THIRD GENERATION ATM USING ADVANCE IMAGE PROCESSING

A PROJECT REPORT

Submitted by

GOKULAKRISHNAN V	**820319104017**
SATHISH S	**820319104037**
VISHWA VENGADESH D	**820319104048**
TAMILSELVAN S	**820319104303**

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

A.V.C. COLLEGE OF ENGINEERING, MAYILADUTHURAI

MANNAMPANDAL – 609 305

ANNA UNIVERSITY, CHENNAI – 600 025

MAY 2023

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report **"THIRD GENERATION OF ATM MACHINE USING ADVANCED IMAGE PROCESSING"** is the bonafide work of **GOKULAKRISHNAN V (820319104017), SATHISH S (820319104037), VISHWA VENGADESH D (820319104048), TAMILSELVAN S (820319104303)** who carried out their project work under my supervision.

SIGNATURE	**SIGNATURE**
Dr. S. PADMAPRIYA, M.E, Ph.D.,	**A. ARUNPANDIYAN, M.E.,**
PROFESSOR & HEAD	**SUPERVISOR**
	Assistant Professor
Department of CSE	Department of CSE
A.V.C College of Engineering	A.V.C College of Engineering
Mayiladuthurai	Mayiladuthurai
Mannampandal-609 305	Mannampandal-609 305

EXAMINED ON:

INTERNAL EXAMINER | **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people, and we are extremely fortunate to have this all along the completion of my project work. Whatever we have done is only due to such guidance and assistance and we would not forget to thank them.

We extend our deep gratitude to our Administrator **Justice Mr.K.VENKATARAMAN** for the words of wisdom. We extend our deep gratitude to our Management. We are sincerely obliged to our respected Principal **Dr. C. SUNDAR RAJ, M.E., Ph.D.,** who has always been a constant source of inspiration.

We express our respectful thanks to **Dr. S. PADMAPRIYA, M.E., Ph.D.,** the Professor and Head of our Department for her kind and mutual aid to complete our project.

At this juncture we feel deeply honoured in expressing our sincere thanks to our project guide **Mr. A. ARUNPANDIYAN, M.E.,** Assistant Professor in our department, who took keen interest on our project work and guided us all along, till the completion of our project work by providing all the necessary information for developing a good system.

We heartily thank our project coordinator **Dr. K. KRISHNAKUMARI, M.E., Ph.D.,** of our department for providing us all the facilities and suggestions during this project work. We are also thankful all the review committee members for their valuable suggestions given in all reviews.

We are thankful to and fortunate enough to get constant encouragement, support and guidance from all **Teaching staff members** of our department which helped us in successfully completing our project work. Also, we would like to extend our sincere regards to all the **non-teaching staff members** of our department for their timely support.

Finally, we express our heartfelt gratitude to our **Parents and Friends** who had encouraged us in successful completion of our project and people who have willingly helped us out with their abilities.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO

ABSTRACT

Automated teller machines (ATMs)are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. For example, ATMs are typically found in restaurants, ,Convenience stores, malls, schools, gas stations, supermarkets hotels, work locations, banking centre's, airports,entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry week for this purpose we are using face recognition step with haar cascade classifier to find out the features of face. When face is detected then it will give access to do transactions otherwise not allow.

Keywords – Haar cascade, Automatic Teller Machine, Annaconda (PROMPT, NAVIGATOR), Machine learning,

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Third Generation ATM Machine

A computer-implemented method for cardless use of an automated teller machine (ATM) is provided. The method includes receiving as an input, a user-identified ATM that the user wishes to use. The method also includes generating and transmitting a one-time password (OTP) for the user to enter at the identified ATM. The method further includes receiving and verifying the OTP entered into the ATM, and on successful verification, authorizing access to services available through the ATM, without use of a card. to reduce the threat involved in ATM machines that were installed in remote area, also the issue related to fraudulent sale like misusing others card to withdraw plutocrat and etc. So in order to overcome these challenges, we've developed result that will work the ML & AI to circumscribe card access to only the authorized druggies those are linked by face recognition algorithm.

This method is useful in many fields such as the military, for security, schools, colleges and universities, airlines, banking, online web applications, gaming etc. this system uses powerful python algorithm through which the detection and recognition of face is very easy and efficient.

Surveillance cameras are an essential security precaution in all public places. In a centralized surveillance system, videos collected from different cameras are stored in a centralized server. If any security threat is caused by the presence of an individual in a particular place, the law enforcing team will have to identify the current location of the particular person involved in the event as early as possible. Though the videos collected from surveillance cameras help to identify the person's presence in a location, checking the person of interest from a large collection of videos is a herculean task if it is done manually. The complexity of the task depends on the number of cameras involved in the surveillance process. Deep Learning-based video analytics can help us to automate this identification task. Deep Learning is a powerful tool to do image classification.

1.2 Difference between physical ATM Card and Face recognition

Physical ATM cards and face recognition ATM machines each have their own advantages and disadvantages. Here are some key differences between the two:

1. **Convenience** A face recognition ATM machine eliminates the need for a physical ATM card, making it more convenient for users who may forget their cards or prefer not to carry them. On the other hand, physical ATM cards can be used at any ATM, whereas a face recognition ATM machine may only be available at specific locations.
2. **Security** Physical ATM cards can be lost or stolen, which can result in unauthorized access to the user's account. In contrast, face recognition ATM machines provide an additional layer of security as users need to be authenticated by their facial features. However, there is still a risk of facial recognition technology being spoofed or hacked.
3. **Reliability** Physical ATM cards rely on magnetic stripes or chips, which can wear out or become damaged over time. Face recognition ATM machines, on the other hand, are reliant on advanced software and hardware which can also fail due to technical issues or maintenance requirements.
4. **Cost** Implementing a face recognition ATM machine can be expensive as it requires the installation of advanced cameras, software, and databases. Physical ATM cards, however, are relatively cheap to produce and distribute.

