GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(Deemed to be University)

Bengaluru-561203

"FACIAL RECOGNIZATION USING LBPH ALGORITM FOR DIGITAL PAYMENTS"

Department of Electronics and Communication Engineering

Submitted by:

NAMES	REGISTER NUMBERS
Kodidela Dinesh Naidu	**322010403006**
Boksam Nithin Varma	**322010403031**
Mange Amith Das	**322010402033**
R Nikhil Kumar	**322010402004**

Under the Guidance of

DR Ramesha M

Assistant professor, Department of Electronics and Communication Engineering,

GITAM School of Technology
GITAM
(DEEMED TO BE UNIVERSITY)
(Estd. u/s 3 of the UGC act 1956)
NH 207, Nagadenehalli, Doddaballapur taluk,
Bengaluru-561203
Karnataka, INDIA.

GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(Deemed to be University)
Bengaluru - 561203

Department of Electronics and Communication Engineering

Certificate

This is to certify that the project titled "Facial recognition using LBPH algorithm for Digital Payments " is the bona fide work carried out by , Kodidela Dinesh Naidu (322010403006) , Boksam Nithin Varma (322010403031), Mange Amith Das (322010402033), R Nikhil Kumar(322010402004),the students of B Tech (ECE) of GITAM Deemed to be University, Bengaluru campus during the academic year (2020-2024), in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology (Electronics and Communnication Engineering) and that the project has not formed the basis for the award previously of any other degree, diploma, fellowship or any other similar title. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the departmental library.

_____	_____
Signature of the Guide	Signature of HOD
DR RAMESHA M	DR AJAY KUMAR MANDAVA
Assistant Professor	Head of the Department
Department of ECE, GST	Department of ECE, GST

DECLARATION

We **Kodidela Dinesh Naidu, Boksam Nithin Varma, Mange Amith Das , R Nikhil Kumar,** students of 7th semester B.Tech in Electronics and Communication Engineering from GITAM (Deemed to be University),Bangalore, hereby declare that the dissertation work entitled **"Facial recognition using LBPH Algorithm -for Digital Payments"** has been carried out under the guidance of **DR RAMESHA M** Assistant Professor Department ECE, GITAM (Deemed to be University), Bangalore, in the partial fulfilment of the requirement of the degree of the **BACHELOR OF TECHNOLOGY in ELECTRONICS AND COMMUNICATION ENGINEERING of GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT (GITAM).** We declare that we have not submitted this dissertation either in pass or in full to any other University for the award of any degree.

Place: Bengaluru

Date: 7/11/2023

signature of students

Kodidela Dinesh Naidu
Boksam Nithin Varma
Mange Amith Das
R Nikhil Kumar

ABSTRACT

The digital payment systems are evolving rapidly from past few decades by overcoming the problems that were existing in the previous payments system. In this paper, we proposed the system for digital payments by using the facial recognition. By using this proposed system it is possible to make the payments without using any cards or cash or mobile hence even if customer forgot his wallet or mobile the payments system will be uncompromised. In this paper LBPH is used for facial recognition as LBPH algorithm can be used to represent local features in the images. Good results can be obtained using LBPH algorithms primarily in a managed environment.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

CHAPTER 1
INTRODUCTION

In most transactions involving its citizens in digital nation should be "Paperless and Cashless". Traditionally, cashless transfers are encouraged by using Payment Cards (Debit Card, Credit Card, Prepaid Card, and Gift Card). Nevertheless, the need to allow payments via them has emerged as a normal necessity, leading to the enormous proliferation of mobile phones and other digital apps worldwide. Mobile payments have been enabled in the initial years by USSD, UPI AEPS, Mobile Wallets, POS, Micro ATMs, Mobile Banking, Internet Banking, etc. of which transfers are gaining popularity via mobile wallets (wallet apps) as they provide consumers with greater accessibility and versatility [1]. In fact, mobile payments use the wallet app to transfer money or pay for goods or services. According to KPMG, India has over 45 mobile wallet providers, and some 50 UPI-based wallet providers. There is still a lot of growth: In India, according to the BIS, there were only 18 cashless payments per inhabitant on average in 2018 compared to 142 in China and 529 in Sweden [2]. While these digital payment systems offer ease of use, prevent cash management and omnipresence, customers may reveal their wallet or bank details to the retailer, which may result in theft, consumer profiling and impersonation [3]. Mobile wallet payments may face several threats affecting secure transactions. Unintentional updation of Malware programs and installation of non-trusted applications, phishing strikes, and unauthorized access of missing and stolen mobile devices, security threats related to the use of public Wi-Fi connections for mobile payments and several others including the misuse of account details by cybercriminals. The possible Merchant threats encompass the malware upload on POS device terminal, Man-in-the-Middle (MITM) between POS and server, Relay attacks against the NFC based POS interface and so on [4].

The security aspect of digital payments remains paramount importance. We propose a new platform to allow Electronic Payments quick and secure by using Face Recognition. Purchases with small purchases can be made without cards or tablets. We also made a step forward by developing an authentication mechanism focused on the combination of human face and mobile fingerprint recognition. Due to image processing technologies, the distinguishing attributes of both the person and the camera that recorded the facial picture can be derived from a single photo or video frame and used for double consumer identification verification [5].

The currency or actual distribution of money was the only primary thing used before the technological evolution contributed to the creation of the payment system. The customer always had to bring the amount of cash that wasn't easy to carry as there would be more actual money in volume

and holding huge amount of cash wasn't secure that was vulnerable to robbery. Later the credit card and debit card payments were introduced and made the transfers smoother and reduced the burden of bringing the huge sum of cash around. The credit card details could also be used by using the card details in online payments through websites or mobile application. This advancement has also introduced another challenge as payments can only be made by using the details on the card if the cards are missing or the cards are in the wrong hands then the card holders are in trouble as the payments can be made by anyone who has a card. The card details entered in the website or mobile application will be kept in the databases if that data is not secured or encrypted in the database then the cardholders details can be leaked.

Authentication can be achieved with one or a combination of the following items:

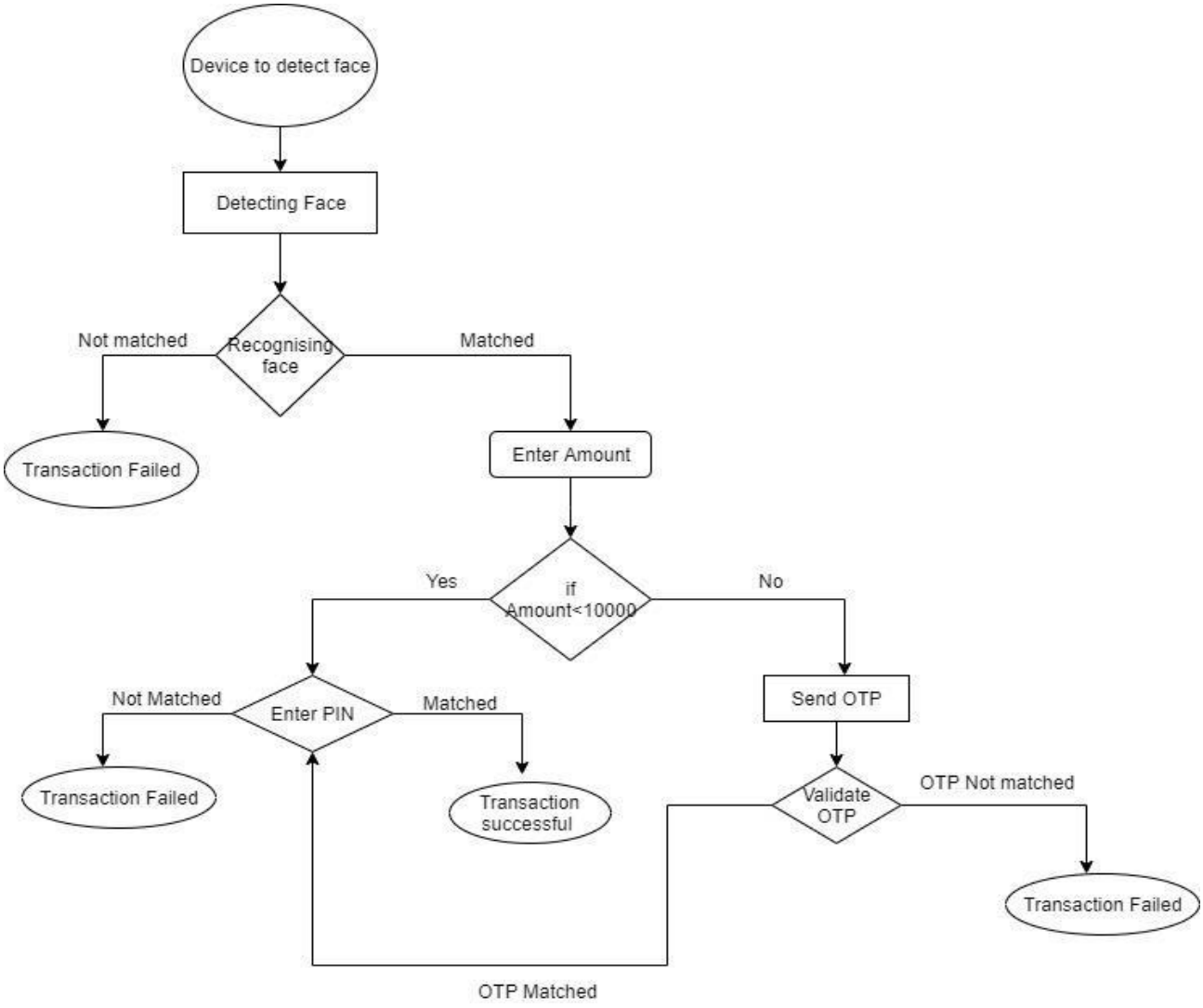
• Whatever the user knows (e.g. password, personal identification number (PIN)).

