature: Date: 21/02/2023

Faculty Advisor & Department Chair: *Sign below to certify that you endorse the proposed project and that the student meets all appropriate eligibity criteria as stated in the GSSF Guidelines & Instructions.*

Advisor: Chair:

For GAA Office Use Only:
Date Proposal Received: _____ On time: ☐Yes ☐No
Dates Progress Report(s) Received: _____ On time: ☐Yes ☐No
Presentation(s) at Stander: ☐Yes ☐No
For third award applicants, is there evidence of other presentations? ☐Yes ☐No
If yes, ☐Internal ☐External

GAA Signature: _____

February 23, 2023

To Graduate Student Summer Fellowship Committee:

I am writing to highly recommend Ishwar Jadhav for the Graduate Student Summer Fellowship in Facial Expression Analysis for User Authentication. As Ishwar's advisor for the semester, I have had the pleasure of watching him excel in his academic pursuits and develop a strong interest in facial expression analysis for user authentication.

Student's academic performance to date:
Ishwar has a keen interest in exploring the intersection of computer vision and user authentication, with a particular focus on facial expression analysis. His strong foundation in machine learning and computer vision has been evident in his research projects, where he has demonstrated a deep understanding of the underlying algorithms and a talent for applying these techniques to solve complex problems. His past research experience, including developing a facial recognition system for user authentication, has been particularly relevant to the proposed project. He has worked extensively with open-source tools like MediaPipe Holistic and demonstrated the ability to leverage these tools effectively to achieve the desired outcomes.

Quality and anticipated contribution of the proposed scholarly effort:
As mentioned above, Ishwar's previous work in facial gesture recognition not only outperformed. the literature but also opened a new gate for him to improve the work further and enhance the results. His idea of using the Face mesh technique to plot facial landmarks is genius, I am confident that his work will contribute to the field, and many researchers will benefit from his work. I have no doubt that his research work will lead to several important projects.

I believe Ishwar is an excellent fit for the Graduate Student Summer Fellowship in Facial Expression Analysis for User Authentication. His ability to work collaboratively and communicate technical concepts clearly would be an asset to any research team. His passion for the topic and drive to learn and improve are infectious and inspiring.

In conclusion, I have no hesitation in strongly recommending Ishwar for the GSSF. I am confident that he will be an asset to the program and will make valuable contributions to the field of facial expression analysis.

Sincerely,
Dr. Tam Nguyen
Department of Computer Science
University of Dayton
Hathcock Hall 141
(937) 229-3893
tamnguyen@udayton.edu

Facial Expression Analysis for User Authentication

Student: Ishwar Jadhav

Advisor: Dr. Tam Nguyen

I. Research Objectives

Do you know the feeling when you go out and realize you left your phone at home? Yeah, you know that feeling I´m talking about. Our mobile device these days are more than just a tool for communication, it has a lot of serious data and personal information, such as contacts, emails, photos, and passwords that can put our privacy at risk. A modern security feature like FaceID though prominent is not sufficient to safeguard our data. “For instance, Security researchers attending the annual Black Hat hacker convention in Las Vegas have managed to bypass the iPhone FaceID user authentication in just 120 seconds. These researchers were able to demonstrate that they could bypass the FaceID user authentication and access the iPhone of the victim in less than 120 seconds. To do so, they needed three things: a pair of spectacles, some tape, and a sleeping or unconscious iPhone user” [1].

II. Methods

Using Mediapipe, facial gesture recognition involves collecting a dataset of facial gesture images or videos, pre-processing the data by identifying and extracting facial landmarks, and extracting features for recognition. A machine learning model then is trained, its performance is evaluated, it is integrated into an authentication system, potential security risks have been considered, and user testing is done. The facial landmark detection and feature extraction method proposed by Mediapipe is effective and reliable. Key facial features are identified and extracted as part of the approach to produce relevant features for recognition. These characteristics are used to train a machine-learning model to differentiate between genuine and fake facial motions. The user is prompted to make a particular gesture, which the system compares to the trained model to confirm their identity. spoof-blocking methods and potential security theft.

