National College of Ireland

Combination of Face recognition and Handprint Biometrics with Fingerprint Image Encryption Using Multiple QR Decomposition

MSc Research Practicum part 2
MSc in Cybersecuirty

Rishan Backer
Student ID: 22235949

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rishan Backer
Student ID:	22235949
Programme:	MSc in Cybersecuirty **Year:** 2023/24
Module:	MSc Research Practicum part 2
Supervisor:	Mark Monaghan
Submission Due Date:	12/Aug/2024 2:00 P.M
Project Title:	Combination of Face recognition and Handprint Biometrics with Fingerprint Image Encryption Using Multiple QR Decomposition
Word Count: 8206	**Page Count**: 21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rishan Backer

Date: 12/Aug/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Combination of Face recognition and Handprint Biometrics with Fingerprint Image Encryption Using Multiple QR Decomposition

Rishan Backer
22235949

Abstract

In this project the different types of biometric traits are combined together by different methods and the encryption of fingerprint is also considered with the help of multiple QR decomposition method in order to enhance the security of the system. The major biometric traits are considered as palmprint biometric, fingerprint biometric and facial biometric. The different biometric traits are considered here because thus this can enhance the stability of biometric authentication. If we consider any single biometric trait for authentication, there is a high chance of failure of system in the future when the physical biometric trait of any person has any newly developed minor differences such as marks or cuts or nay physically damaged signs can also void the system's authorization capability, thus in order to overcome this, the combination of biometrics are very important, this ensure the person was right even when the person was physically right person. But when considering any single biometric trait, the system will be wrong even though the person was physically right.

There are different biometric traits are available widely according to a human body, these biometric traits has its own advantages and disadvantages, here we are going to consider the biometric traits of the person such as palm print biometric, fingerprint biometric and face biometric trait. These biometrics are considered here because these can fit very well to my project, such as when considering the palm print biometric the unique characteristics of palm print are very different and has strong security unique features when compared to other biometric traits that are widely available, the area of features that is for palm print are larger when compared to other traits, this is the major reason for considering the palm biometric trait as an important trait here. Same character applied for fingerprint, the security features are high for fingerprint biometric when compared to any other biometric traits, the fingerprint biometrics are widely accepted. Finaly, the face biometric has large biometric security features, which is considered as the strong biometric security authorization system here, because when the scanning technologies are capable enough to identify the person, the authorization will be strong and secure. This project excluded other biometric traits for example iris biometric, vein biometrics due to much more complex and time-consuming process and also the final efficiency will be very less as compared to the three biometric traits that we are considered here.

This project uses different types of tools and algorithms in order to achieve the result, the major tools and algorithm such as for adjusting contrast and equalization of captured biometric images, such as CLAHE, other tools such as for extracting the Region Of Interest. The function such as Softmax function is used for the calculation of similarities for each biometric trait are considered here. Finally, the algorithm such as Score Level fusion algorithm which is used to combine these identified biometric traits together in order to identify the person for authorization.

Through this tool the project aims to be successful project with more efficient way of authorization using these strong biometric traits with unique features, the achievability of these project is almost 100 % due to the unique biometric traits and these powerful algorithms and tools.

The project aims to capture different biometric traits without physically touching the scanner, that is one of the major advantages of this project because of contactless reading system can enhance the overall security and maintain the health of the human.

Thus, biometrics are initially gone for image acquisition process for capturing the biometrics and then the pre-processing are done for fine tuning and enhancing the quality of the image. Then, the next step is for the feature extraction process where the biometric unique features are extracted here. Finaly, as the final step of authorization, these are then gone to similarity calculation and final evaluation process, where the authorization process is done and the identification of the real person with the help of these biometric traits are done here in this process. Finally, here we are doing the multiple QR decomposition method that is iterative matrix method in order to encrypt the fingerprint data to provide more security to the sensitive biometric data that are captured.

According to this, the final decision can be made by the authorization of the person's different biometric traits and finding similarities and combining these biometric traits helps to identify the exact real person even though if there is any physical cuts or marks are present the system will not void its authorization and identification process, because the identification process is made by score level fusion method and thus a threshold score is set to identify the person as the result. It is found out that this method is more successful and secured method because it is also helps to encrypt the sensitive fingerprint data that are collected using multiple QR decomposition method.

1. Introduction

The biometric recognition system are the unique features of a human body, in which unique different traits are extracted for different authorization purpose. The authorization includes many different types of things in order to access for security purpose, from our hand held smartphone to high security airport to military authorization are done with the help of biometric authentication system.

There are different types of biometric traits such as fingerprint, face recognition, palmprint, finger knuckles, iris biometric, hand and vein biometric, vocal biometric, DNA matching, behavioral biometric and much more in order to authorize using biological characteristic. These biometrics are designed for security, fraud prevention and gaining the access. [33] Each biometric traits are used for different purposes and each has its own unique characteristics. The security, authorization capabilities, reliabilities and collectability are different for each biometric system.

Fingerprint, hand biometric and iris biometric are the common methods of authorization in the case of biometric system, but there are other several complicated biometric system too such as DNA matching. There are many methods which are used in biometric system such as machine learning algorithms in order to extract the region of interest, feature extraction and much more.

The common biometric system for fingerprint scanning and fingerprint data protection are FIDO2 authentication system, in this system the authentication works based on public key cryptography. Here the system generates a public key when a user tries to attempt the authorization, the private key remains stored and the public key is shared. The protocols used here is WebAuthn and CTAP2, this provides phishing proof, fast authorization. But the

problem is which only accepts fingerprint scanning for biometric authorization commonly. [34]

Thus here the multiple biometric authentication system can provide more reliable security of authorization, which helps to more secure way of authorization process, thus here the combination of fingerprint, palmprint and face biometric trait are used for authorization process, in order to secure the biometric data that are given to the system, here we are using the QR decomposition method and for more security we are decomposing this QR technique into multiple times numerically by decomposition, thus provide more reliable and secure data that will store.

The current studies shows different biometric traits and its reliability but according to the simplicity, security and collectability, the fingerprint face recognition and palmprint biometric traits are easy to collect and can be combined with different machine learning algorithm in order to achieve the maximum security and reliability of biometric authorization. Most of research showing the difficulty in biometric collectability and accuracy of performance but while comparing these three traits, its almost reliable and accurate in every manner.

In this paper it is understand that the novelty can be filled by combining these biometric traits by giving the encryption technique with multiple QR decomposition method. Thus these multiple QR decomposition methos can increase the maximum security not only for the authorization but also for biometric stored data.

2. Review of Literature

The major aspect of this project is to develop a secured biometric system in order to provide maximum security during the access of information. The research papers contains biometric combination, thus here we are going to take the necessary biometric traits according to our security needs.