• The customer has something (e.g., smart card, ID card, authentication token, and smartphone).

• User is or does something.

If we consider all possible combinations of the three authentication factors, we get the ranking, from the lowest to the highest security. Even for small payments, a user must always carry cash or cards or mobiles.

Cashless payments are taking off in India, growing faster than in other countries around the world. The shift has attracted a host of tech companies, backed by deep-pocketed foreign investors, battling for market share. According to data from the Bank for International Settlements (BIS), Indian digital transactions rose by 55% last year, compared to 48% in China and 23% in Indonesia. In comparison, the UK, where card sales have now died down, expanded in 10 percent in cashless payments [3]. In spite of the fact that there are scarcely any security worries in versatile financial applications, they are as yet favoured by everybody, due to its notable points of interest like quick, simple to utilize, helpful to take care of tabs, convenient, accessible and so forth. Indeed, even banks advance portable banking as it assists with taking care of more clients with improved client administrations at decreased operational expense without settling on administration quality. Banks likewise offer limits, blessings and so on., to advance portable banking.



1.1 System Architecture

1.1 Problem Statement

As many people are habituated to stay in the comfort zone by using the new technologies are evolving day by day in the world, but the one difficulty where we are suffering or in out of that comfort zone is at the payments or transactions. Generally the payments are happening through the paper / card / mobile. Each of the available methods will deals with the need of effort from us. The mobile

transactions are also not easy when we are doing shopping as it goes through of effort of opening the phone and then opening the particular payment application and scanning of the QR code or entering the merchants phone number, the exchange of money is requires a lot of time, now the debit / credit card the customer has to give the card and then entering of PIN also requires of handling the card from us. For this purpose, in our work, the payments using the face will takes us to the comfort zone as our system does not require anything that a customer should handle, similarly like other payment applications our system requires the customer interaction of entering the ID and the as usual Unified Payments Interface PIN, the one main thing that a customer should handle is the face, you heard it right we use face of the person for the transactions to happen. By using the LBPH algorithm we classifies the face of a person for handling their accounts. With the use of face the payments are going to happen in our system in an easy and efficient manner.

In conclusion, the transition to cashless and paperless transactions, particularly through mobile payments, has revolutionized the way we handle financial transactions. While these methods offer unparalleled convenience, they also raise significant concerns about security and privacy. The integration of advanced technologies, such as face recognition, presents a promising solution to enhance the security of digital payments. As the world continues to embrace digital transactions, it is crucial for individuals, businesses, and financial institutions to prioritize the implementation of robust security measures, ensuring a seamless and safe experience for users in the evolving landscape of electronic payments.

.

CHAPTER 2

LITERATURE SURVEY

CHAPTER 2

LITERATURE SURVEY

A literature survey or a literature review in a project report is that section which shows the various analyses and research made in the field of interest and the results already published, considering the various parameters of the project and the extent of the project. It is the most important part of report as it gives a direction in the area of research. It helps to set a goal for the analysis - thus helping to get the problem statement.

The digital era has made transactions go paperless and cashless. Cashless transactions have evolved through the banking sectors making people more reliable on digital transactions rather than going to bank or depending on cheque books. These digital payment services have opened ways to frauds, customer profiling and impersonations. The increasing challenge in this cyberspace has necessitated several researchers to improve security of existing electronic payment systems and also develop novel strategies to address the issue.

Husni and Ariono. 2014,[6] developed an electronic payments system using Near Field Communication (NFC) enabled android smartphone transactions. Transaction data was composed of encrypted payloads, header, and initialization vector used to decrypt the payload. Advanced Encryption Standard (AES) algorithm secured the key used to encrypt the transaction data. This technology offered easy and secured two way communication based transaction for electronic payments. In an attempt to address the security and privacy issues, Rajendran et al. 2017,[1] proposed an intermediate entity which involves the digital token system based on the principles of cryptography. The system facilitates the payer and payee transactions with digital token DTE generated by bank for the customer by encrypting using public key. Privacy of the customer is reserved by avoidance of payments using pseudo identity, convenience of payments across any device, counterfeit avoided by encryption with RSA/ECC signature schemes to DTE and its scalability.

A Biometric face recognition based digital payment system was proposed by Gondhkar et al. 2018,[7] for ubiquitous, card less and cashless payments with simple and secure features. This system verifies the person's face and compares the input image with those existing in the database further implementing normalization. Image normalization is crucial in processing digital images involving their enhancement, compression, segmentation and description. The eigenfaces were constructed from various eigenvectors using Euclidean distance algorithm and the face image was envisaged into face space for analysis and representation. But, the drawback of this system is its ability to recognize the face at the merchant payment device which already exists in the stored data base. With the ever-increasing threats in cyber space, its pivotal to eliminate Man-In-The-Middle attack (MITM), session

hijacking, illegal transaction, phishing Attacks, pharming, malware and so on. Several investigators have proposed the application of the Three-factor authentication protocols encompassing passwords, smart cards, and bio measurements to address the vulnerability of network security in digital financial transactions. Nair et al. 2019[8] devised a robust three-factor authentication protocol employing the combination of password, certificate and biometric/ Time based One Time Password (TOTP) for UPI mobile wallet to defeat session capture attacks thus securing the transactions.

Facial recognition technology is highly prone to face spoof attack that is simply instigated through high resolution printed face images, video replays and 3D face masks. Patel et al. 2016,[9] used an image distortion analysis in 2D spoof face images to address face spoof detection mainly applicable in smartphone unlock and mobile payment systems. This investigation suggested face normalization based on Inter-Papillary Distance (IPD) and the use of red color channel for feature extraction in comparison to the grayscale image improved spoof detection and bezel detection, thus efficiently detecting face spoof attacks in real applications. Face recognition with the aid of video monitoring cameras face challenges of inadequate identification, illumination and resolution. To resolve these issues faced by face recognition system, several researchers have designed algorithms including Sparse Coding (SC), Local Binary Pattern (LBP), Histograms of Oriented Gradients (HOG) , Linear Discriminant Analysis (LDA) and Gabor feature algorithm that operate with 50-75% accuracy. [10] Ahmed. et al. 2018 proposed a system for recognition employing the Local Binary Patterns Histogram (LBPH) algorithm architecture for face representation, feature extraction and later categorization of the detect face by comparing with the dataset (LR500). The proposed system operated even at very low resolution aiding in face identification from different angles and during human movement, and distinguished between identified and unidentified face thus helping in the detection of criminals. However, this algorithm limits for the detection and recognition on only available dataset of databases. Zhang et al., 2018, [11] proposed a combination of algorithms to secure mobile financial transactions using face identity authentication system. Initially preprocessing was carried out for image quality enhancement, face detection was achieved by implementing Haar and AdaBoost algorithms and LBP operator was employed for extracting features of face area and finally authentication achieved using Euclidean distance.

In this paper they proposed a Age -invariant system which uses a facial aging algorithm in order to recognize face shapes, textures (ex: wrinkles) .This model adapts 3D face models to the given 2D face aging database, their approach includes three different databases of FG-NET,MORPH and BROWNS using 'FACEVACS' and "a state-of-the-art commercial face recognition engine". The accuracy is 63% in real time so its not a good idea to implement in digital payments at present[5],With

the arrangement of Face Recognition framework being utilized in PDAs and different applications over worldwide an extremely basic test that is looked by many is face-mocking assaults. By Face ridiculing one can open someone else's telephone and applications and abuse it. This assault can be handily propelled by 3D veils or printed photographs. We address this issue of face mocking location against print photograph and 3D covers dependent on the investigation of picture mutilation, for example, surface reflection, shape disfigurement, shading twisting. For 3D face profundity examination a live face is recognized as 3D while a mock picture or face is distinguished as 2D. These 2D face ridiculing are fundamentally propelled by printing face picture or by showing advanced face picture or video since they have reflexive surface they reflections can be effectively distinguished and perceived.