5. **Accessibility** Physical ATM cards can be used by individuals with physical disabilities or impairments that may affect their ability to use facial recognition technology. Face recognition ATM machines may have to provide alternative methods of authentication, such as PIN codes or voice recognition.

In summary, face recognition ATM machines can provide added convenience and security compared to physical ATM cards, but at a higher cost and potential limitations. Ultimately, the choice between the two would depend on the user's preferences, the bank's resources and priorities, and the availability of technology.

1.3 Uses of an Automated Teller Machine

Automated Teller Machines have revolutionized the banking sector by providing easy access to customers and loading off the burden from bank officials. Some of the uses of an ATM are the most common uses of an Automated Teller Machine include withdrawing money, checking balance, transferring money, or changing the PIN (Personal Identification Number). Newer and advanced ATMs also provide options to open/withdraw a Fixed Deposit (FD), or to apply for a personal loan. You can also book railway tickets, pay the insurance premiums, income tax & utility bills, recharge mobile, and deposit cash. Some of these facilities require you to register at the bank branch• Customers can now do money transactions at their convenience. ATMs today are installed in public spaces, highways, malls, market places, railway/airport stations, hospitals, etc.• Automated Teller Machines provide 24×7 access anywhere• ATMs help to avoid the hassle of standing in long queues at the bank even for simpler transactions like withdrawing money. It has also helped in reducing the workload of the bank officials.

1.4 ATM Fraud

Over the last two decades, automated teller machines (ATMs) have become as much a part of the landscape as the phone booths made famous by Superman. As a result of their ubiquity, people casually use these virtual cash dispensers without a second thought. The notion that something could go wrong never crosses their minds. Most ATM scams involve criminal theft of debit card numbers and personal identification numbers (PINs) from the innocent users of these machines. There are several variations of this confidence scheme, but all involve the unknowing cooperation of the cardholders themselves. ATM fraud is described as a fraudulent activity where the criminal uses the ATM card of another person to withdraw money instantly from that account. This is done by using the PIN.

Skimming This type of ATM scam involves a skimmer device that criminals place on top of or within the card slot. To record your PIN number, the criminals may use a hidden camera or an overlay that covers the original PIN pad. Using the card numbers and PIN's they record; thieves create duplicate cards to withdraw money from consumers' accounts. Unlike losing your debit card or having it stolen, you won't realize anything is amiss until unauthorized transactions take place. Take a look at these so you know how to detect ATM skimmers.

Shimming This is the latest update to skimming. Instead of reading your card number, criminals place a shimming device deep inside the ATM to record your card's chip information. The end result is the same as skimming because thieves use the stolen chip data to create "cloned" versions of your debit card.

Card trapping This is a type of ATM security attack, where the cyber- criminals trap a user's credit or debit card to obtain the card details. The criminals install a device inside the card acceptance slot of an ATM to trap the ATM cards.

CHAPTER 2

LITERATURE SURVEY

[2] ATM Security System Modeling Using Face Recognition with FaceNet and Haar Cascade.

ATM or Automated Teller Machines are widely used by people nowadays. The existing conventional ATM is vulnerable to crimes because of the rapid technology development. A total of 270,000 reports have been reported regarding credit card fraud and this was the most reported form of identity theft in 2019. A secure and efficient ATM is needed to increase the overall experience, usability, and convenience of the transaction at the ATM. To provide better security for the conventional ATM, this paper proposed a face recognition system using FaceNet combined with Haar Cascade Classifier. Haar Cascade is used to detect the haar features based on the face features and stored to the FaceNet model as the face recognition model. The scale factor from the Haar Cascade is also modified a few times to get a better accuracy and processing time. With the proposed method, the Personal Identification Number (PIN) will be replaced by face recognition. Every time the customers insert their card, the system will detect and start to identify the face. If it does not match, the card will be blocked. This research uses the Face Recognition Dataset from Kaggle. By using this dataset, the proposed system achieves the highest accuracy with 90.93%.

[1] Analyzing the noise robustness of deep neural networks.

Adversarial examples, generated by adding small but intentionally imperceptible perturbations to normal examples, can mislead deep neural networks (DNNs) to make incorrect predictions. Although much work has been done on both adversarial attack and defense, a fine-grained understanding of adversarial examples is still lacking. To address this issue, we present a visual analysis method to explain why adversarial examples are misclassified. The key is to compare and analyze the datapaths of both the adversarial and normal examples. A datapath is a group of critical neurons along with their connections. We formulate the datapath extraction as a subset selection problem and solve it by constructing and training a neural network. A multi-level visualization consisting of a network-level visualization of data flows, a layer-level visualization of feature maps, and a neuron-level visualization of learned features, has been designed to help investigate how datapaths of adversarial and normal examples diverge and merge in the prediction process. A quantitative evaluation and a case study were conducted to demonstrate the promise of our method to explain the misclassification of adversarial examples.