Different types of biometric traits recognized are considered as facial recognition, fingerprints, finger biometrics, palm biometric, knuckle biometrics, iris biometric, vein recognition, retina and voice recognition, DNA matching, digital signatures, behavioural identification and much more. Each traits has its own benefits and drawbacks as its comes to real life security. [26]

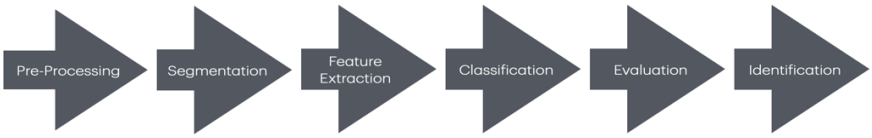

Figure 1: The process of biometric system) [26]

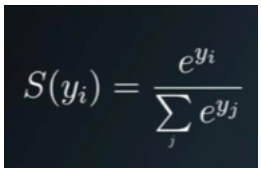

Figure 2: Softmax function [26]

- S stands for softmax function
- yi is the input vector
- e^yi is the exponential function for the input vector
- yj is the output vector
- e^yj is the exponential function for the output vector

According to the paper Mouad et al. the fingerprint biometric system consists of different stages such as enrolment, identification and verification of fingerprint data in order to recognize and authorize. The fingerprint consists of minutiae.
While concluding this paper they shows every features of fingerprint from fingerprint data collection to preprocessing, data acquisition and the identification of fingerprint.
The finger prints are different for each individuals, but if any structural damage occurs the fingerprint biometric systems can fail to detect even though the person was right. [27]
The paper Nikhil Maurya et al. consists of multiple biometric system such as the recognition based on palmprint, finger knuckles and nails, for the process of combination of biometric system here they are using certain tools and algorithm in order to provide the authorization and verification. Here the tool such as CLAHE which stands for Contrast Limited Adaptive Histogram Equalization for pre-processing the image of the biometric traits. The deep learning method DenseNet 201 are used here for the feature extraction method. The ROI, Region of Interest is calculated using Softmax function, that is the identification process, if the function identifies as binary 1, then the process of identification is true for authorization and if the detection is false, then the authorization detects as zero.
This paper concluded as palm print has more dense information while compared to other finger print traits and the fingernails provides least information in the case of biometric authorization.
The usage of other biometric traits can be usefull which can strengthen the biometric secuirty such as facial recognition or iris scanning. [31]
Thus here we are going to use this method for our biometric recognition, but we are taking the different biometric traits. According to Shuyi et al. each biometric system has its own functionalities and benefits. Here we are not going to take all the biometric traits due to complication of implementation. Thus we are going to take the important biometric traits with best functionality. The hand biometric traits such as finger knuckles, palm print and finger nails as considered as great universality, great uniqueness and great collectability, these traits has good security, these traits has also the best permanence and time consumption. In this paper they combined these biometric traits with best algorithms such as sensor level fusion, feature level fusion, Score level fusion, rank level fusion and decision level fusion. From these we are taking the score level fusion, in this algorithmic method the iteration like method is used to determine the output by using the matching score of each biometric traits, the highest score is considered here, this algorithm is very reliable and secure with less time consuming.
The major fusion algorithm and its functions in this paper are,

- Score level fusion: Similar matching scores of each biometrics are considered such as mean score. This algorithm has an accuracy of 98-100%
- Sensor Level Fusion: In this image from the sensors are considered here. The accuracy of sensor level fusion relies between 90 to 98%
- Feature-level Fusion: The features extracted from different biometric traits are considered here. The accuracy are considered here as 99%
- Rank-Level fusion: The highest ranked algorithm are considered here, such as borda count. The rank level fusion method has an accuracy level of 89-100%.
- Decision-Level fusion: The mathematical calculation methods are used here, such as AND, SUM, OR. The decision level fusion has an accuracy level of 89-100%.

They concluded as there are several challenges faced according to hand based biometric system such as difficulty in developing the hand print datasets, difficulty in adaptability methods in different scenarios, challenges faced due to incomplete data. [28]

Here in this paper the usage of multiple fusion algorithm can be reduced, this helps to reduce the complexity of the system.
The paper of Bayan Alharbi et al. has the method of different extraction tools for biometric traits, here they are using the combination of voice and face. The voice extraction is done here using the GMM (Gaussian Mixture Model) and the extraction of face data using FaceNet tool, these tools are best in considering the accuracy and reliability of the system.
They concluded as it when it obtained the result the Equal Error Rate decreased in the case of facial recognition system, the FaceNet plays a major role in providing the accuracy of the result, it is claimed that the accuracy of the result is 99.6%. But the voice recognition is not performed as expected, which provides least Equal Error Rate as compared to facial recognition system.

From this system it is understood that the combination of facial and hand recognition data plays a major role in biometric system rather than taking voice recognition as biometric. Here we are going to take the tool FaceNet for the extraction of our face biometric data. [29]
The security of fingerprint data are important, Isha Mehra et al. wrote a paper named Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition, through this paper we are taking the security for fingerprint data, in this paper they are using QR decomposition method in order to satisfy the security needs. According to this paper they are using optical asymmetrical cryptographic method secure data using encryption technique. In this paper the first method is the Gerchberg-Saxton phase retrieval algorithm method, then they utilize the Ortho triangular decomposition (QR decomposition) method for the process of encryption. Here for the decryption they are using the asymmetrical key. This is one of the best paper providing the security to fingerprint image data. While concluding this paper includes a high level of security with less memory and space usage.[30]
The equation for QR decomposition used in this paper are shown below,

- $M \times P = Q \times R$

Here,

- M is the matrix
- P is appropriate permutation matrix
- R is the upper triangular matrix

For complex decomposition matrix, the equation for orthogonal matrix Q,

- $Q \times Q^T = I$

Here, the equation represents transpose and transpose conjugate of Q matrix. Here P inverse will be the cypher text and Q x R will be asymmetric key.
After carefully analyses this paper can include multiple iteration method such as utilizing multiple QR decomposition method can increase the overall security and which helps to increase the overall fingerprint data in a secure way.
From the paper of Muhammad Rafiq Abuturab et al. introduced a multicolour image encryption using QR decomposition, in this paper they proposed a very reliable system with high security of QR decomposition, he proved the reliability of the security of the system with image exploit method. Here they are using different security keys, the decryption method is satisfied by four different keys. Thus which ensure the security of the system, the exploit methos is used to attack the encryption system, thus which confirms the security. Here the encrypted image data are the iris image data, thus from the conclusion of this system it is

clear that the numerical simulation results provides high security and feasibility of this system. [32]

3. Research Methodology

The project includes different methods with the help of research papers, the biometric digital images of different traits are taken here, such as hand biometric and face biometric. In the case of hand biometric, the fingerprint biometric and palm print biometric traits are considered here. These biometric traits are scanned using digital capable cameras, thus which helps the authentication without the need of physical touch. There are several algorithms and tools used in the case of this project, the major tools used here are,

1. CLAHE
2. DenseNet201
3. ImageNet
4. Softmax Function
5. Score Level Fusion Algorithm

According to this project the project contains five different parts, they are shown in below figure,