CHAPTER 3

PROBLEM IDENTIFICATION AND OBJECTIVES

CHAPTER 3

PROBLEM IDENTIFICATION AND OBJECTIVES

LBPH algorithm is one of the technique that is used for the face recognition purpose. The main objective of this project is to find the easy and secured way of digital payments using the face of a authorized person (obtained from the device). This process usually comprises of the following steps. Firstly the face is to be detected and stored in the database in the grayscale format as the pixels range from (0 ~ 255) and a unique ID is generated to the user, this resembles like registration process. Then while making the payment the user has to enter the particular id given to the user, so as to match the face of the person and then goes to the payment process of Unified Payments Interface and asks the user to enter PIN to complete the transaction. Thus, this system involves the fundamental idea of various algorithms required to accomplish the transaction using the face recognition.

- Creating the dataset for faces
- Training of the dataset using IDs (Histograms are created for images)
- Recognition of the face
- Matching histogram checking using ID
- Payment Interface

This feature of the algorithm mentioned above helped in achieving faster and secured way of payments. This process of matching the face consists of steps like image capturing, storing at the data base, creating histograms and combining them in a folder by the name of ID, training the dataset, providing the unique IDs, converting the input to grayscale format and size should be taken care.

3.1 Solution for the problem statement

A device with camera that can capture pictures / images of at a size of 300*300 though the face is present at the low resolution. A typical installation consists of an interface device with the internet connection and camera and that works in the fast and efficient manner, so for that a system of high ram and Operating System can be of Windows / Linux. A database should be present at the server side to manage the images stored with a particular ID. The server system should be able to handle the database that where the images are stored as handling of images in the database is quiet complicated rather than handling of normal relational database with rows and columns.

An image matching at the dataset is a difficult problem, to overcome this we created a ID for each person so that while starting the transaction first the user has to enter that provided ID by using that

we can recognise the persons face to match at the particular folder with ID where the images are stored. For this the main cause to occur the transaction is the number given to the user. The Local binary pattern histogram algorithm will works efficiently in recognizing the face.

The system normally consists of the following parameters:

- **Radius –** the image radius of size 3*3 square (only face)
- **Histogram(s) –** Generates graph of the face
- **Illumination –** a controlled light that can bright up the face and allows day and night operation.
- **Computer –** normally pc running Windows or Linux. It runs the payment and face application which is used at the recognition side.
- **Software –** the application and the recognition package and payment interface. Usually the payment application is of UPI.

There are several possible difficulties that the software must be able to cope with. These include:

i. Poor image resolution, usually because the face is too far away but sometimes resulting from the use of a low-quality camera.

ii. Bad images particularly blur.

iii. Poor lighting and low contrast due to overexposure, reflection or shadows.

iv. An object obscuring (part of) the face, quite often a hand, or shades on the plate.

v. A different face, popular for other faces as while capturing the face some other person might disturb or enters at the camera

While some of these difficulties can be adjusted within the software, it is primarily left to the hardware side of the system to work out to these difficulties. Adjusting the position of the camera may avoid problems with objects. In some cases due to camera position is not good at the time of recognising some problems like other person may come into the camera covering or objects that interrupts the face like heavy brightening at the back of the persons face or the person is looking at somewhere may cause the matching of the face after entering the ID. These are some problems that we should take

into considerations so that we take those as challenges and can overcome. Some problems may be avoided in this system such as the expression as we did not taken that and it is our future work, we use that expression and we have an idea of providing the threat alert.

CHAPTER 4

SYSTEM METHODOLOGY

CHAPTER 4
SYSTEM METHODOLOGY

This system takes the input and returns the face that matches with ID and histogram value is calculated for this input using the Euclidean distance formula, checks with matching histogram value at the trained dataset is checked and provides the output along with the identification number. The idea to develop this system came from the money. Since the growth of money started with barter scheme which the mutual exchange of goods and services and drawn over these years from coins to paper (cash) to plastic money (Cards) and now the mobile payments came into picture, it provides the facilities of instant money transfer with the several modes of NEFT, UPI, IMPS, USSD, Mobile wallet and some other options of payment. The user has to choose any of the available mode that can be of either offline / online and maybe of confidential ways of payments with the phone. We created a new mode of payment that doesn't needs of anything that a user should carry. The only one that requires is to keep the numbers remember to make the payment. The face is the major thing in our system, it leads the entire process.

The workflow of the face recognition system involve various steps: The first thing after starting is to load the camera and after opening the camera the algorithm will detects the face and now the performs the image pre-processing which means of extracting the features from the image and catches only the face of the person and after catching the histogram value is evaluated for each of the images captured by the camera, the extraction is done now the classification and training classifier dataset module will occurs. The workflow of camera system can be shown in below fig

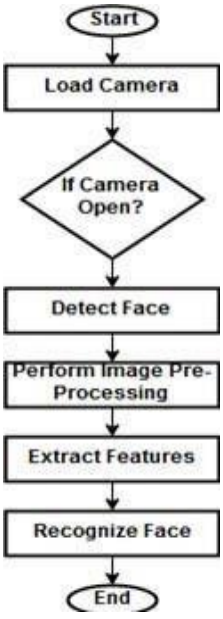


Figure 4.1: Workflow of Camera system

4.1 FACE DETECTION:

We have utilized OpenCV which presents a Haar cascade classifier, which is utilized for face discovery. The Haar cascade classifier utilizes the AdaBoost calculation to recognize different facial highlights. To start with, it peruses the picture to be recognized and changes over it into the dim picture, at that point loads Haar cascade classifier to choose whether it contains a human face. Provided that this is true, it continues to inspect the face highlights and draw a rectangular casing on the distinguished face.

4.2 FEATURE EXTRACTION:

The LBP administrator is applied to depict the complexity data of a pixel to its local pixels. The first LBP administrator is characterized in the window of 3*3. Utilizing the middle pixel esteem as the edge of the window, it contrasts and the dim estimation of the contiguous 8 pixels. On the off chance that the local pixel esteem is bigger or equivalent contrast with the middle pixel esteem, the estimation of pixel position is set apart as 1, in any case set apart as (0).

$$f(x) = \{^{1, x \geq 0}_{0, x < 0}\} \quad (1)$$

1	2	3
6	5	7
5	3	1

Threshold

0	0	0
1		1
1	0	0

Table 4.2.1 : LBP Operator

The above table contains the Binary value: 00010011 which is equivalent decimal value of 19. The f(x) value is the central value of the first table based on that value on the table is filled with zeros and ones or as binary values. Those binary values can be taken in any order of rows like first, second, third or first, third, second. The values of the first table are pixel values of the input image captured. The LBPH calculation utilizes the histogram of the LBP trademark range as the component vector for characterization. It partitions an image into a few sub districts, at that point removes LBP highlight from every pixel of the sub-locale, setting up a measurable histogram of the LBP trademark range in each sub area, with the goal that each sub district can utilizing a factual histogram to depict the entire picture through various factual histogram segments.

4.3 HISTOGRAMS:

The histogram is nothing but the graphical representation. But here the histograms are generated for each region of the pixel which is extracted feature from the input image. The grid x and grid y the grayscale image is divided for that histogram is generated for each region, at last the histograms created are concatenated so as to develop the huge graph for the image. The histogram development how it happens step by step can be referred from the below image.

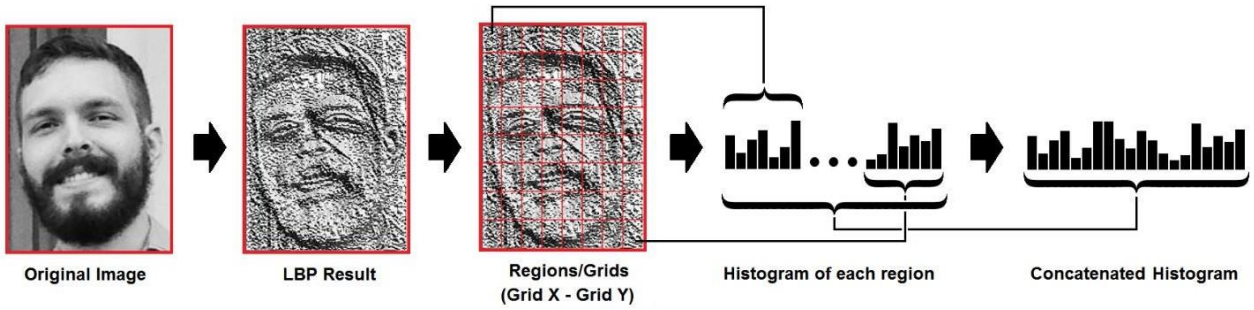


Figure 4.2: Histogram creation

4.4 FACE RECOGNITION:

To perform the face recognition, the algorithm should be already trained. The histogram each used to represent each picture from the training data. So to discover the picture that coordinates the information picture we simply need to look at two histograms and return the picture with the nearest histogram. We can utilize different ways to deal with look at the histograms (ascertain the separation between two histograms), for instance: Euclidean distance, chi-square, outright worth, and so on. So the calculation yield is the ID from the picture with the nearest histogram. The formula ought to conjointly come the calculated distance, which might be used as a 'confidence' measuring. Note: don't be fooled regarding the 'confidence' name, as lower confidences area unit higher as a result of it suggests that the space between the 2 histograms is nearer.