III. Significance

When paired with facial recognition technology, facial gesture recognition is a promising technique that can offer additional benefits for unlocking mobile devices. Asking the user to make a specific facial gesture in addition to face recognition, adds an extra layer of security and can assist prevent unauthorized access to the device. Also, instead of inputting passcodes or utilizing fingerprint scanners, face movements can unlock a smartphone more quickly and conveniently. Facial gesture recognition can also increase accessibility for people who find entering a passcode or using a fingerprint scanner challenging. Last but not least, it can provide a pleasant and unique user experience by letting users select memorable or meaningful actions that increase a sense of ownership.

Proposal Outline

Facial Expression Analysis for User Authentication

Student: Ishwar Jadhav

Advisor: Dr. Tam Nguyen

I. Introduction and Problem Statement

Traditional authentication methods, such as passwords, PINs, or tokens, have several limitations, including the potential for theft, loss, or forgetfulness. Even having basic Facial recognition is not secure enough. In this experiment, researchers used a 3D mask (which costs just ~200 USD), made of stone powder, with glued 2D images of the eyes as you can see in Fig.1. The experts found out that stone powder can replace paper tape to trick FaceID AI at higher scores. The eyes are printed infrared images – the same technology that Face ID itself uses to detect the facial image. These materials and tools are casual for anyone to find.

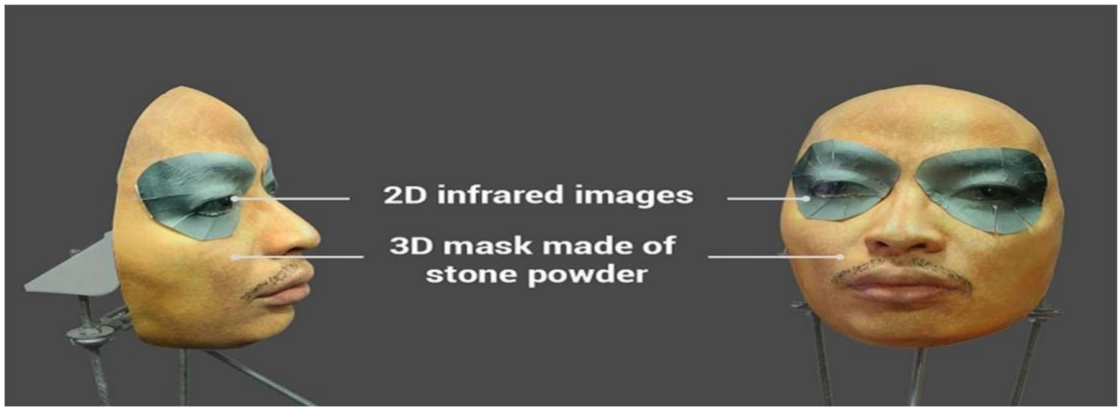


Fig.1. Illustration of 3D Face which looks like the user's face used to hack FaceID.

Facial gesture recognition, which involves analyzing and identifying specific facial expressions or movements, has emerged as a promising solution for user authentication. This method leverages the unique characteristics of the user's face, which are difficult to replicate, to provide secure and convenient authentication.

The goal of this problem statement is to design and implement a facial gesture recognition system that can accurately and efficiently authenticate users. The system should be able to identify the user based on specific facial expressions or movements, such as blinking, nodding, or smiling. The system should also be able to differentiate between the user's gestures and those of an imposter, such as a photograph or video of the user.

The key challenges in developing such a system include selecting appropriate facial features to analyze, designing effective algorithms to recognize these features and mitigating potential threats

such as spoofing attacks. The system should also be designed with consideration for user experience, such as ensuring that the recognition process is fast, easy to perform, and does not require specialized hardware.

The successful implementation of a facial gesture recognition system for user authentication has the potential to improve security and convenience in a variety of settings, including mobile devices, computer systems, and physical access control.