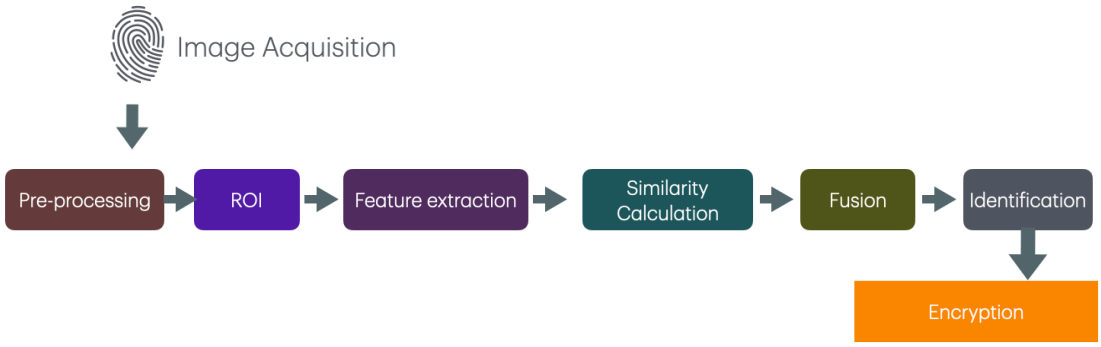

Figure 3: Showing the different types of methods used

3.1 Image Acquisition Process

The image Acquisition process is the method of collecting biometric data, here we are using digital image of biometric traits,

1. Fingerprint: For fingerprint we are using the camera in order to capture digital images by contactless system.
2. Palmprint: In the case of palm print we are using the same method of capturing images of palms using the same digital camera.
3. Face biometric: The different face images are captured with the help of camera for the image acquisition process.

All these biometric traits captured for acquisition through contactless and without any physical touch.

3.2 Pre-processing (CLAHE Algorithm)

The preprocessing includes the preprocessing of image, this is done by a special tool called CLAHE (Contrast Limited Adaptive Histogram Equalization), this method can equalize the contrast and histogram of the image thus to enhance the fingerprint, palm and facial data. The CLAHE is just an updated version of AHE (Adaptive Histogram Equalization), in this

method the the removal of halo effect in the image by enhancing the contrast of the image but limited over enhancement, the limiting is done by clipping with pre-defined values, this is usually called clip limits.

In the case of CLAHE image enhancement, the image is split into small regions and then the histogram is calculated and set to each tile of the image, then the clipped image is equalized, resulting an equalized image, then finally, the CLAHE contrasting method is used to adjust the enhanced but not over enhanced contrastive image to produce the final result. [1]

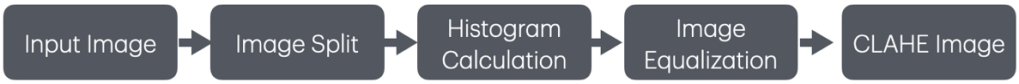

Figure 4: CLAHE Algorithm

Thus, the CLAHE algorithm is used for the set of biometric data that are taken after image acquisition process, the same applied

Fingerprint: For fingerprint the CLAHE method is applied with certain values such as "3" for the clip limiting function in the case of CLAHE clip limit and tile grid value is 8x8 pixel.

Palmprint: In the case of palm print, the CLAHE method is used to calculate the histogram and then done the enhanced image and finally, the clip limit is set as same 3 and pixel of tile is 8x8.

Face Biometric: In the case of face biometric the image histogram is calculated with a histogram interval of 100 bins,in order to get the enhanced visual clarity. Thus the histogram will show pixel values between them, then the image is converted to 2D image and converted to equalized image. Then the CLAHE is calculated with a clip limit of '3' and tile pixel of 8x8. [1][2]

3.3 ROI (Region of Interest)

ROI stands for Region of Interest, in this method certain contours are taken in order to identify the specific features of each biometric traits, because each biometric traits of each individual are unique and different, thus taking those unique area is important in the case biometric system. Thu here we are using unique feature bounded inside an area with the help of contours. Here we are using the contour in order to establish the area of interest, here we are using the contour threshold with specific values.

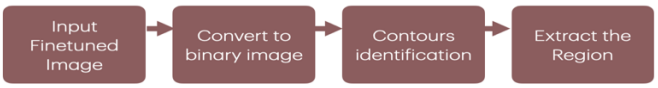

Figure 5: (Shows the ROI for fingerprint and palmprint)

Fingerprint: For fingerprint biometric we are using certain threshold value in order to achieve the contours around the area of interest, the threshold value for fingerprint here we are used as 250.[3][4]

Palmprint: In the case of palm print the exact boundaries are defined, the width of the boundaries, size and much more, the pixel here is set as 200x200, and the region of axis is also calculated for palmprint [5]

Figure 6: Shows the ROI for the face biometric

Face biometric: In the case of face biometric, the region of interest is calculated by using the Dlib function with calculating the vertical and horizontal coordinates for the region of interest and also by calculating the size, width and height of the detected image if we need the exact coordinates of the detected image [6]

3.4 Feature Extraction

In the case of feature extraction, the features are extracted from the region of interest using the specific algorithm called Densenet201. The Densenet201 can be very useful which is efficient in the case of feature extraction.

The DenseNet 201 is a model from the TensorFlow module, the DenseNet201 stands for Dense Convolution Network, which connects every layer to subsequent layer, there are several advantages in DenseNet201 such as which is subsequently reduce the number of parameters, the feature reuse encouragement [8][7]

Fingerprint: In the case of fingerprint the region of extracted image is resized into 224x224 pixel, then the densenet201 module imported with finetune function such as 'imagenet' with size and RGB, then with the data given the densenet201 predicts the feature to be extracted, after the feature is extracted this extracted feature is saved to our local disk with an extension of npy.

Palmprint: In the case of palmprint we are using the same configuration as in the fingerprint, with a pixel density of 224x224 with convert greyscale image to RGB image, also with the fine tuning using the Imagenet function. Finally, the prediction of the feature using the densenet201 with the ROI processed image.

Face biometric: In the case of facial extraction, the image is resized in to 224x224 pixel, then the image is converted to RGB from grey scale, then with the help of imagenet function we fine tune the image and the prediction of feature using densenet201 is took, then the feature vector shape is printed finally with a result of 1 vector and 1920 features, finally, the file is saved to our local disc.

Figure 7: Showing the feature extraction using DenseNet201

3.5 Similarity Calculation

In the case of similarity calculation here we are using the SoftMax function, in order to identify the exact output of the similarity and the stability to numerical functions are better. Here we are taking the extracted features of different biometric traits, we have a set of biometric traits for fingerprint, palmprint and face biometric, we are applying the SoftMax function to each biometric, the first step is to normalize the features, which improves the quality of similarity calculated from the extracted features of different biometrics. Then here the next step we are going to do is the feature reshape, that is converting the feature in to two dimensional in order to improve the speed of the machine learning, we are here applying the -1 function in order to gain the automated reshaping function, then we apply this reshape to every biometric extracted features.[10]

Finaly, we need to calculate the similarity of each feature set, for this we are taking the similarity calculation function, the cosine similarity calculations are done here, the feature

sets are already converted to two-dimensional image. Here the image classification of each biometric traits are done by softmax function, along with that, we need calculate the similarity for the biometric set and then we need to calculate the similarity score for each set after the similarity calculation, the similarity score is usually calculated with the similarity of cosine function and then calculate the average mean similarity of different biometric traits[9]

$$f(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{N} e^{x_j}} (i = 1, 2, \ldots, N),$$

Figure 8: Showing the mathematical equation for Similarity calculation

Here, the i and j denotes the input value for each set, the f(xi) is the output value.