4.5 ALGORITHM:

To perform the face acknowledgment framework here the Local Binary Pattern Algorithm has been applied. The LBP administrator is utilized in nearby highlights through Local Binary Pattern acts which abbreviate the neighbourhood uncommon plan of a face picture. The LBP administrator is the quantity of twofold proportions of pixels powers inside the pixel of revolve and it's around eight pixels. The flowchart depicts the clear observation of the algorithm that how and what and are all

included in the algorithm, how the rules are indicated for each phase and flow of for the face recognition.

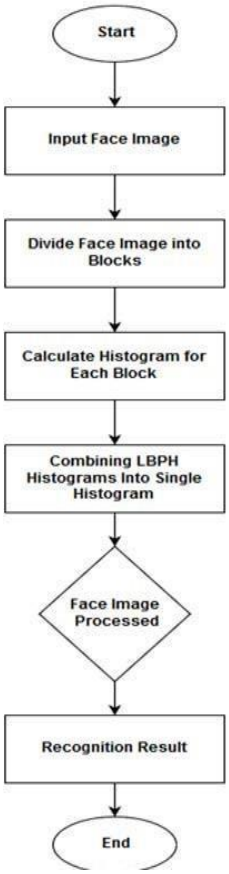


Figure 4.3: Algorithm Flowchart

The LBPH algorithm has a particular order in which it has go or to procedure it has to follow so as to get the efficient result for the input image.

The below steps shows how the LBPH algorithm actually flows in step by step manner:

1. Initially, we have to begin with temp=0

2. Where I, is the preparation for each picture

3. H=0,then Initialize the example histogram

4. Ascertain the model name of LBP

5. Continue including the relating canister by 1.

6. Get the best LBP include during each face picture and afterward converging into the one of a kind vector.

7. It's an ideal opportunity to think about the highlights.

8. At long last, in the event that it looks like with the put away database the picture is perceived.

4.6 Working Model

The new users should complete the registration. The registration process involves taking the face data of user. The unique Identification (ID) will be provided to the particular uses during the registration process. The collected user face data and the unique ID will be stored in the data base. The registered merchants will have a device to scan the face of the customer's .The users or payer just has to show his/her face to the device which will scan the face. User will be used to take the input of the face of the payer or customer. Then the user should enter their unique ID which they got during registration. Initially, set up the face database, and afterward, remove the LBP surface highlight afters of each test picture. At long last, arrange and perceive the face data. We contrast the info face pictures and database face pictures and work as though the given appearance pictures, after removing highlights contrasted and the dataset so at last, we can make sense of the face picture is well perceived in any case the face picture would not be perceived.

The Input of face from the device and the unique ID which the user entered will be checked in the database. If the face is matched with the data of the database and the unique ID entered by the user are same as that of the unique ID of the face that are in the database then the transaction will be processed to further process. If the input from the device didn't match with any face data in the database or If the face got detected and the unique ID that the user entered didn't match then the transaction will be failed and the process will be start from the first phase.

If the input and the data from the database matched then the user will be asked to enter the amount for transaction or the amount will be entered by the merchant. If the entered amount is exceeded the available balance in the account than the user will be informed with the message "amount should be less than or equal to the balance" or "insufficient balance". If the entered amount is less than or equal to available balance the transaction will be further processed. If the entered amount is less than 10000 or any specified amount then the transaction will be further processed. If the entered amount is more than specified amount the One Time Password (OTP) will be sent to the

user registered number later the user will be asked to enter the OTP. OTP will be used for extra layer of security so that the unauthenticated users cannot get more than the specified amount even if the attackers gain the access by cracking the face authentication layer and even if he know the unique ID of the user. The system will be secure even without OTP but using OTP will provide extra factor of authentication for the payment system. If the entered OTP is valid then the transaction will be further processed. If the user enters the wrong OTP then the user will be alerted and asked to re-enter the OTP again. If the user enters the wrong OTP three times continuously or any 3 wrong attempts before successful transaction in time span of 24 hours then the user's account will be blocked for 24 hours. This step will prevent the gaining access to the pin by brute force attacks or guessing the OTP by the attacker. If the OTP is used as alpha numeric it will be even more secured than that of numeric OTP. As it is highly impossible to brute force an alpha numeric OTP.

When the user enters the OTP it will be checked by the system and if the OTP is valid then the user will be asked to enter his Personnel Identification Number (PIN). If the PIN entered by the user matched with his account in the database then transaction will be successful. If the user enters the wrong PIN three times continuously then the user's account will be blocked for 24 hours.

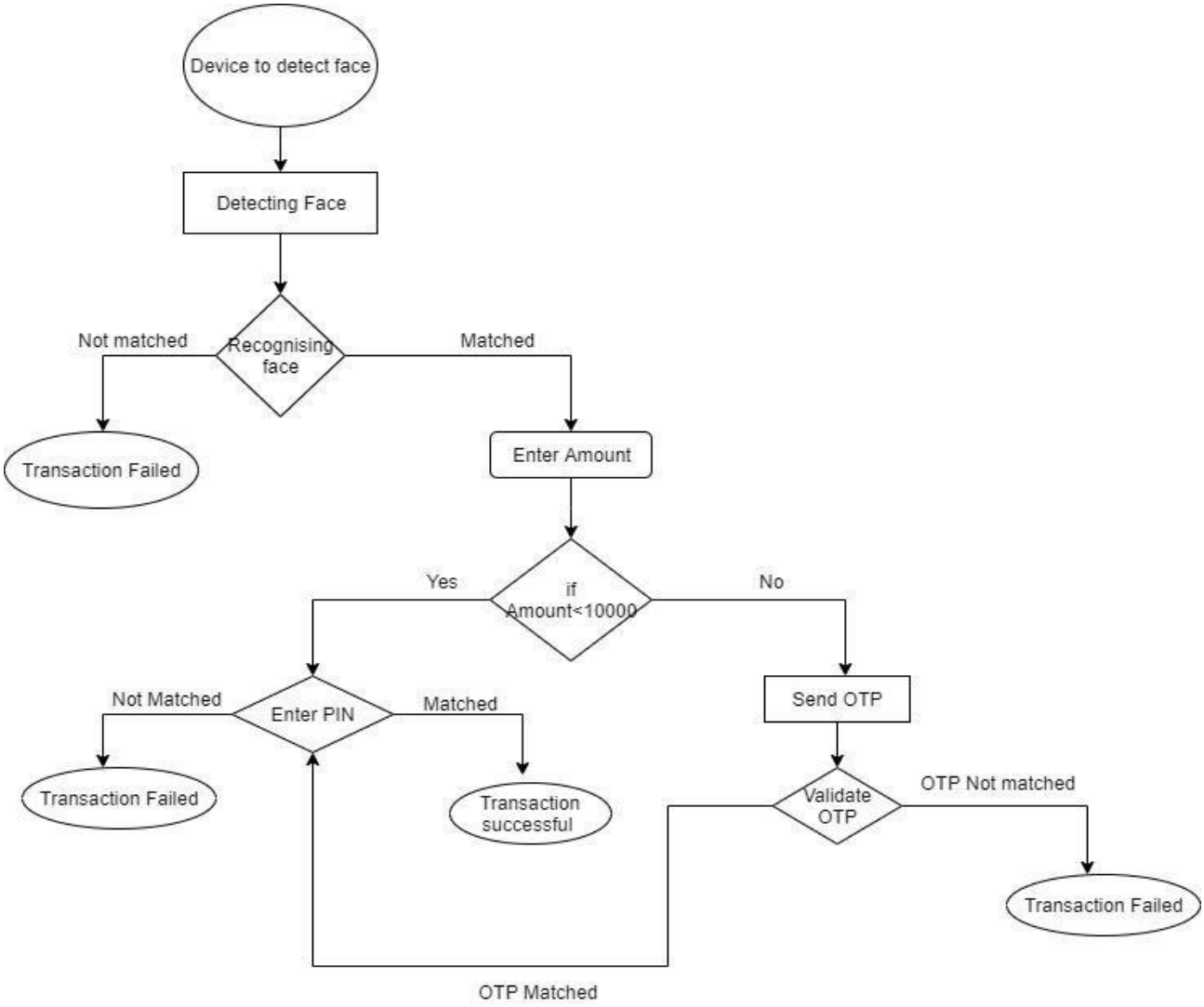


Figure 4.4: System Architecture

CHAPTER 5

OVERVIEW OF TECHNOLOGIES

CHAPTER 5
OVERVIEW OF TECHNOLOGIES

5.1 Software and hardware specifications:

Programming necessity Specification is a crucial record, which frames the establishment of the product improvement process. It records the prerequisites of a framework as well as has a depiction of its significant component. A Software prerequisite Specification is essentially an association's understanding recorded as a hard copy of a client or potential customer's framework necessities and conditions at a specific point in time as a rule before any genuine structure or improvement work. It's a two-way protection strategy that guarantees that both the customer and the association comprehend different prerequisites from that viewpoint at a given point in time. The Software prerequisite Specification additionally works as a diagram for finishing an undertaking with as meagre cost development as could be expected under the circumstances. The Software necessity Specification is frequently alluded to as the "parent" record since all resulting venture the executives reports, for example, structure determinations, articulations of work, programming design particulars, testing and approval plans, and documentation plans, are identified with it. Note that a Software necessity Specification contains utilitarian and non-useful prerequisites just; it doesn't offer structure recommendations, potential answers for innovation or business issues, or some other data other than what the advancement group comprehends the client's framework prerequisites that has to be.

