International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Technology Behind Face Unlocking in Smartphones

Mr. Guru Moorthy S[1]*, Mr. Kavin Raaj S*[2]*, Miss. Akshayaa S*[3]*, Mr. Manoj B*[4]

[1,2,3,4]Sri Krishna Arts and Science College, Coimbatore

DOI: https://doi.org/10.55248/gengpi.2023.4.4.35678

ABSTRACT : -

Face unlocking technology in smartphones is a biometric authentication system that allows users to unlock their devices by scanning and verifying their facial features. This technology uses a combination of hardware and software components to provide a secure and convenient way to access a smartphone.

Keywords-face recognition; face detection; mobile phones

1.1 INTRODUCTION

Face unlocking technology in smartphones has become increasingly popular in recent years as a secure and convenient way to access your device. This technology utilizes various sensors and algorithms to create a unique facial profile that can be used to authenticate the user and unlock the device. The technology works by using a front- facing camera to capture an image of the user's face. This image is then analysed by software that identifies key features of the face, such as the distance between the eyes, the shape of the jawline, and the contours of the nose and mouth. These features are then used to create a unique facial profile that is stored on the device. When the user attempts to unlock their phone, the front-facing camera is activated and captures another image of their face. The software compares this image to the stored facial profile and, if there is a match, the device is unlocked.

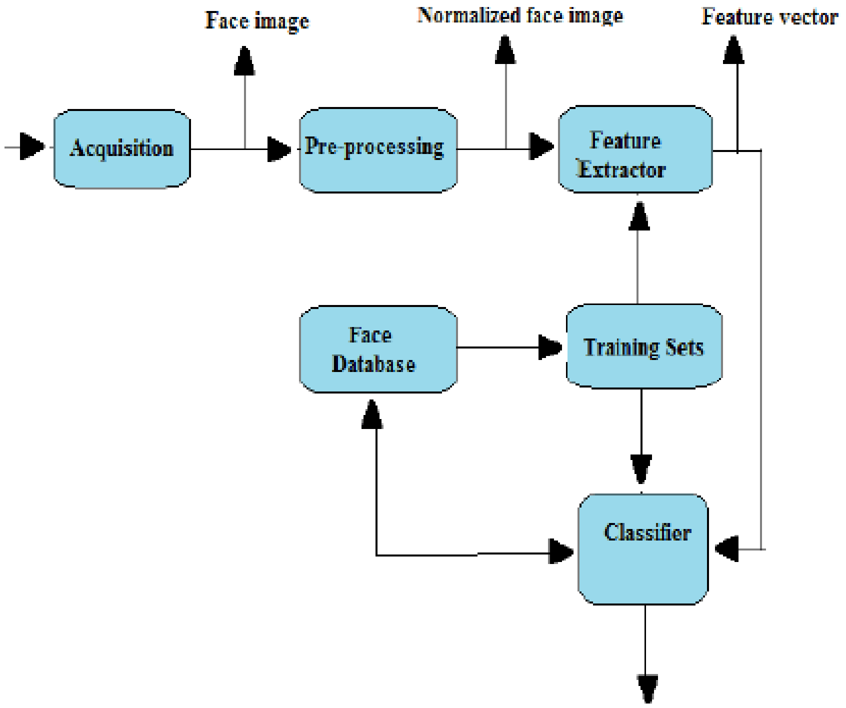
1.2 PRIOR AND RELATED WORK

There has been a significant amount of prior and related work on the technology behind face unlocking in smartphones, as it has become a popular feature in modern mobile devices. One of the earliest works in this area was by Viola and Jones (2001), who proposed the Viola-Jones algorithm for face detection using Haar-like features. This algorithm was later used as the basis for many face detection and recognition systems, including those used in smartphones. In 2006, the Eigenface method was introduced by Turk andPentland, which used principal component analysis (PCA) to represent faces as a set of eigenfaces. This method was later improved upon with the introduction of Fisher faces, which used Fisher linear discriminant analysis (LDA) to enhance the performance of face recognition. Since then, there have been numerous studies and advancements in the field of face recognition and detection, including the use of deep learning methods such as convolutional neural networks (CNNs). In particular, the Face Net system proposed by Schroff et al. (2015) used a CNN to learn a high-dimensional feature space where faces could be easily distinguished and recognized.