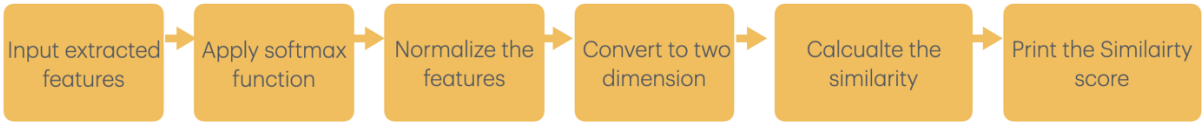

Figure 9: Shows the similarity score calculation using SoftMax function

3.6 Fusion (Score level fusion method)

In this method we are now combining the similarity score of each biometric traits in order to find out which person's biometric traits is defined here. After the similarity calculation we apply the algorithm of Score level fusion method in order to attain the maximum output of each biometric combination. Each biometric combination has a similarity value, thus with the help of threshold value that is specifically set to the combination value, thus the threshold value defines the person was right or wrong. Here the threshold value is set as 0.9. The combination of similarity between palmprint, fingerprint and faceial biometric similarity values are taken here for the combination method.[13]

Figure 10: Shows the score level fusion method

3.7 Identification

The identification part is major final part in the case of biometric combination, in this part the identification of the person is done with the help of fused score, we have already set a threshold value of 0.9, thus in the identification part if the out value is more than or equal to 0.9 the output can be confirmed as the authorized person was detected and if the ouput value is less than 0.9 the system understand that the person was not the right person and show the output as 'fail'. In this project if the person was right it shows the right person name, here we input the name as 'Rishan', because I took my own biometric traits here.[13]

That is if the similarity score of each trait average was calculated here and the final fused score is also calculated and finally, if the fused score is more than or equal to 0.9, then the person was identified, here we has already the similarity score of each set of biometric traits as '1', that is the cosine similarity score for palmprint, face recognition and fingerprint score, then by taking the average of this fused score, we get the output as '1', then it is identified the person was right and shows the output as 'Rishan' as identified person.

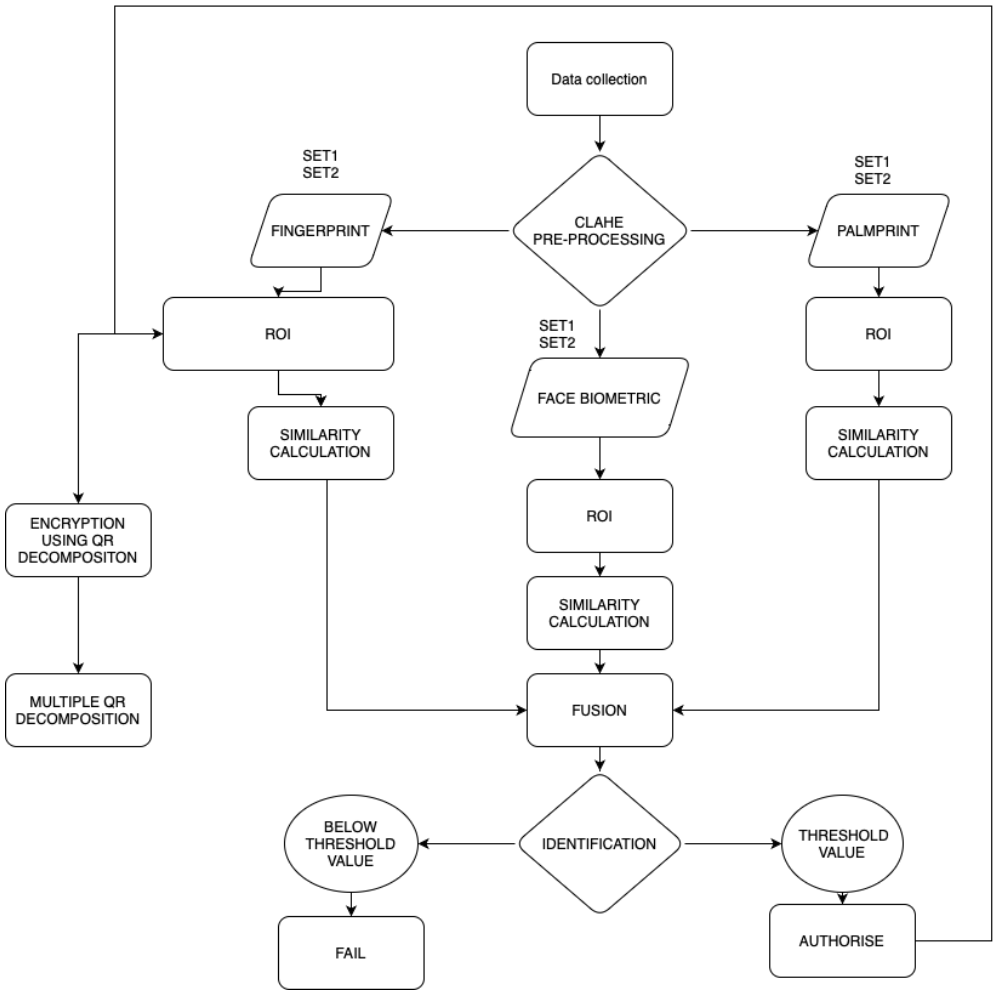

Figure 11: Shows the flowchart for biometric authorization

3.8 Encryption (Multiple QR decomposition method)

In this encryption process we are encrypting the fingerprint features data sets, in order to gain the maximum security for the data we collected, which is actually protecting the fingerprint data from cyber-attack.

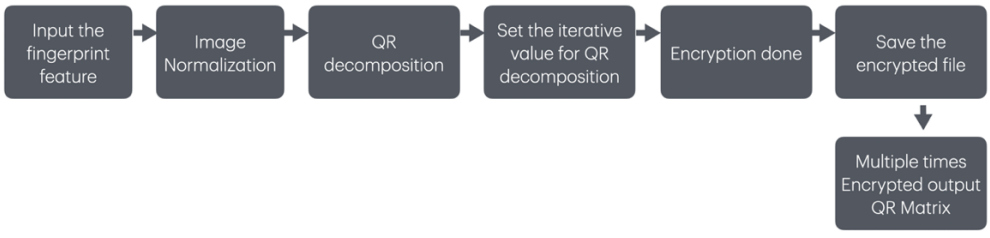

Figure 12: Shows the multiple QR decomposition

Here we are taking the multiple QR decomposition method, but only for the fingerprint sets, in order to do the multiple QR decomposition method, we are taking the numpy file that is already saved in our local disc, which contains the fingerprint features of different fingerprint set, after importing the feature set we need to normalize the set to correct the pixel density for the decomposition, Here we are taking 255 pixel density, after setting the normalization, we are applying the QR decomposition script using the linear algebra

algorithm of numpy for QR decomposition.[13], then we are applying this algorithm for Q and R matrix of the image feature. [14], after applying the QR decomposition, we are using the multiple QR decomposition method, in order to attain the maximum encryption, that is almost 3 rounds of iteration are using here for the QR decomposition. In order to do the multiple QR decomposition, we are using a set of defined number of decompositions to the earlier QR decomposition, thus here we are taking the number decomposition value as 3 for the fingerprint feature set, thus here we can get the encryption done as 3 times for Q and 3 times R and the file is saved in our local disc as numpy format. Then finally, we can see the output of the encrypted matrix as there are three matrixes named as 0,1,2 and the we got the encrypted output.