II. Review of Related Work and Significance of the Proposed Effort

Researchers, technology firms, and end users have all paid particular attention to the quickly developing subject of facial gesture detection. In comparison to more traditional approaches, using facial gestures for user authentication has several benefits, including enhanced security, practicality, and accessibility. Recent studies have used a variety of technologies and algorithms to examine the possibility of facial gesture recognition systems for user identification.

A recent example of such a technology is Mediapipe, an open-source framework designed by Google that provides several premeditated for real-time, cross-platform media processing. Mediapipe is the perfect platform for creating facial gesture recognition systems for user identification since it offers a robust set of facial analysis and recognition capabilities.

Several recent studies have explored the potential of Mediapipe for facial gesture recognition, demonstrating its ability to accurately recognize specific facial movements and expressions [2]. Another developed a Mediapipe-based system for detecting fake facial gestures and demonstrated its effectiveness in preventing spoofing attacks [3].

The proposed effort to develop a facial gesture recognition system for user authentication using Mediapipe is significant for several reasons. Firstly, it builds on previous research in this field and leverages the capabilities of Mediapipe to develop a robust and accurate facial gesture recognition system. Secondly, it has the potential to enhance security and convenience for users, providing a more secure and easy-to-use authentication method. Finally, the proposed effort can help to address some of the key challenges in developing facial gesture recognition systems, such as mitigating potential spoofing attacks and designing effective algorithms for gesture recognition.

In conclusion, the proposed effort to develop a facial gesture recognition system for user authentication using Mediapipe holds significant promise for improving security, convenience, and accessibility for end-users. It builds on existing research in this field and leverages the capabilities of Mediapipe to develop a powerful and accurate facial gesture recognition system. The successful implementation of this system could have broad applications across a range of industries and settings, including mobile devices, computer systems, and physical access control.

III. Objectives of the Proposed Project and Questions to be addressed.

Facial gesture recognition using MediaPipe Holistic is an important application of computer vision and machine learning that has numerous practical applications in areas such as human-computer interaction, biometrics, and healthcare. Facial gesture recognition aims to detect, track, and classify different facial gestures and expressions in real time using a camera and machine learning algorithms accurately and robustly.

The specific objectives of facial gesture recognition using MediaPipe Holistic may include:

1. Developing machine learning models that can accurately detect and track different facial landmarks and gestures in real-time, using the MediaPipe Holistic framework.
2. Implementing facial gesture recognition algorithms that can identify and classify different facial expressions, such as smiles, frowns, and raised eyebrows, with high accuracy.
3. Integrating facial gesture recognition into various applications, such as video conferencing software, gaming, and healthcare applications.
4. Improving the robustness and accuracy of facial gesture recognition algorithms through data augmentation, feature engineering, and other techniques.

Overall, the objective of facial gesture recognition using MediaPipe Holistic is to develop accurate, robust, and practical applications that can enhance human-computer interaction, facilitate biometric identification, and improve healthcare outcomes.