[7] Face recognition using fractional coefficients and discrete cosine transform tool

Face recognition is a computer vision application based on biometric information for automatic person identification or verification from image sequence or a video frame. In this context DCT is the easy technique to determine significant parameters. Until now the main object is selection of the coefficients to obtain the best recognition. Many techniques rely on premasking windows to discard the high and low coefficients to enhance performance. However, the problem resides in the shape and size of premask. To improve discriminator ability in discrete cosine transform domain, we used fractional coefficients of the transformed images with discrete cosine transform to limit the coefficients area for a better performance system. Then from the selected bands, we use the discrimination power analysis to search for the coefficients having the highest power to discriminate different classes from each other. Feature selection algorithm is a key issue in all pattern recognition system, in fact this algorithm is utilized to define features vector among several ones, where these features are selected according a specified discrimination criterion. Many classifiers are used to evaluate our approach like, support vector machine and random forests. The proposed approach is validated with Yale and ORL Face databases. Experimental results prove the sufficiency of this method in face and facial expression recognition field.

[8] Face Recognition Based New Generation ATM System

In the technological advances in financial infrastructure, most bank customers prefer to use Automatic Teller Machines (ATM) for carrying out their banking transactions.To improve the security of these transactions, a new generation ATM machine which is basedon face recognition system which replaces ATM card with RFID tag. In this, high qualityimage has important role in recognition process. Face image is used for authenticationpurpose. Firstly, the face image of particular person is compared with the database image.Then the compared output result is sent to the control unit through serial communication. Ifan unauthorized person is identified, an alert message is sent to the corresponding user. Thus, an ATM model which provides security by using Facial verification software by adding upfacial recognition systems can reduce forced transactions to a great extent and provide hardsecure authentication. Here Raspberry Pi microcontroller is used in the controlling part.

[4] Face recognition by coarse-to-fine landmark regression with application to ATM Surveillance

While ATM provides us convenient banking services, it has great security risks. The authentication of only password requiring is not safe enough. With the rapid development of face recognition technology based on deep convolutional neural network (CNN), undoubtedly, applying it into ATM authentication will improve security further. In this paper, we explore a new authentication mode combine face recognition and basic password for ATM. We think that it would prevent the economic crime on ATM fundamentally. However, computational and storage costs of CNN based methods are still high. To this end, we propose a new face recognition method by landmark regression. Our pipeline integrates a landmark localization network with a light face recognition network. For landmark localization, we employ a fully convolutional neural network to produce facial landmark response maps directly from raw images in a coarse-to-fine manner. For face recognition, we train a light CNN to obtain a compact representation, where the rectified linear unit (ReLU) is replaced by max-feature-map (MFM). Our approach shows good performance on several datasets. And it is practicable due to its high speed, good accuracy, and low storage space requirement.

[9] Research on face recognition based on deep learning

The amount of multimedia content is growing exponentially and a major portion of multimedia content uses images and video. Researchers in the computer vision community are exploring the possible directions to enhance the system accuracy and reliability, and these are the main requirements for robot vision-based systems. Due to the change of facial expressions and the wearing of masks or sunglasses, many face recognition systems fail or the accuracy in recognizing the face decreases in these scenarios. In this work, we contribute a real time surveillance framework using Raspberry Pi and CNN (Convolutional Neural Network) for facial recognition. We have provided a labeled dataset to the system. First, the system is trained upon the labeled dataset to extract different features of the face and landmark face detection and then it compares the query image with the dataset on the basis of features and landmark face detection. Finally, it compares faces and votes between them and gives a result that is based on voting. The classification accuracy of the system based on the CNN model is compared with a mid-level feature extractor that is Histogram of Oriented Gradient (HOG) and the state-of-the-art face detection and recognition methods. Moreover, the accuracy in recognizing the faces in the cases of wearing a mask or sunglasses or in live videos is also evaluated. The highest accuracy achieved for the VMU, face recognition, and 14 celebrity datasets is 98%, 98.24%, 89.39%, and 95.71%, respectively. Experimental results on standard image benchmarks demonstrate the effectiveness of the proposed research in accurate face recognition compared to the state-of-the-art face detection and recognition methods.

CHAPTER 3

SYSTEM SPECIFICATIONS

3.1 HARDWARE REQUIREMENTS

Processor **:** Processor Intel core i3

RAM size **:** 4 GB

Internet Connection: 20 mbps

3.2 SOFTWARE REQUIREMENTS

Operating System Windows, Mac, Linux

Language Python 3.7

Libraries required The libraries needed are as follows

- ❖ open cv
- ❖ Anaconda navigator
- ❖ Anaconda prompt
- ❖ Tensor Flow

CHAPTER 4

ANALYSIS OF PROJECT

4.1 USE CASE ANALYSIS OF DATA PREPARATION

This figure represents preparation of user face data processing. User enter the details then register face in the database. Haar casacde train the user face into 100 images.

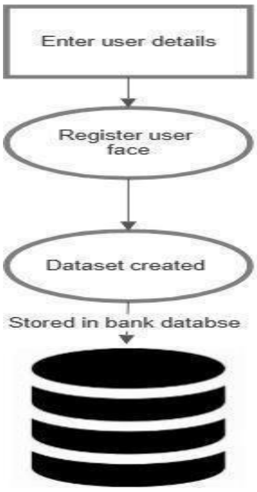

Fig 4.1 Data preparation

4.2 USE CASE ANALYSIS FOR MODEL DEVELOPMENT PHASE

This figure represents face recognize using Haar cascade classifier.