In this project I use my own biometric data for the facial, fingerprint and palmprint and combined these biometric data to find the similarity between the two sets of these biometric data and found out the final fusion score and encrypted the fingerprint data that I captured.

4. Design And Solution Development

In this project the solution for the proposed system is fit very well, here in the case of this project the security of authorization with multiple biometric technologies such as fingerprint, palmprint and face recognition along with the combination of these biometric traits improves a significant security in the case of authorization process. This combination of biometric can improve the efficiency and enhance the security of the authorization process. There are different techniques and most efficient and noncomplex methods are used here in order to find the reliable output such as the usage of specific algorithms for feature extraction, fusion of biometric traits, the similarity calculation and for the encryption process for the data that are collected.

With the help of QR decomposition method here, the security of the fingerprint data that are collected can be enhanced and also here not only the QR decomposition method, here the iteration method is used for multiple time the QR decomposition process is done without compromising the security of the overall system. Thus, from the proposed project it can understand that the project not only aims for the security of the authorization but also aims the security of the authorization data that are collected.

4.1 Technologies and tools used in this project:

Here we used Samsung Galaxy Note 10 Lite 12Megapixel camera to capture the set of digital images of the fingerprint, palmprint and the face, then imported the digital image to the programming language python. Python is the major programming language used here.

Table 1: Software and functions

Software and tools used	Functions
CLAHE	Used to fine tune the image as pre-processing
DenseNet201	Used to extract the features from the biometric image
SoftMax function	SoftMax function is used to classify the biometric image
ImageNet	Finetune the image for densenet201 processing

Cosine function	Cosine function is used to calculate the similarity between different set of biometric images
Score Level fusion	This algorithm is used to combine the different biometric traits together

The major tools such as CLAHE (Contrast Limited Adaptive Histogram Equalization) is used for the image tuning and enhancing, the CLAHE comes under the library of Scikit-image, which is a python library, the purpose of the CLAHE is mainly adjusting the contrast of the image by equalizing image histogram which spreads over the image with most intensity values.[16]
The DenseNet201, which is dense convolution network, here it is used to extract the features from the region of interest. This is the more accurate and efficient way of extracting the features from the image, in the case of densnet201, which connect each layer from the image, thus the unique feature of different region can be extracted. Here the library used for densenet 201 is tensor flow keras. [18]
The softmax function is machine learning algorithm, which is used particularly used I neural networks in order to classify images, this mainly function like prediction method. Here the function is prediction and classification of image that we input. [21]
Cosine function is used to calculate the similarity between the input classified images, the cosin function is used here to find the similarity between the fingerprint, palmprint and face image along with classification of softmax function, cosine similarity measures similarity between two non zero vectors in n dimensional space. The mathematical formula for cosine simalairty are,

Cosine similarity (A,B) = (A.B) / (||A|| * ||B||)
Where A and B are vectors and A.B are the dot product of these two vectors. [22]

Score level fusion method is used to combine the fingerprint plam print and face image after the similarity calculation, the fusion method helps to identify the person based on the biometric traits. [23] Associated libraries as follows,

Table 2: Libraries and functions

Libraries	Functions
Scikit-image	The CLAHE image tuning is included in this library
Matplot	Matplot library is used to visualize the tuned image
Dlib	For face detection and ROI extraction
numpy	Used here for hand biometric ROI extraction and QR decomposition
Tensorflow, keras	Used for feature extraction by Densenet201
Scikit-cosin	Calculate the similarity cosine score

The scikit image is a python library which includes several tools for image processing, this is an open-source algorithm with free of cost, this is written by volunteers of their community, this can process image with high quality. The version used here is the latest version that is 0.24.0 released on 18-06-2024. [17]

Matplot library is used to visualize the image that we input, here we are using the matplot library along with the CLAHE tool in order to visualize the image [24]. The library here we used is matplotlib 3.9.0 which is released on May 16, 2024.
DLib is a python library used to detect the face and extract the region of interest from the face [25]. The dlib is a C++ library for machine learning with open source programming.
Tensorflow keras is a library in python which is used to classify different images, this library is mainly used for DensNet201 in order to classify the image and extract the features from the image. [19] The tensor flow is an end-to-end machine learning program, which is used to build and fine tune the models, this can initiate the densenet201 tool to extract the feature [20]
Scikit-cosin is the same library which is used in the CLAHE, this also includes the cosine similarity function.
Numpy is a powerful library in the case of python, which includes with the working with array and used different types of domain such as linear algebra, Fourier transform, and matrices, here which is used here to extract the region of interest and QR decomposition for encryption.

4.2 Architecture:

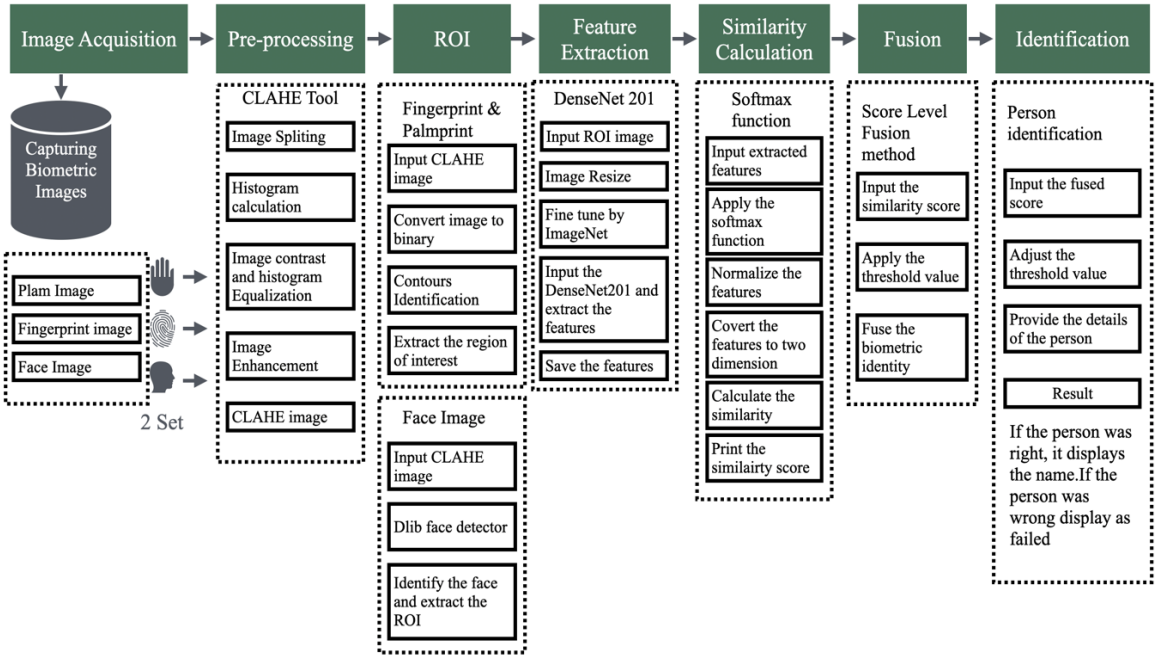

Figure 13: Shows the architecture

The figure above shows the architecture diagram of different components, the capturing of image is done in the image acquisition process, in this process the major tools used is a physical digital camera, in order to capture different types of biometric traits, the next process is the image pre-processing, in this process the processing of image is done with different tools and libraries such as CLAHE and the library used for this is the scikit image library, the matplot library is also used here to visualize the image. The next stage is the region of extraction, in this process the major libraries such as Dlib and numpy are used in python, the dlib library is used for the face detection, thus which helps to detect the region of interest from the face image. The numpy is used for the fingerprint and palmprint contour detection. In the case of feature extraction, the tools such as DenseNet 201 is used to extract the features form the region of interest, here the tools such as imagnet also used to fine tune the image for