5.2 Purpose of Software Requirement specification:

This Program Framework Specification incorporates a total diagram of both the highlights and parameters of the "Distinguishing proof of least and jug neck hubs to extend the life expectancy of the system." It likewise characterizes the non-practical determinations, for example, time breaking point, dependability and giving over disappointment and so forth. It additionally centers around the System's planned users. This enrols the ends made for future usage; the framework must be executed with programming and equipment.

5.2.1 Specific Requirements

This section provides details about the functionality expected by the system. Also, it specifies the constraints considered in providing such functionality.

- Goals are achieved through use cases.
- Use cases are enabled by functional requirements.
- Functional requirements lead to design and implementation
- Non-functional requirements characterize how functional requirements must work

- Constraints restrict how functional requirements may be implemented.

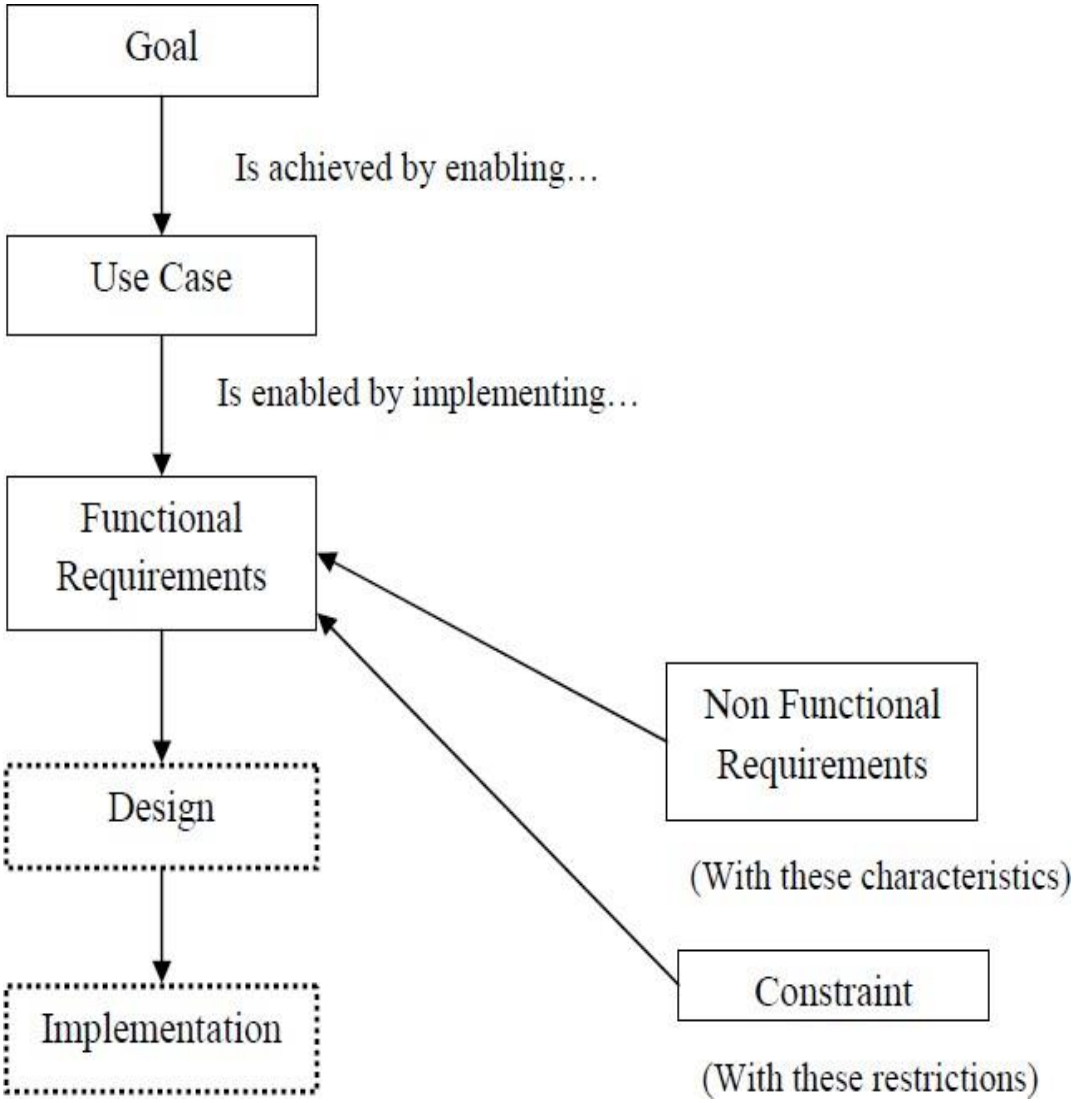


Figure 5.1: Software Requirements

5.3 Hardware and Software Requirements

Equipment rundown of the face recognition and digital payments system depend on the client. If there should arise an occurrence of retailers they ought to have the gadget which comprise of camera that perceives the essence of the client. The fast internet is required to process the exchanges rapidly. The gadget ought to likewise comprise of keypad to enter the OTP if the amount entered is more that specified limit and PIN for authentication .

Software or packages that are need to be imported to the program are:

1. Numpy
2. Opencv2
3. OS
4. PIL
5. PIP

1. Numpy:

NumPy is a library for the Python programming language, adding support for large, multi-dimensional arrays and matrices, along with a large collection of high-level mathematical functions to operate on these arrays. It is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays. It is the fundamental package for scientific computing with Python. It contains various features including these important ones:

- A powerful N-dimensional array object
- Sophisticated (broadcasting) functions
- Tools for integrating programming languages
- Useful linear algebra
- Fourier transform
- It has random number capabilities

NumPy, which represents Numerical Python, is a library comprising of multidimensional array objects and an assortment of schedules for handling those clusters. Utilizing NumPy, scientific and coherent procedure on exhibits can be performed.

Besides its obvious scientific uses, Numpy can also be used as an efficient multi-dimensional container of generic data. Arbitrary datatypes can be defined using Numpy which allows Numpy to seamlessly and speedily integrate with a wide variety of databases.

Numpy will be imported to the programming language.

Syntax: import numpy

Example: import numpy as np

2.OpenCV2

OpenCV (Open Source Computer Vision Library) is a library of programming capacities for the most part focused on constant PC vision. Initially created by Intel, it was later upheld by Willow Garage then Itseez which was later gained by Intel. The library is cross-stage and free for use under the open-source BSD permit.

OpenCV-Python is a library of Python ties intended to tackle PC vision issues. cv2.imread() technique stacks a picture from the predefined document. In the event that the picture can't be perused (in light of missing record, ill-advised consents, unsupported or invalid arrangement) at that point this strategy restores a vacant network.

Python is a universally useful programming language began by Guido van Rossum that turned out to be famous rapidly, predominantly on account of its straightforwardness and code intelligibility. It empowers the developer to communicate thoughts in less lines of code without decreasing comprehensibility.

OpenCV (Open Source Computer Vision Library) is an open source PC vision and AI programming library. OpenCV was worked to give a typical foundation to PC vision applications and to quicken the utilization of machine discernment in the business items. Being a BSD-authorized item, OpenCV makes it simple for organizations to use and change the code.

The library has more than 2500 enhanced calculations, which incorporates a far reaching set of both exemplary and best in class PC vision and AI calculations. These estimations can be used to recognize and see faces, recognize objects, bunch human exercises in chronicles, track camera advancements, track moving articles, remove 3D models of things, produce 3D point mists from sound system cameras, join pictures together to create a high goals picture of a whole scene, find comparable pictures from a picture database, expel red eyes from pictures taken utilizing streak, follow eye developments, perceive landscape and set up markers to overlay it with enlarged reality, and so forth. OpenCV has in excess of 47 thousand individuals of client network and evaluated number of downloads surpassing 18 million. The library is utilized broadly in organizations, examine gatherings and by administrative bodies.

OpenCV-Python utilizes Numpy, which is an exceptionally improved library for numerical tasks. All the OpenCV exhibit structures are changed over to and from Numpy clusters. This additionally makes it simpler to coordinate with different libraries that utilization Numpy.

OpenCV presents another arrangement of instructional exercises which will manage you through different capacities accessible in OpenCV-Python. This guide is chiefly centred around OpenCV 3.x form (albeit the majority of the instructional exercises will likewise work with OpenCV 2.x).