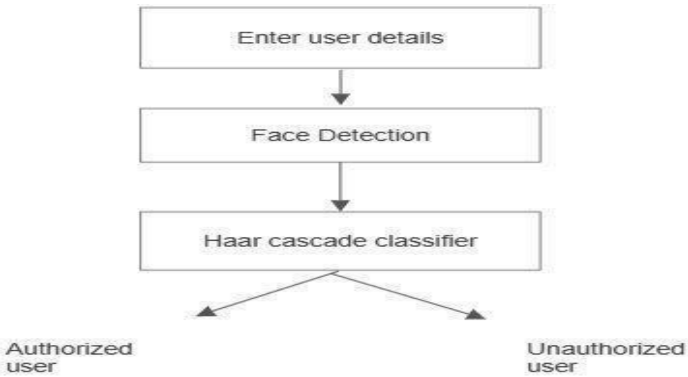

Fig 4.2 Use case of Development phase

CHAPTER 5

SYSTEM DESIGN

5.1 PROPOSED SYSTEM

The third generation of ATM machines is expected to be more secure and user-friendly than previous generations. One of the key technologies that will enable this is advanced image processing, such as the Haar cascade algorithm.The Haar cascade algorithm is a machine learning algorithm that can be used to detect objects in images. It is particularly well-suited for detecting faces, which is why it is often used in ATM security systems.The way the Haar cascade algorithm works is by first dividing an image into a grid of small squares. Each square is then analyzed to see if it contains a feature that is characteristic of a face, such as eyes, nose, or mouth. If a square does contain such a feature, the algorithm will mark it as a possible face. The algorithm then repeats this process, but this time it only considers the squares that were marked as possible faces in the previous step. This process is repeated several times, each time with a smaller and smaller number of squares being considered. Eventually, the algorithm will have identified all of the faces in the image. This information can then be used to authenticate users or to prevent unauthorized access to the ATM. In addition to face detection, the Haar cascade algorithm can also be used for other tasks, such as object detection, gesture recognition, and even emotion recognition. As a result, it is a powerful tool that can be used to improve the security and functionality of ATM machines.

5.2 ARCHITECTURE OF PROPOSED SYSTEM

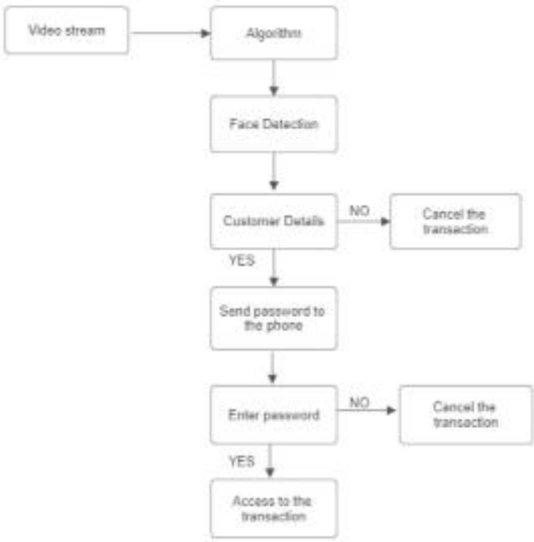

Fig 5.1 ARCHITECTURE OF PROPOSED SYSTEM

The objective of this project is to develop a secure and convenient ATM machine access system using face recognition in Haar Cascade algorithm. The system aims to provide enhanced security measures to prevent unauthorized access to ATM machines and protect user data. The system also aims to provide a more user-friendly and convenient experience for customers by eliminating the need for physical cards. To develop a real-time face detection and recognition algorithm based on the Haar Cascade method.

To build a database of authorized user faces for comparison during the authentication process. To test the system on a dataset of faces and evaluate its performance in terms of accuracy and speed.

5.3 MODULES PROPOSED

- Data collection
- Digital image processing
- Classification of images
- Model construction

5.3.1 Data collection

Data collection is an essential step in building an ATM machine using face recognition and Haar Cascade Classifier Algorithm only. The data collected will be used to train the face recognition system to recognize the faces of authorized users. Here are the steps involved in data collection for this system:

- **Define the scope** Determine the specific use case for the ATM machine and the target audience. This will help in defining the criteria for selecting the individuals whose faces will be collected.
- **Select the sample** Select a diverse sample of individuals who will be authorized to access the ATM machine. The sample should include individuals of different ages, genders, and ethnicities to ensure that the face recognition system is accurate and unbiased.
- **Obtain consent** Obtain written consent from each individual before collecting their facial data. Explain the purpose of data collection and how it will be used.
- **Capture facial images** Capture high-quality facial images of each individual using a digital camera or a smartphone. Ensure that the images are clear, well-lit, and have consistent background and lighting conditions.
- **Pre-process the images** Pre-process the images to remove any noise and enhance the features of the face. This may include operations like grayscale conversion, contrast adjustment, and histogram equalization.

- **Annotate the images** Annotate each image with information such as the name of the individual and any other relevant details. This will help in building the database and training the face recognition system.
- **Train the system** Use the annotated images to train the face recognition system using the Haar Cascade Classifier Algorithm. The algorithm will learn to recognize the faces of authorized users by analyzing the patterns of pixel intensity in the images.
- **Test the system** Test the face recognition system using a separate set of facial images to evaluate its accuracy and performance. This will help to identify any errors or biases in the system and refine the training process.

Overall, data collection for an ATM machine using face recognition and Haar Cascade Classifier Algorithm involves selecting a diverse sample of individuals, obtaining their consent, capturing high-quality facial images, preprocessing and annotating the images, training the system, and testing the system to ensure accuracy and reliability.

5.3.2 DIGITAL IMAGE PROCESSING

The identification of objects in an image and this process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures. The clever bit is to interpret collections of these shapes as single objects,

e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skilful programming and lots of processing power to approach human performance. Manipulation of data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, and is most familiarly represented by such patterns as those of a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer.