These advancements in face recognition technology have paved the way for the development of face unlocking in smartphones. Apple's Face ID, which uses a combination of infrared sensors and machine learning algorithms, was introduced in 2017 and has since become a standard feature in the iPhone line-up. Similarly, many Android phones have implemented their own facial recognition systems, such as Samsung's Intelligent Scan and Google's Face Match.Overall, the technology behind face unlocking in smartphones is a rapidly evolving field with a rich history of prior and related work. Researchers continue to develop new and innovative methods for face recognition and detection, which will likely lead to further improvements in smartphone security and usability.

1.3 ALGORITHM

The below block diagram depicts the major steps in the face recognition algorithm,



1.4 FACE DETECTION

Face detection is a technology that has been increasingly used in smartphones for features such as face unlocking. It involves the use of computer algorithms and machine learning to detect and recognize human faces in digital images and videos.

The following steps are typically used in face detection:

IMAGE ACQUISITION: The first step in face detection is to acquire an image or video feed that may contain a face. This can be done using a camera, webcam, or other imaging device.

PRE-PROCESSING: Once the image is acquired, pre- processing is performed to enhance the quality of the image and make it easier for the face detection algorithm to analyse. This can include operations such as noise reduction, colour normalization,andimageresizing.

FACE CANDIDATE GENERATION: The face detection algorithm then analyses the pre-processed image to identify areas that may contain a face. This is done using machine learning algorithms that have been trained to recognize specific patterns in images that are indicative of a face, such as the presence of two eyes, a nose, and a mouth in close proximity.

FEATURE EXTRACTION: Once potential face regions are identified, the face detection algorithm then extracts features from these regions. This feature may include colour, text, shape and information.

1.5 COLOR SEGMENTATION

Color segmentation is a technique used in computer vision and image processing to segment an image into regions based on the color or color distribution in the image. This technique is often used in the technology behindfaceunlockinginsmartphones.

Color segmentation is typically performed using color space transformations, which map the color values in an image from one color space to another. For example, an image in the RGB color space can be transformed into the HSL or HSV color space, which separates color information into hue, saturation, and value (or brightness) components. Once the image is transformed into a different color space, color segmentation algorithms can be applied to the image to segment it into regions based on color. One common approach is to use clustering algorithms such as K-means clustering or mean shift clustering to group similarcolors together. In the context of face unlocking in smartphones,

color segmentation can be used to identify the region of the image that contains the user's face. This is done by applying color segmentation to the image and identifying the region with the highest concentration of skin-tone colors. Once the region containing the user's face has been identified, more advanced techniques such as face detection and recognition can be applied to the image to unlock the phone. Color segmentation is a powerful technique that can be used in combination with other techniques to achieve accurate and reliable face unlocking insmartphones.