the densenet processing, the libraries such as tensorflow and keras are mainly used here for the densenet201. The next step in the architecture is the similarity calculation, in this the tools such as softmax function and cosine similarity calculations are used, the cosine is used to calculate the similarity score and the softmax function is used to identify the image, the amjor library used here is Scikit-cosin for the cosine similarity calculation. After this we need to do the combination of biometric traits, for this fusion we are using the score level fusion method, in this score of the similarity value is considered in order to fuse these biometrics with a certain threshold value, the final identification of the person is done with this score level fusion method. This is the first stage of design architecture, and tools used in this project.

4.3 Encryption architecture:

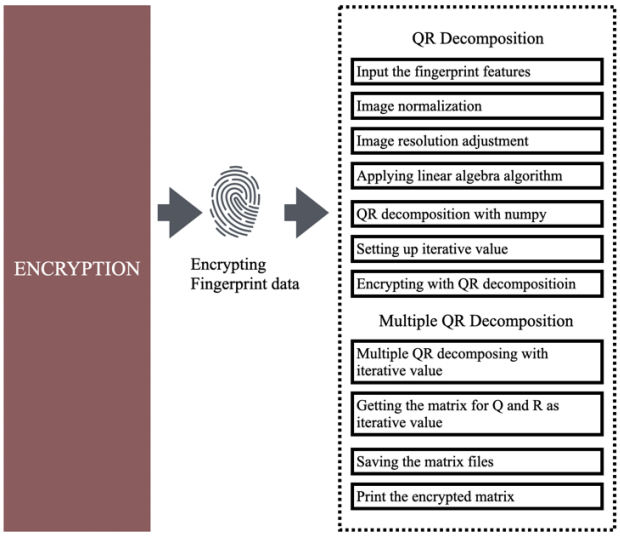

Figure 14: Shows the encryption using multiple QR decomposition

The next stage of the architecture design is the encryption stage, in this stage the encryption is done for the fingerprint data that we collected, the encryption is done with the help of QR decomposition method, here numpy is the major library used for the python in order to decompose the image to Q and R matrix for encryption purpose, then the use of numerical decomposition also done here to ensure maximum protection, that is decomposing the Q and R matrix with multiple times with a desired threshold value, so the decomposition is done by multiple time.

4.4 Solution Development:

The solution is the final stage of the development, the solution of this project contains the combination of biometric traits such as the fingerprint, palm print and face biometric. After the combining of these biometric traits we are calculating the value of the similarity score, here we took the same fingerprint, palmprint and face image by two sets and then pre-processing done for each set using the CLAHE algorithm and we extracted the region of interest for both the set of images. Then we extracted the features using densenet201 for each set.

Then we used to calculate the similarity using the cosine function and the classification done by the SoftMax function, the image set we took exactly the same image for the two set and image score is calculated as 100% for each set of similarity as shown in below table.

Table 3: Similarity score

Biometric set	Feature set file name	Cosine Similarity score
Fingerprint set 1 Fingerprint set 2	fingerprintfeatures.npy fingerprintfeatures2.npy	1.00
Palmprint set 1 Palmprint set 2	palmfeatures.npy palmfeatures2.npy	1.00
Face biometric set 1 Face biometric set 2	facialfeatrues.npy Facialfeatures2.npy	1.00

The final solution of the biometric traits are done with the help of score level fusion method, here the combination of these score to identify the person, thus here it is identified the person, with the help of these biometric cosine similarity score the person can be identified.
The next process is the encryption, in this case we need to encrypt the fingerprint data. In order to make the encryption process, we are using the QR decomposition, here the data of fingerprint features are extracted, the encryption is done by three iteration in order to achieve the maximum encryption using multiple QR decomposition, the image feature is decomposed to Q and R matrix and the iterations done, here there are two sets of fingerprint data, thus the output here is three Q matrix and three R matrix on each set, here there are 2 sets thus the total matrix will be 12.

Table 4: Showing the fingerprint feature encryption using matrix

Fingerprint set	Matrix	Iteration done
Fingerprint set 1	Encrypted Q matrix	Three round iterations
Fingerprint set 1	Encrypted R matrix	Three round iterations
Fingerprint set 2	Encrypted Q matrix	Three round iterations
Fingerprint set 2	Encrypted R matrix	Three round iterations

5. Evaluation And Result Analysis

5.1CLAHE

The Contrast Limited Adaptive Histogram Equalization, in this we done the histogram equalization, adjusted the contrast, the output of the histogram after clip limit is shown below, the original image, CLAHE image and the equalized image is shown below. This is used as pre processing of the image, as a result we get the equalized and CLAHE image and the histogram as well. The image is visualized with the help of matplot.

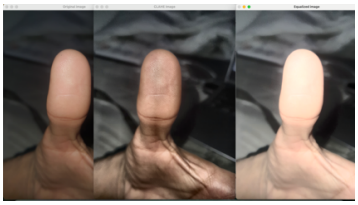

Figure 15: Showing the original, CLAHE and equalized image of fingerprint

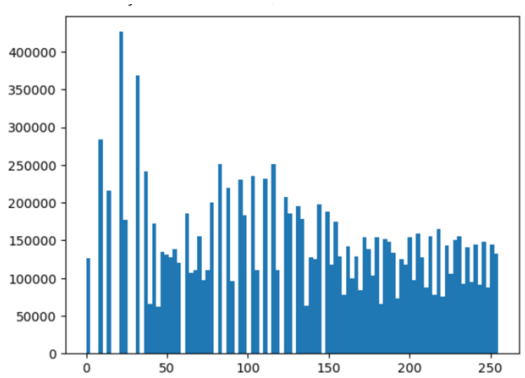

Figure 16: Showing the histogram after equalization of fingerprint

The CLAHE pre-processing is also done with the palmprint biometric set, the pre-processed image of palmprint is shown below, here the clip limit is done and the equalization of image histogram is also done by adjusting the contrast, the figure below shows the original image, equalized image and the CLAHE image.