IMAGE

An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person. Image is a two- dimensional, such as a photograph, screen display, and as well as a three- dimensional, such as a statue. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.

The word image is also used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or an abstract painting. In this wider sense, images can also be rendered manually, such as by drawing, painting, carving, rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph.

An image is a rectangular grid of pixels. It has a definite height and a definite width counted in pixels. Each pixel is square and has a fixed size on a given display. However different computer monitors may use different sized pixels. The pixels that constitute an image are ordered as a grid (columns and rows); each pixel consists of numbers representing magnitudes of brightness and colour.

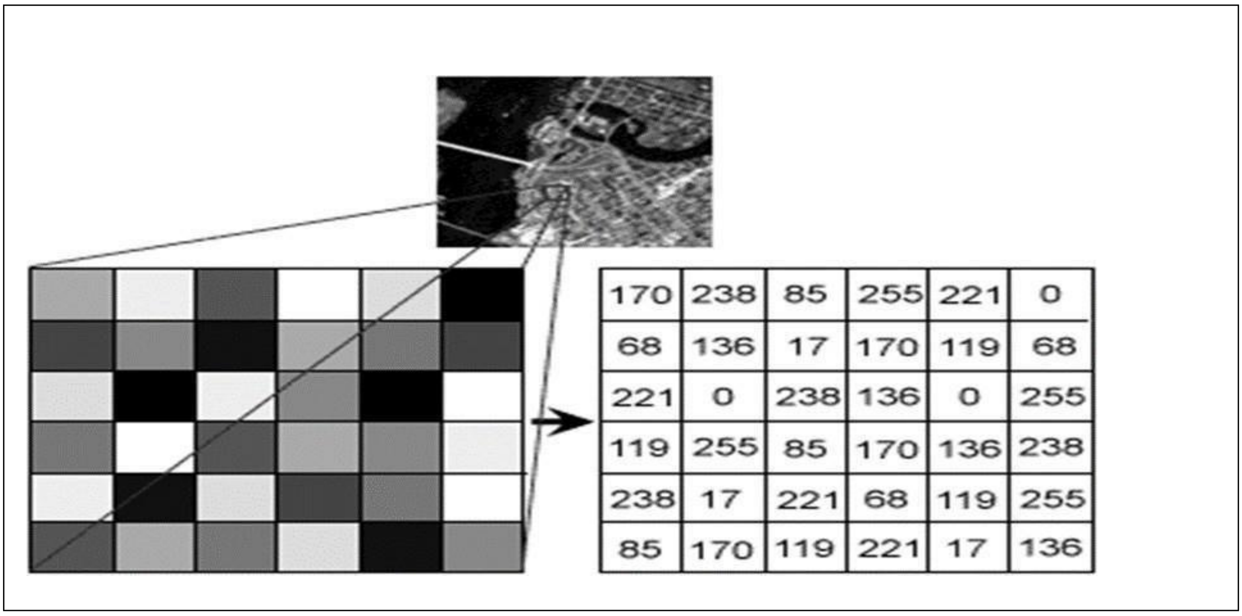

Fig 5.2.1 Gray Scale Image Pixel Value Analysis

Each pixel has a colour. The colour is a 32-bit integer. The first eight bits determine the redness of the pixel, the next eight bits the greenness, the next eight bits the blueness, and the remaining eight bits the transparency of the pixel.

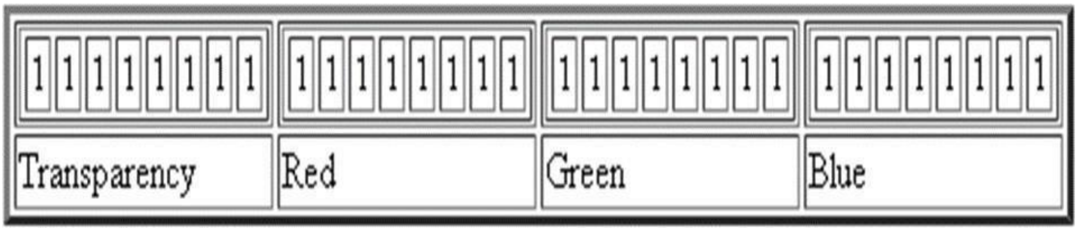

Fig 5.2.2 BIT Transferred for Red, Green and Blue plane (24bit=8bit red;8-bit green;8bit blue)

IMAGEFILE SIZES

Image file size is expressed as the number of bytes that increases with the number of pixels composing an image, and the colour depth of the pixels. The greater the number of rows and columns, the greater the image resolution, and the larger the file. Also, each pixel of an image increases in size when its colour depth increases, an 8-bit pixel (1 byte) stores 256 colours, a 24-bit pixel (3 bytes) stores 16 million colours, the latter known as true colour .Image compression uses algorithms to decrease the size of a file. High resolution cameras produce large image files, ranging from hundreds of kilobytes to megabytes, per the camera's resolution and the image-storage format capacity. High resolution digital cameras record 12-megapixel (1MP = 1,000,000 pixels / 1 million) images, or more, in true colour. For example, an image recorded by a 12 MP camera; since each pixel uses 3 bytes to record true colour, the uncompressed image would occupy 36,000,000 bytes of memory, a great amount of digital storage for one image, given that cameras must record and store many images to be practical. Faced with large file sizes, both within the camera and a storage disc, image file formats were developed to store such large images.