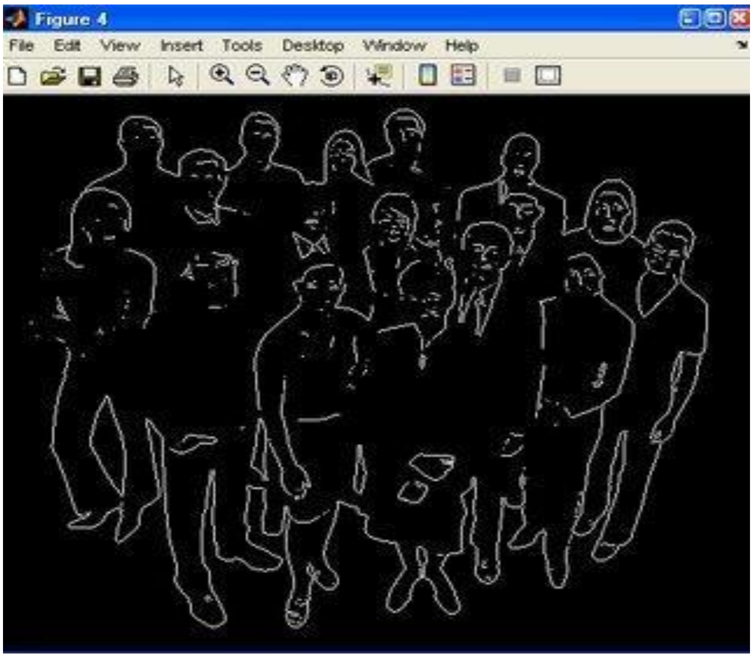


Figure : Example of bad performance for the Hue classifier If the Hue classifier is showing poor performance, there are several potential reasons for this. Some of the common reasons include:

LIMITED TRAINING DATA: The classifier may not have been trained on a sufficient amount of data, or the training data may not be diverse enough to capture the variability in skin tones across different individuals. This can result in poor performance on test data, as the classifier may not be able to generalize well to new and unseen images.

POOR FEATURE SELECTION: The features used by the classifier to distinguish between different skin tones may not be well-suited to the task. For example, if the classifier is only using the Hue component of the image, it may not be able to capture the full range of color information that is important for distinguishing between different skin tones.

LIGHTNING CONDITION: The performance of the Hue classifier may be affected by variations in lighting conditions. For example, if the lighting conditions in the test images are significantly different from those in the training data, the classifier may not be able to generalize well.

IMAGE QUALITY: The quality of the test images may be poor, which can affect the performance of the classifier. For example, if the images are blurry or have low contrast, the classifier may have difficulty distinguishing between different skin tones.

To improve the performance of the Hue classifier, it may be necessary to address one or more of these issues. This could involve collecting more diverse training data, selecting more effective features, or developing techniques.

2.1 TEMPLATE MATCHING

Template matching is a technique used in image processing and computer vision to match a given template image to a larger image. In the context of face unlocking in smartphones, template matching can be used to match a stored template of the user's face to a live image captured by the phone's camera. Template matching involves sliding the template image over the larger image and computing a similarity score at each position. The similarity score measures how well the template matches the image at that position, and is typically based on a comparison of pixel values or image features.

One common approach to template matching is to use normalized cross-correlation, which measures the similarity between two images by computing the correlation coefficient between their pixel values. The template is moved across the image, and the normalized cross-correlation is computed at each position. The position with the highest correlation value is considered the best match. In the context of face unlocking in smartphones, the stored template of the user's face can be used as the template image, and the live image captured by the camera can be used as the larger image. Template matching can then be used to find the position in the live image that best matches the stored template.

However, template matching has some limitations. One of the main limitations is that it is sensitive to variations in scale, orientation, and lighting conditions.

- PGM
- SFI
- NRM

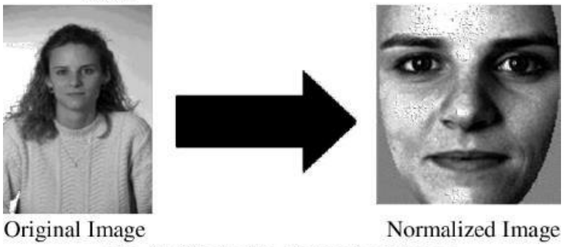


Fig. 4: Original to Normalized image

Figure : sample output for template matching

2.2 ALTERNATE APPROACH

There are several alternate approaches to face unlocking in smartphones that can be used in addition to or instead of the techniques mentioned previously. Some of these approaches include:

3D FACE RECOGNITION: Instead of using 2D images, 3D face recognition techniques capture depth information from the user's face using technologies such as structured light or Time-of-Flight (ToF) sensors. This can improve the accuracy and robustness of the face unlocking system, as 3D data is less sensitive to variations in lighting conditions and is more resistant to spoofing attacks.