Earlier information on Python and Numpy is suggested as they won't be shrouded in this guide. Capability with Numpy is an unquestionable requirement so as to compose improved code utilizing OpenCV-Python.

OpenCV will be imported to the programming language.

Syntax: import cv<version>

Example: import cv2

3.OS

The OS module in Python gives a method for utilizing working framework subordinate usefulness. The capacities that the OS module furnishes permits you to interface with the hidden working framework that Python is running on – be that Windows, Mac or Linux.

The OS module in python furnishes capacities for cooperating with the working framework. Operating system, goes under Python's standard utility modules. This module gives a compact method for utilizing working framework subordinate usefulness. The *os* and *os.path* modules incorporate numerous capacities to interface with the document framework.

Syntax: import OS

4.PIL

PIL(Python Imaging Library) is a free library for the Python programming language that includes support for opening, controlling, and sparing a wide range of picture document designs. It is accessible for Windows, Mac OS X and Linux. The most recent variant of PIL is 1.1.x, was discharged in 2009 and underpins Python 1.5.x–2.x, with Python 3 help to be discharged later.

Improvement seems, by all accounts, to be stopped with the last focus on the PIL store coming in 2011 Consequently, a replacement venture called Pillow has forked the PIL archive and included Python 3.x help. This fork has been embraced as a substitution for the first PIL in Linux appropriations including Debian and Ubuntu.

Syntax: from PIL import <package>

Example:

from PIL import Image

from PIL._imaging import font

5.PIP

PIP is an accepted standard bundle the board framework used to introduce and oversee programming bundles written in Python. Numerous bundles can be found in the default hotspot for bundles and their conditions — Python Package Index (PyPI). Most dispersions of Python accompany pip preinstalled. Python 2.X and later on the python2 arrangement, and Python 3.x and later incorporate pip pip3 for Python 3 as a matter of course.

First presented as pyinstall in 2008 by Ian Bicking the maker of the virtualenv bundle as an option to easy_install, pip was picked as the new name from one of a few proposals that the maker got on his blog entry. As per Bicking himself, the name is an abbreviation for "Pip Installs Packages". In 2011, the Python Packaging Authority PyPA was made to assume control over the upkeep of pip and virtualenv .

Syntax: from PIP import <package>

Example: from pip._vendor.distlib.compat import raw_input

5.3.1 Hardware Requirements

- RAM: 4GB and Higher
- Processor: Intel i3 and above
- Hard Disk: 500GB: Minimum
- Web cam

5.3.2 Software Requirements

- OS: Windows or Linux
- Python IDE: python 3.5
- Setup tools to be installed for 3.6 and above
- pip to be installed for 3.6 and above
- Language: Python Scripting

CHAPTER 6

IMPLEMENTATION

CHAPTER 6
IMPLEMENTATION

6.1 LBPH ALGORITHM

The Local Binary Pattern Histogram (LBPH) algorithm is used for face recognition as it provides good results. For this firstly the image has to be stored, this process involves as the input is given which must be in image / video format from that the face is detected then the face extraction is to be done and now the face recognition occurs. The images can affected while recognising, this can happen due to cameras position or the movement of face of a person and the environment conditions should be good while storing / recognising the face as those may leads to the bad image recognition as the bad image will not give the good result. Now the output is also in image / video format. The LBPH algorithm is simple and it used as based on the pixels of an image and is very effective as the Local Binary Pattern uses the neighbour pixels in calculating the histogram. The other face algorithms are of much similar but this LBPH is very different from other techniques. The LBPH is one of the methods that greatly detect the liveness of the face detection so in case a picture/ photo is placed it cannot proceed further.

6.2 USE CASE DIAGRAM:-

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses as shown in the below figure.

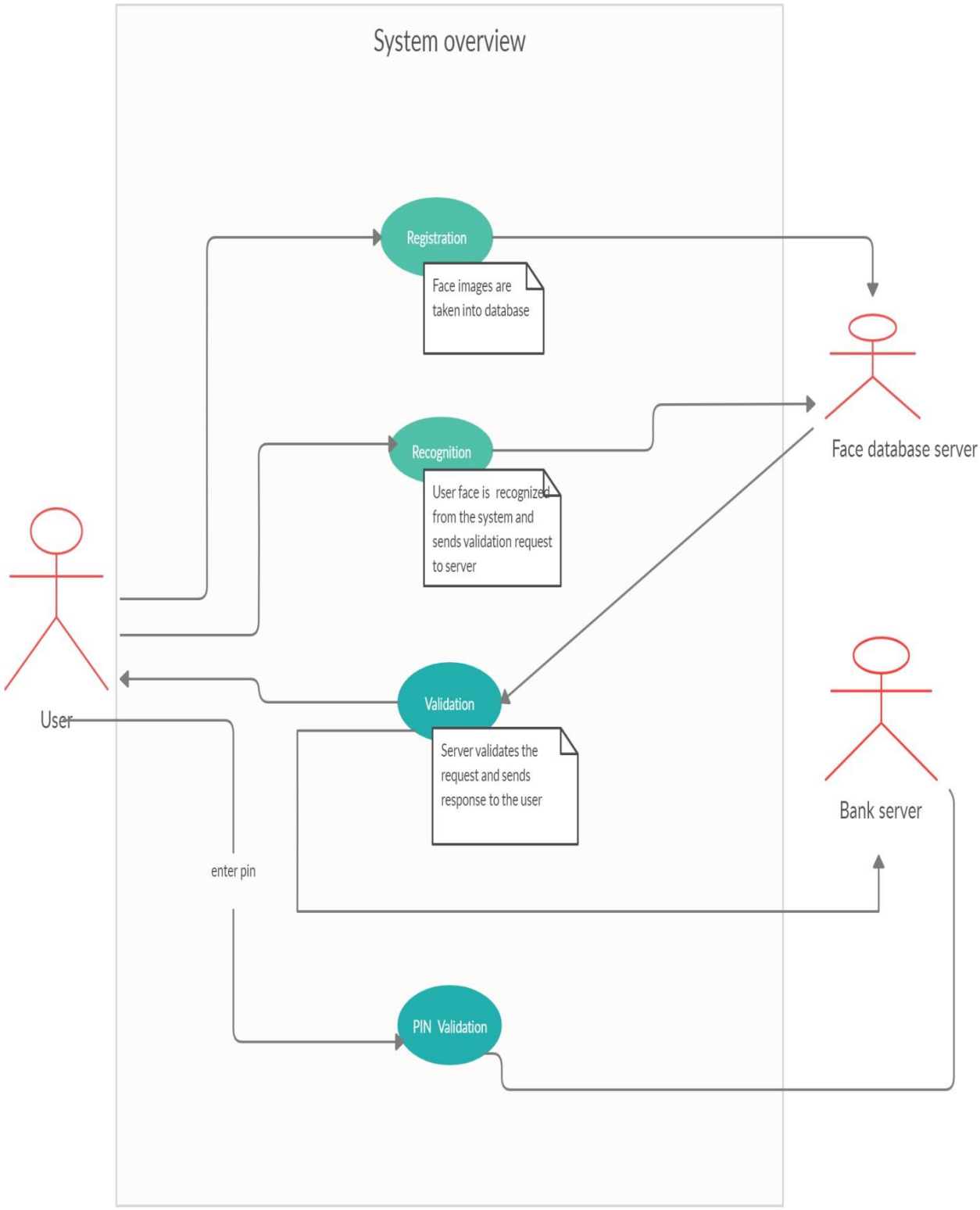


Figure 6.1: Use case diagram

The figure represents the overview of the payment system which uses the face recognition for the payment process.

Initially the user should register. While registration the user face data is collected and stored the data base.

Whenever the user needs to pay using face recognition .The user face is recognized using the system it matches with the face data from face database ,validates the face data and send response to the user and the Bank server for payment. Next step is PIN validation where the user should enter pin ,after the validation it undergoes with the bank payments processing.

6.3 ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams are intended to model both computational and organizational processes (i.e., workflows), as well as the data flows intersecting with the related activities. Although activity diagrams primarily show the overall flow of control, they can also include elements showing the flow of data between activities through one or more data stores.