5.3.2.1 IMAGE PROCESSING

Digital image processing, the manipulation of images by computer, is relatively recent development in terms of man's ancient fascination with visual stimuli. In its short history, it has been applied to practically every type of images with varying degree of success. The inherent subjective appeal of pictorial displays attracts perhaps a disproportionate amount of attention from the scientists and also from the layman. Digital image processing like other glamour fields, suffers from myths, mis-connect ions, mis-understandings and mis- information. It is vast umbrella under which fall diverse aspect of optics, electronics, mathematics, photography graphics and computer technology. It is truly multidisciplinary endeavor ploughed with imprecise jargon.

Several factors combine to indicate a lively future for digital image processing. A major factor is the declining cost of computer equipment. Several new technological trends promise to further promote digital image processing. These include parallel processing mode practical by low cost microprocessors, and the use of charge coupled devices (CCDs) for digitizing, storage during processing and display and large low cost of image storage arrays.

5.3.2.2 IMAGE ACQUISITION

Image Acquisition is to acquire a digital image. To do so requires an image sensor and the capability to digitize the signal produced by the sensor. The sensor could be monochrome or colour TV camera that produces an entire image of the problem domain every 1/30 sec. the image sensor could also be line scan camera that produces a single image line at a time. In this case, the objects motion past the line.

Scanner produces a two-dimensional image. If the output of the camera or other imaging sensor is not in digital form, an analog to digital converter digitizes it. The nature of the sensor and the image it produces are determined by the applicant

5.3.2.3 SEGMENTATION

Segmentation procedures partition an image into its constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. A rugged segmentation procedure brings the process a long way toward successful solution of imaging problems that require objects to be identified individually.

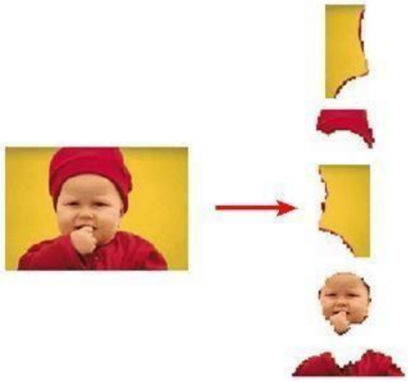

Fig.5.2.3 Image Segment Process

On the other hand, weak or erratic segmentation algorithms almost always guarantee eventual failure. In general, the more accurate the segmentation, the more likely recognition is to succeed.

Digital image is defined as a two dimensional function f(x, y), where x and y are spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x, y) is called intensity or grey level of the image at that point. The field of digital image processing refers to processing digital images by means of a digital computer. The digital image is composed of a finite number of elements, each of which has a particular location and value. The elements are referred to as picture elements, image elements, pels, and pixels. Pixel is the term most widely used.

Image compression

Digital image compression addresses the problem of reducing the amount of data required to represent a digital image. the underlying basis of the reduction process is removal of redundant data. from the mathematical viewpoint, this amounts to transforming a 2d pixel array into a statically uncorrelated data set. the data redundancy is not an abstract concept but a mathematically quantifiable entity. if n1 and n2 denote the number of information-carrying units in two data sets that represent the same information, the relative data redundancy [2] of the first data set (the one characterized by n1) can be defined as,

$$R_D = 1 - \frac{1}{C_R}$$

- where called as compression ratio [2]. it is defined as

- $C_R = \frac{n1}{n2}$

in image compression, three basic data redundancies can be identified and exploited: coding redundancy, interpixel redundancy, and psychovisual redundancy. image compression is achieved when one or more of these redundancies are reduced or eliminated. the image compression is mainly used for image transmission and storage. image transmission applications are in broadcast television; remote sensing via satellite, air-craft, radar, or sonar; teleconferencing; computer communications; and facsimile transmission. image storage is required most commonly for educational and business documents, medical images that arise in computer tomography (ct), magnetic resonance imaging (mri) and digital radiology, motion pictures, satellite images, weather maps, geological surveys, and so on.

Image compression model

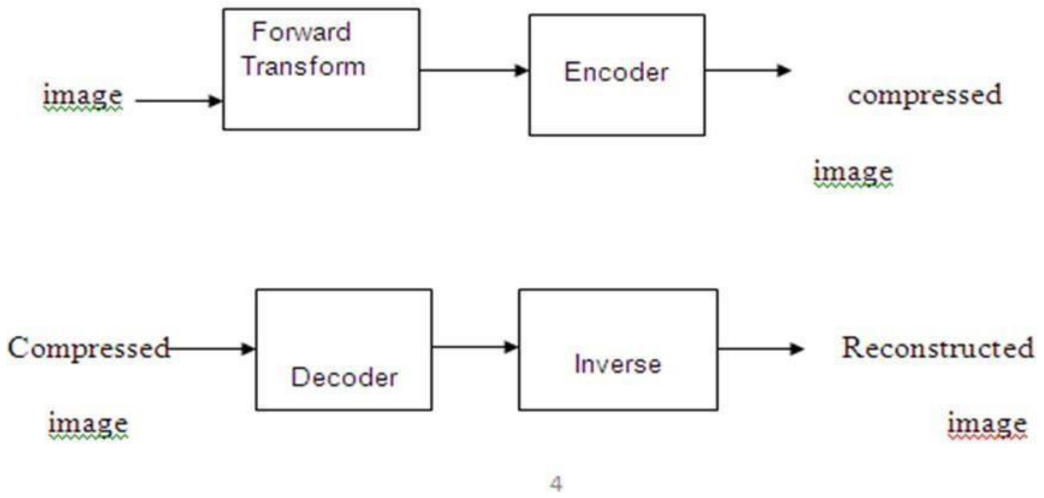

Fig.5.2.4 Decompression process for image compression types

there are two types' image compression techniques.