INFRARED FACE RECOGNITION: Infrared cameras can capture the heat signature of a user's face, which can be used to distinguish between real faces and fake ones. This approach is also more resistant to variations in lighting conditions and can be used in combination with other techniquessuchas3D facerecognition.

DEEP LEARNING: Deep learning techniques such as convolutional neural networks (CNNs) can be used to extract features from images of a user's face, which can be used to identify the user. Deep learning approaches can be more accurate and robust than traditional techniques, as they are able to learn complex patterns and relationships in thedata.

MULTI-FACTOR AUTHENTICATION: Multi-factorauthentication involves using more than one type of authentication method to unlock the phone. For example, a user may need to provide both a facial scan and a fingerprint scan to unlock the phone. This can improve the security and reliability of the face unlocking system, as it is less vulnerabletospoofingattacks.

LIVENESS DETECTION: Liveness detection involves verifying that the user is a real person and not a fake or spoofed image. This can be done by requiring the user to perform a specific action, such as blinking or smiling, or by using techniques such as texture analysis or depth estimation to distinguish between real faces and fake ones.

In conclusion, while the techniques mentioned previously such as color segmentation and template matching are widely used in face unlocking in smartphones.

2.3 TRAINING SET AND TEST SET

In machine learning and computer vision, it is common to split a dataset into a training set and a test set. This is done to evaluate the performance of a model on new, unseen data and to prevent overfitting, which occurs when a model memorizes the training data and performspoorlyonnewdata. In the context of face unlocking in smartphones, the training set would consist of a set of images of the user's face, which would be used to train a machine learning model to recognize the user's face. The test set would consist of a separate set of images of the user's face, which would be used to evaluate the performance of the model.

The training set is used to optimize the parameters of the machine learning model using a process called training. During training, the model is presented with a set of input images along with their corresponding labels (i.e. whether the image is of the user's face or not), and the model adjusts its parameters to minimize the difference between its predictions and the true labels. Once the model is trained, it is evaluated on the test set to see how well it performs on new, unseen data. This is done by presenting the model with a set of input images from the test set and comparing its predictions to the true labels. The performance of the model is typically measured using metrics such as accuracy, precision, and recall..

Figure : training set of images(5 images per person)

3.1 EIGENFACES

Eigenfaces is a popular approach for face recognition that was first introduced in the late 1980s. It is a technique that uses Principal Component Analysis (PCA) to extract features from images of faces and represent them as a set of "eigenfaces". These eigenfaces can then be used to recognize faces by comparing them to a database of known faces.

The process of generating eigenfaces involves the followingsteps:

Collect a set of images of faces. These images are typically grayscale and normalized to a standard size. Apply PCA to the set of images to extract the principal components. These principal components are the eigenvectors of the covariance matrix of the set of images; The first few eigenvectors (typically around 100) are selected and arranged into eigenfaces. Each eigenface is a grayscale image that represents a particular facial feature; To recognize a new face, the input image is projected onto the space defined by the eigenfaces. This results in a set of weights that represent the contribution of each eigenface to the input image; The weights are then compared to those of known faces in a database using a distance metric, such as Euclidean distance or MahalaNobis distance. The closest match is considered to be the identity of the input face