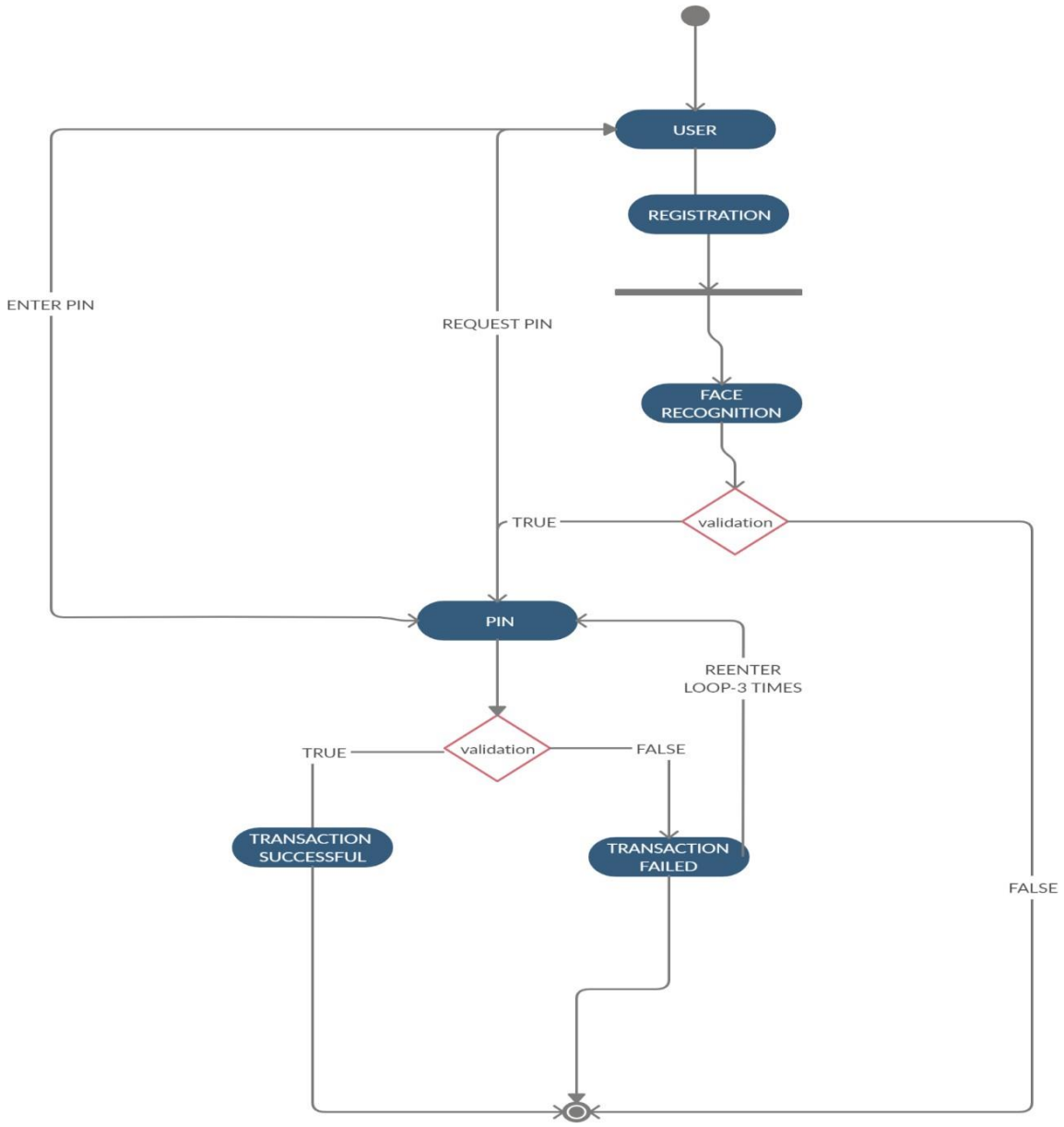


Figure 6.2. Activity diagram

STEP by STEP PROCESS:

1. Begin
2. input: persons face
3. output : matching face with ID
4. Method : LBPH
5. Histogram: Face features graph
6. Capture from camera and convert in to grayscale
7. Crop only face of person
8. Face size is of 300*300
9. Extracting the features

10. Folder with Unique ID is created to store faces.
11. Transform grayscale image to concatenated histogram
12. Input of face from camera and ID
13. Extract features and prepare histogram
14. Euclidean distance is calculated
15. Calculate confidence
16. Based on the confidence provides output face or output will be unknown
17. User Id is obtained from the matched face data and undergoes payment process.
18. End

6.4 CAPTURE FACE DATA:

Local Binary Pattern Histogram uses four parameters they are radius, neighbours, Grid X, Grid Y. The LBPH algorithm is used in the following manner:

First the input, in this the face is recognised and cropped, and then the image is divided into 3x3 pixels. One important thing here is the image captured will be in grayscale format so the each pixel range will be of 0~255.

6.5 STORE FACE DATA:

This cropped images is stored in the data base with id which is used for the uniquely identification of an user. These cropped images are further used for training the data for recognition.

6.6 CONVERTING INTO BINARY:

From this the central pixel value in the matrix is used as a threshold value. This threshold value is used for the other neighbours by defining the new values. The threshold value is used in this way for allocation of binary values (0 / 1) to the neighbours based on their pixel value. If the neighbour pixel value is greater than or equal to the threshold value then the pixel is set as value 1 and if neighbour pixel value is less than threshold value then the pixel is set as value 0.

- Now the 3x3 contains the binary values leaving the centre value (threshold value). All binary values are combined one after the other that generates a sequence of binary values ignoring the central value as it is a threshold value.

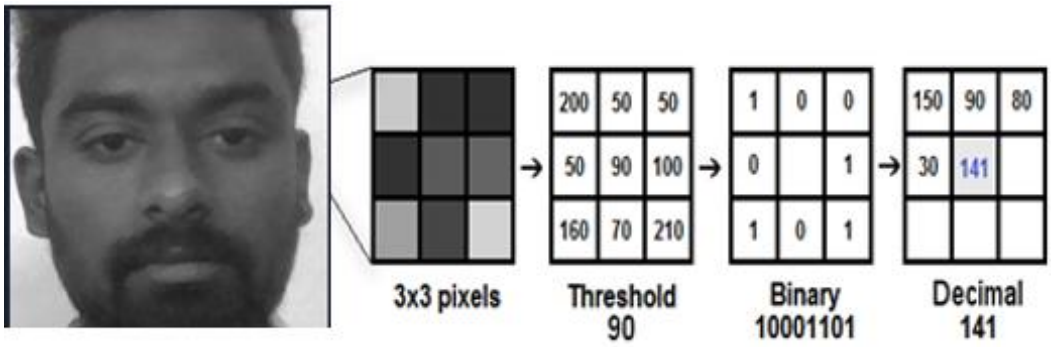


Figure 6.3: Conversion from Binary to Decimal

6.7 HISTOGRAM GENERATION:

The binary values are considered and convert into decimal value and it is allocated for the central value of the 3x3 matrix, as it is the original pixel of the input image. Extracting histograms is the important thing in this algorithm as we are matching the face based on the histogram of the region. Histogram is generated for the previously produced image.

- Histogram is produced by taking the values of third and fourth parameter as mentioned earlier (Grid X and Grid Y), by using those two the image is divided into grids, as the image is in grayscale format histogram of each grid will be having positions of range (0 ~ 255) which represents the intensity of each pixel.

- At the end of image we have to combine histograms of each matrix to generate new and big histogram. The last histogram returns the characteristics of the original image. Face recognition can be done after training the dataset which created for multiple images.

6.8 FACE DETECTION AND RECOGNITION:

• The face recognition will works as the input is given and algorithm generates the histogram of the image The histograms are compared by using the Euclidean distance formula. The input is the user face, which is detected from the camera and under goes the LBPH algorithm and compares the histogram, If the Euclidean distance of the histograms is less the image is very close to the input image and returns the image with very closest histogram one. (i.e. image matches with the input image) then the output will be image with closest histogram .Thus the face is recognized from the existing database. The closest histogram image Id is obtained and used for the further payment process.

CHAPTER 7

RESULTS AND DISCUSSIONS

CHAPTER 7
RESULTS AND DISCUSSIONS

The experiments has been performed to check the proposed system showing the face with correct ID or not. Here, various images are processed with the help of face recognition. Our testing for the pictures clearly depicts that the algorithm has been worked well on the face dataset detection and recognition. The results we received from the implementation of the algorithm are describes in this section. The screenshots has been taken while implementing the algorithm and creating dataset, how the dataset will be present and how the output will be displayed. Here are the following figure that clearly shows the extraction of image and displaying the output.