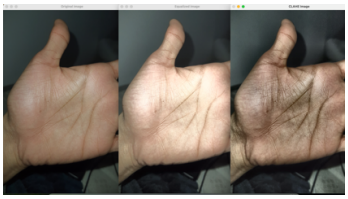

Figure 17: Showing the original, equalized and CLAHE image of palmprint

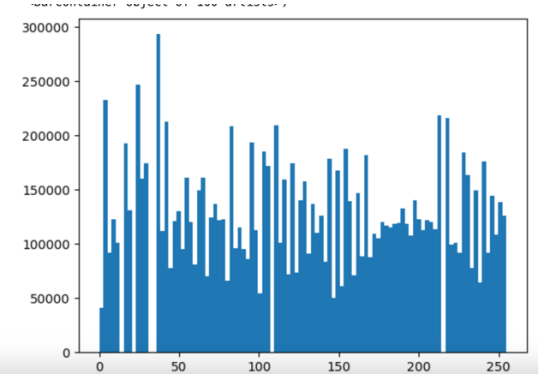

Figure 18: Showing the histogram after equalization of palmprint

The pre-processing of face biometric is also done in the case in the case of face biometric, here, the equalization is done after flattening the image, the equalized histogram is shown in below, the image is also enhanced into equalized image and CLAHE image, below the figure showing the equalized image, the CLAHE image and the normal image.

Figure 19: Showing the equalized, CLAHE and normal image of face biometric image

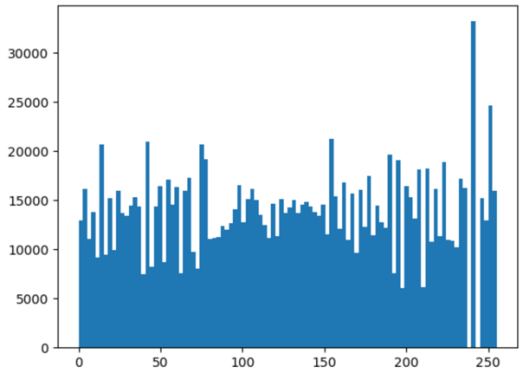

Figure 20: Showing the histogram after equalization of face biometric

5.2ROI

The region of interest is done for different biometric traits in this project in order to identify the uniqueness of the preprocessed image, here the region of interest is done in the case of fingerprint CLAHE image, in order to identify the unique contours, the extracted region of interest is shown in below figure for the fingerprint biometric


Figure 21: Showing the Region of interest for fingerprint biometric

In the case of palm print biometric the region of interest is also extracted with the help of numpy array and the roi size is also calculated as 200 pixel, the contours are identified here the region of interest is shown in below figure for the palmprint biometric.

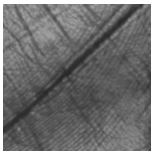
Figure 22: Showing the Region of interest for palmprint biometric

In the case of face biometric the region of interest is extracted with the help of dlib library, here the face detection is done accurately and extracted the region of interest with appropriate size and saved the extracted ROI, the region of interest for the face biometric is shown in below figure

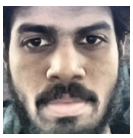
Figure 23: Showing the Region of interest for face biometric

After the region of interest extraction, the feature extraction is done with the help of denset201,eeach biometric trait feature vector is extracted with a vector value of (1,1920) for face and fingerprint, the palmprint has done a feature extraction with (1,7,7,1920) vectors and

saved the feature files to the local disc. The similarity calculated and it is identified that each biometric trait has a value of 1.00 as cosine similarity, then we use the fusion algorithm for fusing these biometric traits using the score level fusion method with threshold value as 0.9 and identified the person for these biometrics with the two sets of similar biometric traits. Then finally, we need to do the QR decomposition for the feature set extracted from the region of interest, this method can encrypt the feature set of fingerprint biometric in multiple levels, here we done numerical decomposition for the QR decomposition with a threshold value of 3, thus the fingerprint vectors are decomposed to multiple 3 times and saved the file to the local disc as multiple QR decomposition, the steps are counted as step0 , step1 and step2 for the decomposition. The output matrix after the QR decomposition is shown below and also the saved files.

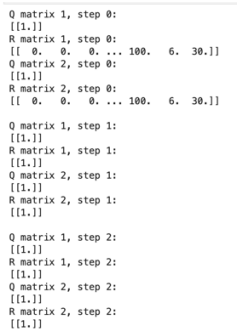

Figure 24: Shows the multiple QR decomposed matrix for fingerprint feature set

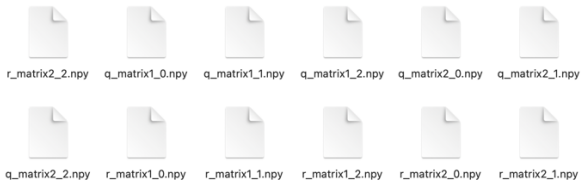

Figure 25: Shows the saved files of matrix decomposed into three time

6. Conclusion And Discussion

The combination of face recognition, fingerprint and palm biometric recognition helps to improve the overall security of authorization according to access control of any biometric system. The authorization security is improved because of combining different biometric traits, but not only the security of authorization but also the security of the overall biometric data that are taken for authorization. Here we used the most advanced tools and algorithms to make the authorization process easy and simple without compromising the security of the system.

In this project the output of each system that are conducted has played an important role in the overall security, reliability and accuracy of the system. The combination of the biometric traits are important here, the cosine similarity value is calculated without compromising the level security and accuracy by setting up the maximum threshold value.

The encryption method here used is the QR decomposition method, through this method the output can be achieved through the matrix of Q and R that are the encrypted key values. These are then iterated and result obtained with the multiple times iterated values can be saved to our local disc. The reliability of the system increased with the multiple times numerical decomposition of Q and R matrix. It is found that the Q is iterated by 3 times and R is iterated by 3 times as the iterative threshold value is 3. Thus each set has been iterated in

the case of fingerprint feature alone. This results the output matrix into 12 different values of each Q and R matrix. Thus this increase the encryption reliability of the system without sacrificing the time and resources. It is identified that the output of the system can be gained by minimum resource requirement that is low percentage memory usage, CPU and graphics usage when calculating the overall result from image acquisition to encryption process. Thus this confirm the low requirement of resources and this is a time saving process without compromising the security and reliability, that is the major advantage of this system.

This application can be used into major authorization process like airport, defense or like universities, college and much more. There are also some minor updation can be considered if the capturing camera used for the acquisition process can be improved, this helps to capture the biometric images with high quality and high accuracy, the implementation of encryption to every biometric data traits can be useful to enhance the overall secuirty, this can be considered as the future work of this project. The major advantages like low resource requirement, very less amount of time is required and also cost effective method without sacrificing the security not only for authorization but also for encrypting the biometric captured data.

Reference:

[1] I. Singh, T. Singh, S. Luthra, and S. Khatri, “Harris Hawk Optimized CLAHE and Novel Score Level Fusion of Lightweight CNNs for Multimodal Biometric Recognition,” Apr. 2024, doi: https://doi.org/10.1109/pais62114.2024.10541196.

[2] R.-C. Chen, C. Dewi, Y.-C. Zhuang, and J.-K. Chen, “Contrast Limited Adaptive Histogram Equalization for Recognizing Road Marking at Night Based on Yolo Models,” IEEE access, vol. 11, pp. 92926–92942, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3309410.