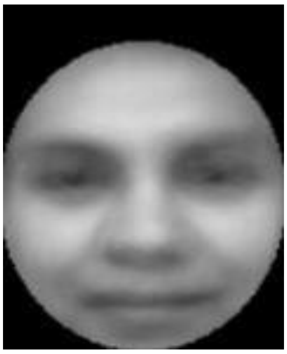


Figure : average face of the training set

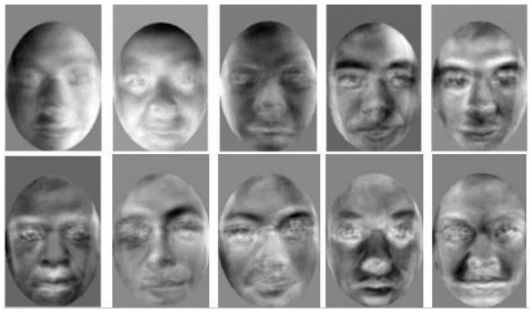


Figure : the first ten eigenfaces

3.2 FISHERFACES

Fisher faces is a technique used in the field of face recognition and is often used in the technology behind face unlocking in smartphones. This technique is based on the Fisher linear discriminant analysis (FLDA), which is a statistical method used to find a linear combination of features that maximizes the separationbetweendifferentclasses. In the case of face recognition, Fisher faces are a set of features extracted from a facial image that are most relevantfordistinguishingbetweendifferent individuals. These features are obtained by projecting the original image onto a lower-dimensional subspace that captures the most significant variations in the data. The Fisherfaces approach has several advantagesoverothermethods usedforface recognition, such as principal component analysis (PCA). One of the main advantages is that Fisher faces can effectively handle non-linear variations in the data, such as changes in facial expression, lighting, and pose. In the context of face unlocking in smartphones, Fisher faces are typically used as a part of a larger system that involves capturing an image of the user's face using the smartphone's camera and then processing that image to extract the relevant facial features. These features are then compared to a pre-existing database of facial features stored on the device to verify the user's identity.

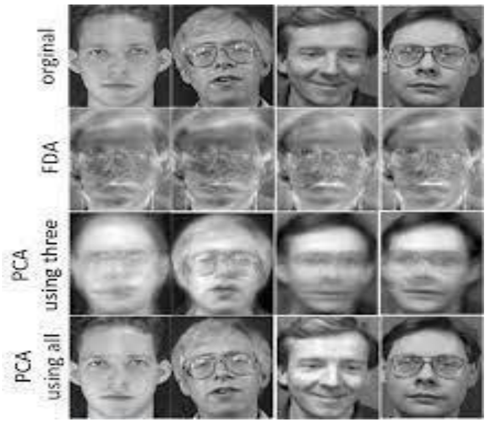
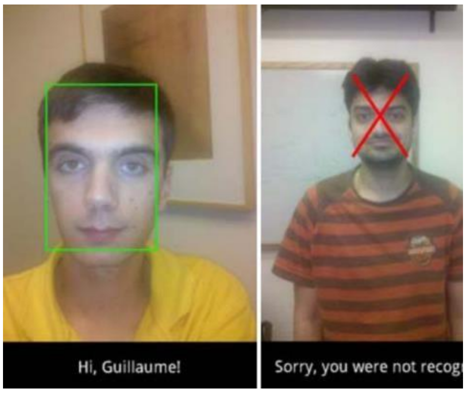


Figure : fisher faces

3.3 IMPLEMENTATION ON DROID

Face unlocking in smartphones has become a common feature, and many Android devices use the technology behind Fisher faces to implement this feature. Android devices typically use a combination of hardware and software components to enable face unlocking. The hardware component of the face unlocking system is typically a camera sensor that captures an image of the user's face. The software component of the system includes algorithms that process the image and extract the relevant facial features. The implementation of Fisher faces on Android devices typically involves the use of machine learning algorithms that are trained on a large dataset of facial images. The algorithm learns to recognize patterns in the data and identifies the most relevant features for distinguishing between different individuals. Once the algorithm has been trained, it can be used to extract the relevant facial features from an image of the user's face. These features are then compared to a pre-existing database of facial features stored on the device to verify the user's identity. One of the challenges of implementing Fisher faces on Android devices is the need to balance accuracy with performance. Face unlocking systems need to be fast and responsive to provide a seamless user experience. This requires careful optimization of the algorithms to ensure that they can perform the necessary computations quickly and efficiently.


Hi, Guillaume!