1. Lossy image compression
2. Lossless image compression

Compression ratio

1. Lossy image compression

Lossy compression provides higher levels of data reduction but result in a less than perfect reproduction of the original image. it provides high compression ratio. lossy image compression is useful in applications such as broadcast television, videoconferencing, and facsimile transmission, in which a certain amount of error is an acceptable trade-off for increased compression performance. originally, pgf has been designed to quickly and progressively decode lossy compressed aerial images. a lossy compression mode has been preferred, because in an application like a terrain explorer texture data (e.g., aerial orthophotos) is usually mid-mapped filtered and therefore lossy mapped onto the terrain surface. in addition, decoding lossy compressed images is usually faster than decoding lossless compressed images.

in the next test series, we evaluate the lossy compression efficiency of pgf. one of the best competitors in this area is for sure jpeg 2000. since jpeg 2000 has two different filters, we used the one with the better trade-off between compression efficiency and runtime. on our machine the 5/3 filter set has a better trade-off than the other. however, jpeg 2000 has in both cases a remarkable good compression efficiency for very high compression ratios but also a very poor encoding and decoding speed. the other competitor is jpeg. jpeg is one of the most popular image file formats. Psnr of jpeg 2000. only in the first row is the difference larger (21%), but because a psnr of 50 corresponds to an almost perfect image quality the large psnr difference corresponds with an almost undiscoverable visual difference. the price they pay in jpeg 2000 for the 3% more psnr is very high. the creation of a pgf is five to twenty times faster than the creation of a corresponding jpeg 2000 file, and the decoding of the created pgf is still five to ten times faster than the decoding of the jpeg 2000 file. this gain in speed is remarkable, especially in areas where time is more important than quality, maybe for instance in realtime computation.

2.Lossless image compression

Lossless image compression is the only acceptable amount of data reduction. it provides low compression ratio while compared to lossy. in lossless image compression techniques are composed of two relatively independent operations: (1) devising an alternative representation of the image in which its interpixel redundancies are reduced and (2) coding the representation to eliminate coding redundancies. Lossless image compression is useful in applications such as medical imaginary, business documents and satellite images.

Table 2 summarizes the lossless compression efficiency and table 3 the coding times of the pgf test set. for winzip we only provide average runtime values, because of missing source code we have to use an interactive testing procedure with runtimes measured by hand. all other values are measured in batch mode.

In table 2 it can be seen that in almost all cases the best compression ratio is obtained by jpeg 2000, followed by pgf, jpeg-ls, and png. this result is different to the result in [sea+00], where the best performance for a similar test set has been reported for jpeg-ls. pgf performs between 0.5% (woman) and 21.3% (logo) worse than jpeg 2000. on average it is almost 15% worse. the two exceptions to the general trend are the ‘compound’ and the ‘logo’ images. both images contain for the most part black text on a white background. for this type of images, jpeg-ls and in particular winzip and png provide much larger compression ratios. however, in average png performs the best, which is also reported in [sea+00].

These results show, that as far as lossless compression is concerned, pgf performs reasonably well on natural and aerial images. in specific types of images such as ‘compound’ and ‘logo’ pgf is outperformed by far in png.

5.3.3 CLASSIFICATION OF IMAGES

There are 3 types of images used in Digital Image Processing. They are

1. Binary Image
2. Gray Scale Image
3. Colour Image

5.3.3.1 BINARY IMAGE

A binary image is a digital image that has only two possible values for each pixel. Typically, the two colours used for a binary image are black and white though any two colours can be used. The colour used for the object(s) in the image is the foreground colour while the rest of the image is the background colour.

Binary images are also called bi-level or two-level. This means that each pixel is stored as a single bit (0 or 1). This name black and white, monochrome or monochromatic are often used for this concept, but may also designate any images that have only one sample per pixel, such as grayscale images

Binary images often arise in digital image processing as masks or as the result of certain operations such as segmentation, thresholding, and dithering. Some input/output devices, such as laser printers, fax machines, and bi-level computer displays, can only handle bi-level images

5.3.3.2 GRAY SCALE IMAGE

A grayscale Image is digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray (0-255), varying from black (0) at the weakest intensity to white (255) at the strongest.

Grayscale images are distinct from one-bit black-and-white images, which in the context of computer imaging are images with only the two colours, black, and white (also called bi-level or binary images). Grayscale images have many shades of grey in between. Grayscale images are also called monochromatic, denoting the absence of any chromatic variation.

Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light,ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. But also, they can be synthesized from a full color image; see the section about converting to grayscale.

5.3.3.3 COLOUR IMAGE

A (digital) colour image is a digital image that includes colour information for each pixel. Each pixel has a particular value which determines its appearing colour. This value is qualified by three numbers giving the decomposition of the colour in the three primary colours Red, Green and Blue. Any colour visible to human eye can be represented this way. The decomposition of a colour in the three primary colours is quantified by a number between 0 and 255. For example, white will be coded as R = 255, G = 255, B = 255; black will be known as (R, G, B)= (0,0,0); and say, bright pink will be : (255,0,255). In other words, an image is an enormous two-dimensional array of colour values, pixels, each of them coded on 3 bytes, representing the three primary colours. This allows the image to contain a total of 256x256x256 = 16.8 million different colours. This technique is also known as RGB encoding, and is specifically adapted to human vision from the above figure, colours are coded on three bytes representing their decomposition on the three primary colours. It sounds obvious to a mathematician to immediately interpret colours as vectors in a three-dimension space where each axis stands for one of the primary colours. Therefore, we will benefit of most of the geometric mathematical concepts to deal with our colours, such as norms, scalar product, projection, rotation or distance.