[3] “Contour Detection using OpenCV (Python/C++),” LearnOpenCV, Mar. 29, 2021. https://learnopencv.com/contour-detection-using-opencv-python-c/

[4] “OpenCV: Contours : Getting Started,” docs.opencv.org. https://docs.opencv.org/3.4/d4/d73/tutorial_py_contours_begin.html#:~:text=contours%20is%20a%20Python%20list

[5] J. Ng, Hui, U. Tunku, and A. Rahman, “TITLE PAGE CONTACTLESS PALMPRINT VERIFICATION USING SIAMESE NETWORKS A REPORT SUBMITTED TO,” 2022. Accessed: Aug. 11, 2024. [Online]. Available: http://eprints.utar.edu.my/4661/1/fyp_CS_2022_NJH.pdf

[6] M. Aydın et al., “FACE RECOGNITION APPROACH USING DLIB AND K-NN.” Accessed: Aug. 11, 2024. [Online]. Available: https://dergipark.org.tr/en/download/article-file/3703733

[7] “tf.keras.applications.DenseNet201 | TensorFlow v2.16.1,” TensorFlow, 2024. https://www.tensorflow.org/api_docs/python/tf/keras/applications/DenseNet201 (accessed Aug. 11, 2024).

[8] G. Huang, Z. Liu, and Weinberger, Kilian Q, “Densely Connected Convolutional Networks,” arXiv.org, 2016. https://arxiv.org/abs/1608.06993

[9] P. Belagatti, “Understanding the Softmax Activation Function: A Comprehensive Guide,” SingleStore, Mar. 11, 2024. https://www.singlestore.com/blog/a-guide-to-softmax-activation-function/

[10] J. Brownlee, “Softmax Activation Function with Python,” Machine Learning Mastery, Oct. 18, 2020. https://machinelearningmastery.com/softmax-activation-function-with-python/

[11] K. Aizi and M. Ouslim, “Score level fusion in multi-biometric identification based on zones of interest,” Journal of King Saud University - Computer and Information Sciences, Sep. 2019, doi: https://doi.org/10.1016/j.jksuci.2019.09.003.

[12] “QR Decomposition with Python and NumPy | QuantStart,” Quantstart.com, 2024. https://www.quantstart.com/articles/QR-Decomposition-with-Python-and-NumPy/ (accessed Aug. 11, 2024).

[13] “Linear algebra (numpy.linalg) — NumPy v1.20 Manual,” numpy.org. https://numpy.org/doc/stable/reference/routines.linalg.html

[14] “QR Decomposition,” Intermediate Quantitative Economics with Python, 2024. https://python.quantecon.org/qr_decomp.html#:~:text=The%20QR%20decomposition%20(also%20called (accessed Aug. 11, 2024).

[15] “skimage.exposure — skimage 0.24.0 documentation,” Scikit-image.org, 2024. https://scikit-image.org/docs/stable/api/skimage.exposure.html#skimage.exposure.equalize_adapthist (accessed Aug. 11, 2024).

[16] “Histogram Equalization — skimage 0.22.0 documentation,” scikit-image.org. https://scikit-image.org/docs/stable/auto_examples/color_exposure/plot_equalize.html

[17] “scikit-image: Image processing in Python — scikit-image,” scikit-image.org. https://scikit-image.org

[18] G. Huang, Z. Liu, L. Van Der Maaten, and K. Weinberger, “Densely Connected Convolutional Networks.” Available: https://arxiv.org/pdf/1608.06993

[19] “How can TensorFlow be used for image recognition?,” Linkedin.com, 2024. https://www.linkedin.com/advice/1/how-can-tensorflow-used-image-recognition-im6lf#:~:text=It%20involves%20teaching%20a%20computer (accessed Aug. 11, 2024).

[20] “tf.keras.applications.DenseNet201 | TensorFlow v2.16.1,” TensorFlow, 2024. https://www.tensorflow.org/api_docs/python/tf/keras/applications/DenseNet201

[21] S. Saxena, “Softmax | What is Softmax Activation Function | Introduction to Softmax,” Analytics Vidhya, Apr. 05, 2021. https://www.analyticsvidhya.com/blog/2021/04/introduction-to-softmax-for-neural-network/

[22] DataStax, “How to Implement Cosine Similarity in Python,” Medium, Nov. 30, 2023. https://datastax.medium.com/how-to-implement-cosine-similarity-in-python-505e8ec1d823

[23] K. Aizi and M. Ouslim, “Score level fusion in multi-biometric identification based on zones of interest,” Journal of King Saud University - Computer and Information Sciences, Sep. 2019, doi: https://doi.org/10.1016/j.jksuci.2019.09.003 .

[24] “matplotlib.pyplot.imshow — Matplotlib 3.5.2 documentation,” matplotlib.org. https://matplotlib.org/stable/api/_as_gen/matplotlib.pyplot.imshow.html

[25] “Face detection with dlib (HOG and CNN),” PyImageSearch, Apr. 19, 2021. https://pyimagesearch.com/2021/04/19/face-detection-with-dlib-hog-and-cnn/

[26] A. Gillis, “What is biometrics?,” *TechTarget*, Jul. 2021. https://www.techtarget.com/searchsecurity/definition/biometrics

[27] Mouad. M. H. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, “Overview of fingerprint recognition system,” *IEEE Xplore*, Mar. 01, 2016. https://ieeexplore.ieee.org/abstract/document/7754900

[28] S. Li, L. Fei, B. Zhang, X. Ning, and L. Wu, “Hand-based multimodal biometric fusion: A review,” Information Fusion, p. 102418, Apr. 2024, doi: https://doi.org/10.1016/j.inffus.2024.102418

[29] B. Alharbi and H. S. Alshanbari, “Face-voice based multimodal biometric authentication system via FaceNet and GMM,” PeerJ, vol. 9, pp. e1468–e1468, Jul. 2023, doi: https://doi.org/10.7717/peerj-cs.1468.

[30] I. Mehra and N. K. Nishchal, “Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition,” Optics Communications, vol. 533, p. 129265, Apr. 2023, doi: https://doi.org/10.1016/j.optcom.2023.129265.

[31] “AN INTELLIGENT MULTIMODAL BIOMETRIC SYSTEM FOR PERSON RECOGNITION BASED ON PALMPRINT, FINGER KUNCKLES AND NAILS,” International Research Journal of Modernization in Engineering Technology and Science, May 2023, doi: https://doi.org/10.56726/irjmets38943.

[32] M. Rafiq Abuturab, “Multiple color image cryptosystem based on coupled-logistic-map-biometric keys, QR decomposition with column pivoting and optical Fresnel transform,” Optics & Laser Technology, vol. 161, p. 109109, Jun. 2023, doi: https://doi.org/10.1016/j.optlastec.2023.109109

[33] M. Musthafa, “Types of Biometrics,” ClaySys Technologies, Dec. 14, 2022. https://www.claysys.com/blog/types-of-biometrics/

[34] V. Savage, “FIDO2 Authentication: Towards a passwordless future - LoginTC,” LoginTC, Jun. 20, 2024. https://www.logintc.com/fido2-authentication/ (accessed Aug. 12, 2024).