Sorry, you were not recog

Figure : result of the face recognition application for android

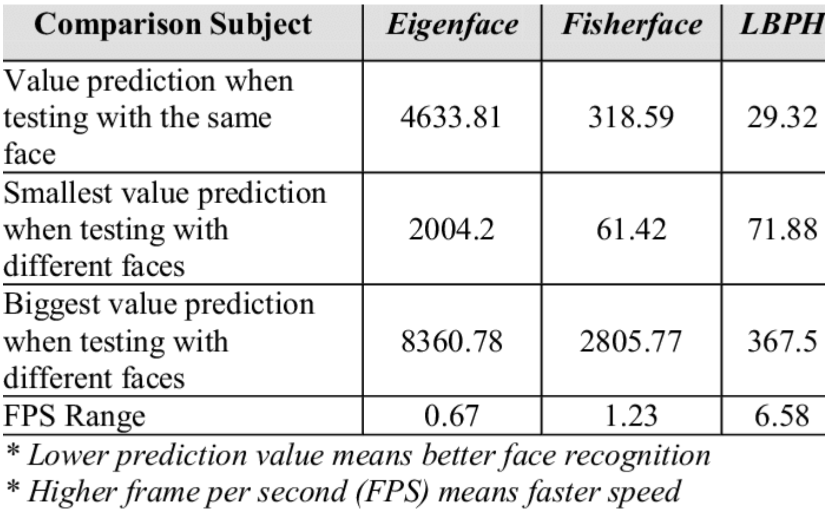
RESULT

False rejection if the face is associated with the correct face, but the distance is larger than threshold.

False acceptance if the face is associated with the wrong face, but the distance is lower than threshold.

Correct rejection if the face is associated with the wrong face, and the distance is larger than threshold.

Correct acceptance if the face is associated with the correct face, and the distance is lower than threshold.



Comparison Subject	*Eigenface*	*Fisherface*	*LBPH*
Value prediction when testing with the same face	4633.81	318.59	29.32
Smallest value prediction when testing with different faces	2004.2	61.42	71.88
Biggest value prediction when testing with different faces	8360.78	2805.77	367.5
FPS Range	0.67	1.23	6.58

** Lower prediction value means better face recognition*
** Higher frame per second (FPS) means faster speed*

Figure : difference table of eigenface and fisher face

4.2 CONCLUSION

In conclusion, the technology behind face unlocking in smartphones has come a long way in recent years, with the implementation of Fisher faces being a major advancement in the field of face recognition. Fisher faces provide a powerful tool for identifying relevant features in facial images and are particularly effective at handling non-linear variations in the data. The implementation of Fisher faces on Android devices method for users to access their devices, and the technology behind it is constantly evolving to improve accuracy and reliability.

However, there are still some challenges to be addressed, such as improving performance in low-light conditions and addressing potential privacy concerns associated with facial recognition technology. As the technology behind face unlocking continues to advance, it is likely that we will see more widespread adoption of the feature in smartphones and other devices..

4.3 REFERENCE

[1]. Joseph Lewis, University of Maryland, Bowie State University, January 2002,Biometrics for secure Identity Verification: Trends and Developments.

[2]. Biometric Recognition2003 ,Security and Privacy Concerns.

[3]. KresimirDelac ,MislavGrgic 2004 ,a survey of biometric recognition methods.

[4]. sulochanasonkamble, 2dr. ravindrathool, 3balwant sonkamble 2010, survey of biometric recognition systems and their applications, journal of theoretical and applied information technology.

[5]. Anil K. Jain, Ajay2010Kumar,"Biometrics of Next Generation: An Overvie

[6]. ShibnathMukherjee,Zhiyuan Chen 2006, A Secure Face Recognition System for Mobile-devices without The Need of Decryption.

[7]. Shang-Hung Lin, Ph.D. 2002,An Introduction to Face Recognition Technology.

[8]. Wei-Lun Chao 2010, Face Recognition.

[9]. M. Turk, and A. Pentland, Eigenfaces for Face Recognition, Journal of Cognitive Neuroscience, vol. 3 num.1 (1991) 71-86.

[10]. Laboratoire, Equipe2000 ,Fuzzy Logic Introduction.

[11]. J. Mendel.1995 Fuzzy logic systems for engineering: a tutorial. Proceedings of the IEEE, 83(3):345{37