IV. Method(s) and Anticipated Results

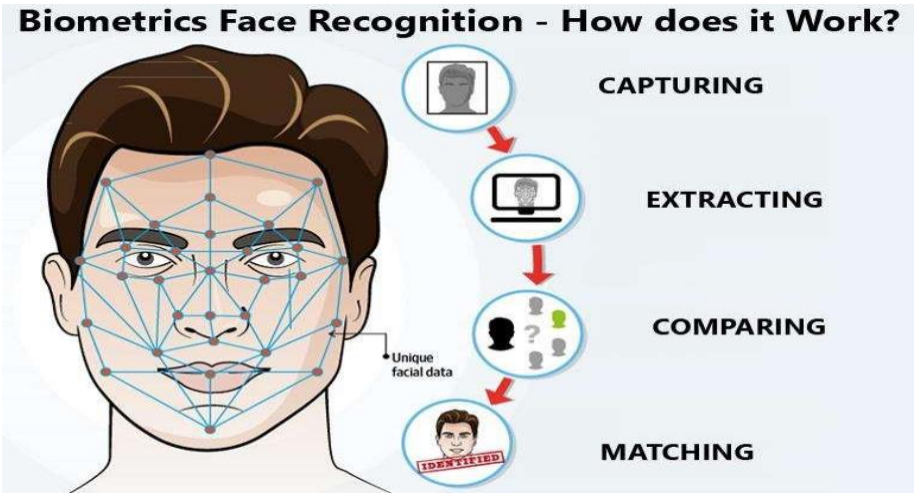


Fig.2. Flowchart for Regular Facial Recognition

1. Understanding how basic Face Recognition works.

Concerning Fig.2., Biometric face recognition is a technology that uses a combination of hardware and software to identify individuals by analyzing their facial features. The process involves capturing an image of a person's face using a digital camera or a video stream and

then analyzing the unique features of the face to create a digital template. The image is then processed using computer algorithms that detect key features such as the distance between the eyes, the nose's shape, and the face's contours. These features are then compared to a database of known faces to determine the identity of the person. Biometric face recognition systems typically use one of two methods for analyzing facial features: geometric or photometric. Geometric methods rely on the relative position and shape of facial features to create a template, while photometric methods use the reflectance and texture of the face to create a template.

2. How the working of facial gestures is different from basic Face Recognition.

We will collect a dataset available from various resources like Google search or Kaggle for evaluation purposes. The data will include images of various facial expressions and short videos of people making these gestures.

To begin with, we apply face detection on the given dataset of images to obtain the bounding boxes that enclose the detected faces. In case there are no faces or multiple faces detected, there is no further action needed. However, if only one face is detected, we proceed to determine the facial landmark points which include features like the nose, eyes, mouth, chin, etc. The landmark points help in estimating the position of the head, and subsequently, correcting the head position to a frontal pose. All this is done with the help of OpenCV [5].

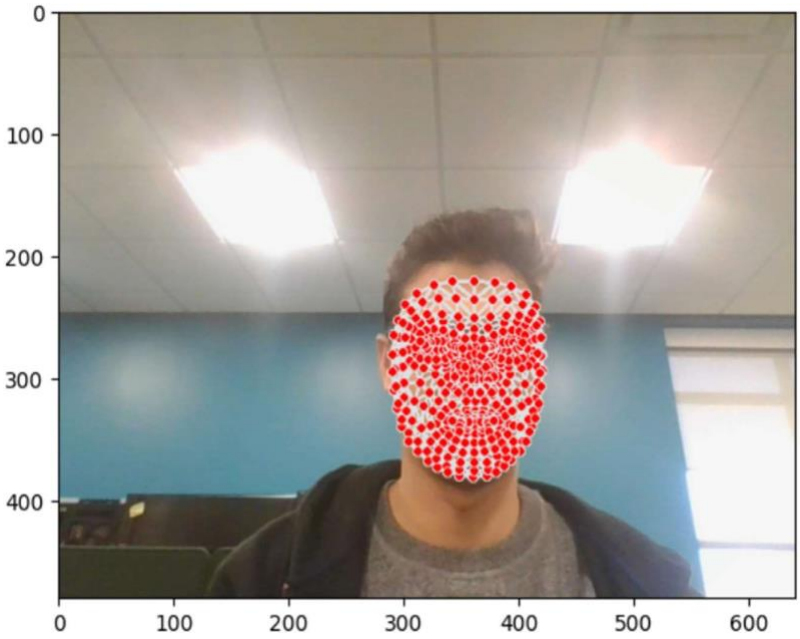
Facial gesture recognition can be used for user authentication, where a user's identity is verified based on their facial gestures. MediaPipe Holistic is a suitable framework for this task since it provides real-time facial landmark tracking and gesture classification capabilities.

The method for facial gesture recognition for user authentication using MediaPipe Holistic involves several steps. The first step is to collect a dataset of facial gesture videos from the users who need to be authenticated. Next, the videos are pre-processed by extracting the facial regions and landmarks and normalizing the frames to a standard size.