7.1 Working

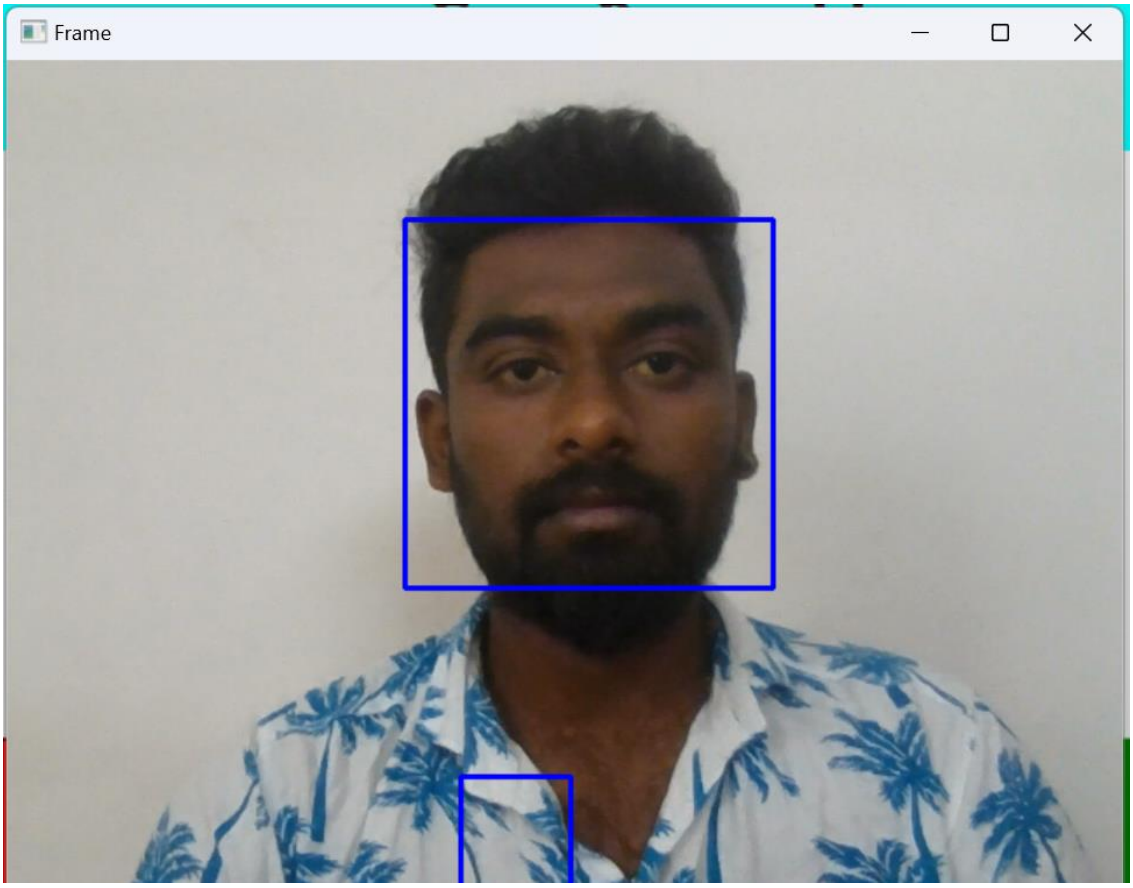


Figure 7.1: Capturing data

The above figure is to explain that how the camera is taking the pictures in order to store images at the dataset. The green colour box is the one biggest proof that the algorithm focuses on only the face of the person, though the camera is in normal RGB format which means of colour pictures. Those are converted into grayscale images.

7.2 Grayscale Image

Figure 7.2. Actual grayscale image

This is one of the sample image how the grayscale image looks like rather that of normal images.

7.3 Dataset

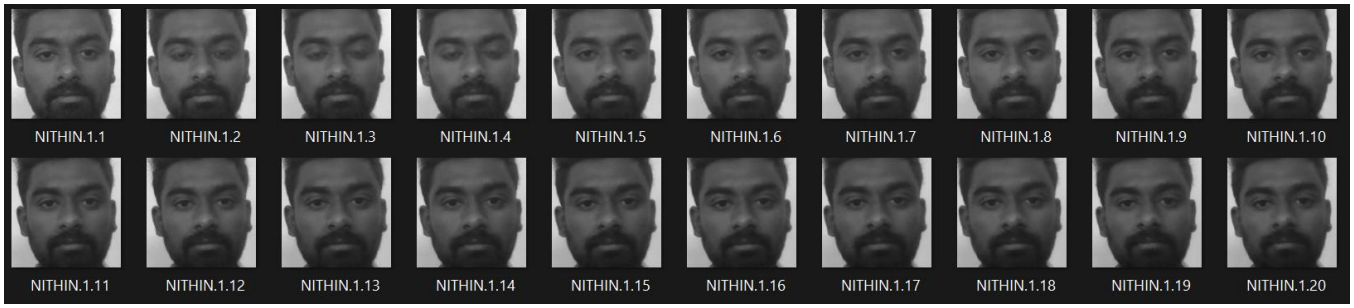


Figure 7.3. Dataset

The above list of images are the samples for how the dataset will be present in a folder of that ID of only one person's face. There will be presence of more persons data, to get the better result we may consider the fast computing computer or the database that can store the faces and should return the value based on the histogram from the database.

7.4 Input Testing

Figure 7.4. Grayscale image from input

• As shown above the algorithm detects the face and stores the face image at the dataset which we create at the beginning or we have to specify the location, where all the images should be stored. This data set is used for the process of recognition. The dataset maybe of large in size but using the ID will become easy for the transactions. As ID plays a vital role in the recognition part, when the user enters the ID then the system goes to the particular ID location for the recognition and for further process.

7.5 Testing Results

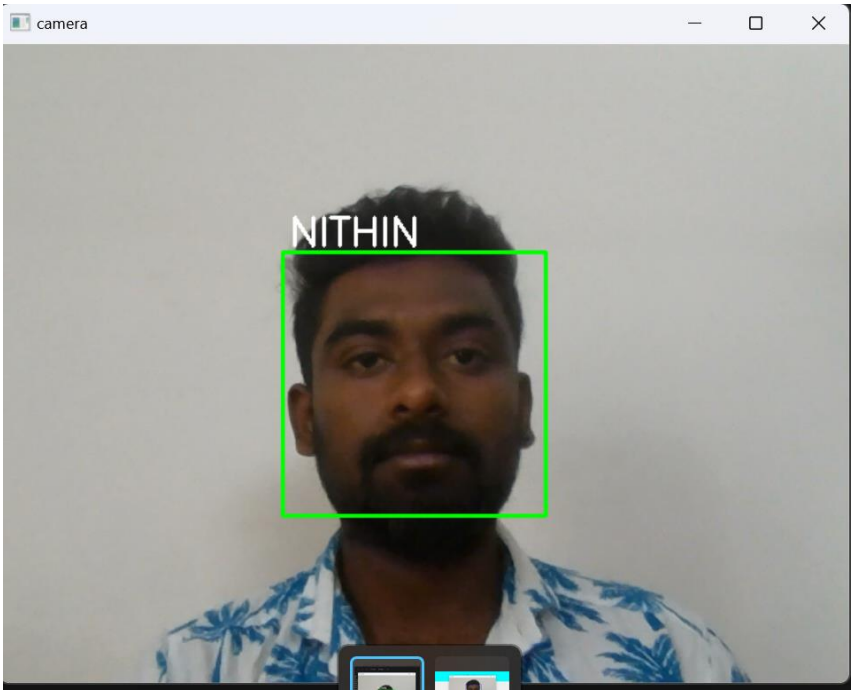


Figure 7.5. Grayscale image which matches with histogram as output

• It is showing the ID that matches with the histogram values in the dataset / database. If an unauthorized person tries to match with other person it will shows as Unknown, otherwise it will catch the ID and then it tries to match the face, if it matches then it goes for the further transaction process.

CHAPTER 8

CONCLUSION

CHAPTER 8

CONCLUSION

This system provides the better and secured online transactions. This will help at the all retail shops or in malls because, after customer purchasing the materials they tend for the easy payment. So this delivers the easy and fast payment using the facial recognition that will directly connects to the customer account and from that the transaction occurs with secure and fast. Both the customers and the merchants will be benefited from this system. Further enhancement we can implement in the ATM's also with changes in ATM's.

9. REFERENCES

[1] B. Rajendran, A. K. Pandey and B. S. Bindhumadhava, "Secure and privacy preserving digital payment," 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, 2017, pp. 1-5.

[2] https://qz.com/india/1746910/cashless-payments-growing-faster-in-india-than-almost-anywhere-else/

[3] **S**ecurity of Mobile Payments and Digital Wallets, ENISA December 2016, https://www.enisa.europa.eu/publications/mobile-payments-security/at_download/fullReport.

[4] J. Ueda and K. Okajima, "Face morphing using average face for subtle expression recognition," 2019 11th International Symposium on Image and Signal Processing and Analysis (ISPA), Dubrovnik, Croatia, 2019, pp. 187-192. doi: 10.1109/ISPA.2019.8868931

[5] U. Park, Y. Tong and A. K. Jain, "Age-Invariant Face Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 5, pp. 947-954, May 2010.

[6] E. Husni and A. Ariono, "Development of integrated mobile money system using Near Field Communication (NFC)," 2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA), Kuta, 2014, pp. 1-6.

[7] Surekha. R. Gondkar, Saurab. B, C. S. Mala, "Biometric Face Recognition Payment System," 2018 International Journal of Engineering Research & Technology (IJERT), Volume 6, Issue 13, 2018, pp.1-6.

[8] S. Nair, S. K. Khatri and H. Gupta, "A Model to Enhance Security Of Digital Transaction," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2019, pp. 17-21.

[9] K. Patel, H. Han and A. K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2268-2283, Oct. 2016.

[10] A. Ahmed, J. Guo, F. Ali, F. Deeba and A. Ahmed, "LBPH based improved face recognition at low resolution," 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, 2018, pp. 144-147.

[11] X. Zhang, K. Jing, Y. Dai and X. Xu, "Face Biometric Identity Authentication System," 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 2018, pp. 1473-1477.

[12] https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b