As you can see in Fig.3. the details were drawn between the eyes, nose, eyebrows, and mouth using drawing utils. These markings were drawn by understanding the starting node and ending node of each part. For e.g. An eyebrow can be marked from the left landmark point where it begins up to the right landmark point where it could end.

As we see in Fig.3., in the user enrolment step, I have recorded myself performing a set of specific facial gestures that will be used for authentication. These enrolled gestures are used to train a facial gesture recognition model using MediaPipe Holistic's pre-built facial landmark detection and tracking module, along with a classifier that can classify the facial gestures.

Fig.4. 468 Facial Landmarks being plotted.



Facial landmarks are an important component of face detection in MediaPipe Holistic. MediaPipe Holistic's facial landmark detection and tracking module uses a machine learning algorithm to detect and track 468 facial landmarks in real time. These landmarks correspond to key points on the face, such as the corners of the eyes and mouth, the tip of the nose, and the contour of the jawline.

The facial landmark detection and tracking module in MediaPipe Holistic is optimized for speed and accuracy, allowing it to perform well in real-world applications such as facial gesture recognition and face tracking. In addition, the landmarks can be used as input for other computer vision tasks such as facial expression recognition and gaze tracking.

Once the model is trained, the user authentication step involves comparing the user's real-time facial gestures with the enrolled gestures to verify their identity. By training a facial gesture recognition model using the enrolled user gestures, it is anticipated that the model will achieve high authentication accuracy, allowing only authorized users to access the system.

The anticipated results of using facial gesture recognition for user authentication using MediaPipe Holistic are high authentication accuracy and increased security. By training the facial gesture recognition model using MediaPipe Holistic's pre-built facial landmark detection and tracking module and a classifier that can classify the facial

gestures, the model can accurately recognize and authenticate users based on their real-time facial gestures.

The high accuracy of the facial gesture recognition model can lead to increased security, as only authorized users will be granted access to the system. This can prevent unauthorized users from accessing sensitive information or conducting fraudulent activities.

Moreover, the real-time performance of MediaPipe Holistic's facial gesture recognition makes it suitable for applications that require instant authentication, such as accessing secure systems and making financial transactions. The speed and accuracy of the facial gesture recognition model can enhance the user experience by reducing authentication time and providing a seamless authentication process.

In summary, the anticipated results of using facial gesture recognition for user authentication using MediaPipe Holistic include high authentication accuracy, increased security, and improved user experience.

V. References/Selected Bibliography

[1] D. Winder, “Apple’s iPhone FaceID Hacked In Less Than 120 Seconds,” Forbes.

[2] A. I. Siam, N. F. Soliman, A. D. Algarni, F. E. Abd El-Samie, and A. Sedik, “Deploying Machine Learning Techniques for Human Emotion Detection,” Computational Intelligence and Neuroscience, vol. 2022, p. e8032673, Feb. 2022

[3] S. Jia, S. Wang, C. Hu, P. J. Webster, and X. Li, “Detection of Genuine and Posed Facial Expressions of Emotion: Databases and Methods,” Frontiers in Psychology, vol. 11, Jan. 2021

[4] “Top new - Bkav Corporation,” Bkav.com, 2017.

[5] I. Culjak, D. Abram, T. Pribanic, H. Dzapo, and M. Cifrek, "A brief introduction to OpenCV," 2012 Proceedings of the 35th International Convention MIPRO, Opatija, Croatia, 2012, pp. 1725-1730.

[6] V. Bazarevsky, Y. Kartynnik, A. Vakunov, K. Raveendran, and M. Grundmann, “BlazeFace: Sub-millisecond Neural Face Detection on Mobile GPUs.” Accessed: Feb. 23, 2023.

VI. Anticipated Time Schedule

Tasks	May (Week 2, 4)		June (Week 1 - 4)				July (Week 1 - 4)				August (Week 1-2)	
Analysis												
Implementation												
Validation												
Testing												
Report, Publication											`	