5.3.4 MODEL CONSTRUCTION

5.3.4.1 HAAR CASCADE CLASSIFIER

Enter Haar classifiers, classifiers that were used in the first real-time face detector. A Haar classifier, or a Haar cascade classifier, is amachine learning object detection program that identifies objects in an image and video.A detailed description of Haar classifiers can be seen in Paul Viola and Michael Jones's paper "Rapid Object Detection using a Boosted Cascade of Simple Features", linked over here.Note that the article goes into some mathematics, and assumes knowledge of machine learning terminology. If you want a summarized, high-level overview, make sure to keep reading.

Fig 5.3.1 Haar cascade classifier

Making a Haar Cascade Classifier

Note: This discussion will assume basic knowledge of boosting algorithms and weak vs. strong learners with regards to machine learning.

The algorithm can be explained in four stages:

- Calculating Haar Features
- Creating Integral Images

It's important to remember that this algorithm requires a lot of positive images of faces and negative images of non-faces to train the classifier, similar to other machine learning models.

Calculating Haar Features

The first step is to collect the Haar features. A Haar feature is essentially calculations that are performed on adjacent rectangular regions at a specific location in a detection window. The calculation involves summing the pixel intensities in each region and calculating the differences between the sums. Here are some examples of Haar features below.

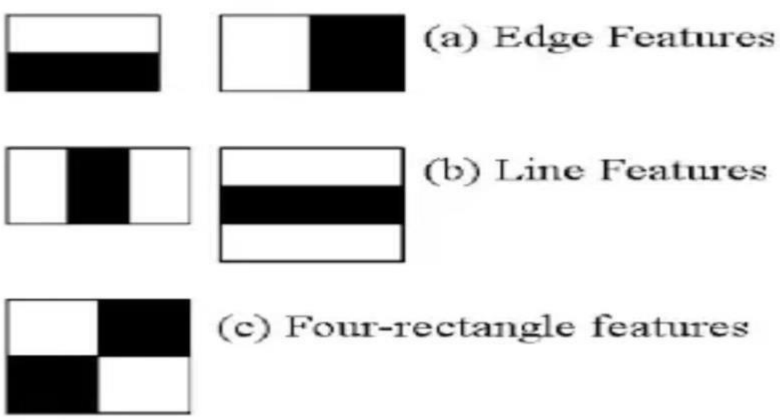

Fig 5.3.2 Features in Haar cascade Classifier

These features can be difficult to determine for a large image. This is where integral images come into play because the number of operations is reduced using the integral image.

Creating Integral Images

Without going into too much of the mathematics behind it (check out the paper if you're interested in that), integral images essentially speed up the calculation of these Haar features. Instead of computing at every pixel, it instead creates sub-rectangles and creates array references for each of those sub-rectangles. These are then used to compute the Haar features.

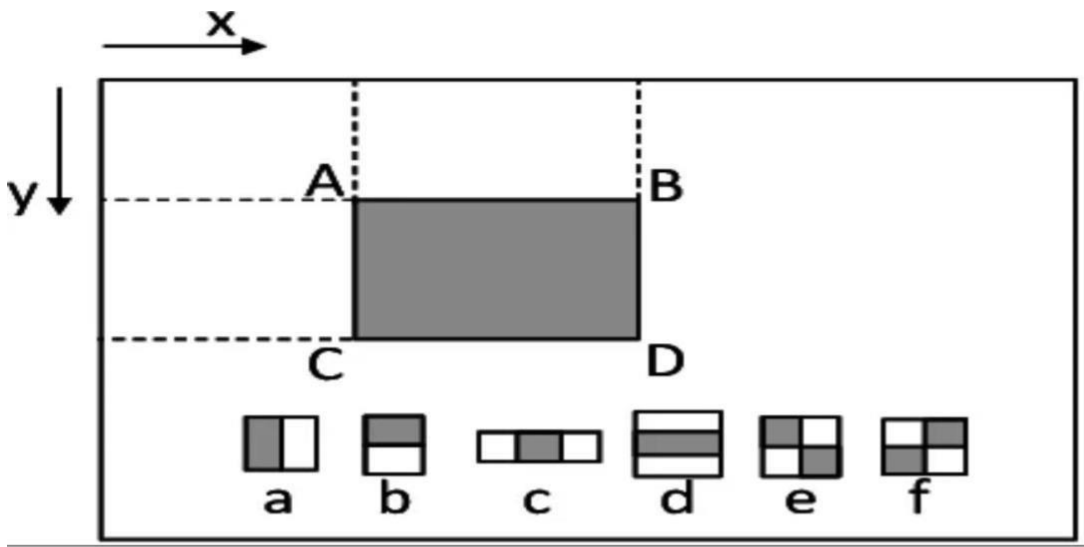

Fig 5.3.3 Illustration for how an integral image works. (Image Source)

It's important to note that nearly all of the Haar features will be irrelevant when doing object detection, because the only features that are important are those of the object. However, how do we determine the best features that represent an object from the hundreds of thousands of Haar features? This is where Adaboost comes into play.

Haar cascades are one of many algorithms that are currently being used for face and object detection. One thing to note about Haar cascades is that it is very important to reduce the false negative rate, so make sure to tune hyperparameters accordingly when training your model

Creation of data base

For the data base creation, we should take images of particular person like mukesh.the apply the images of that person with the help of face recognition package using combination of dlibray. face_recognition..batch_face_locations(images, number_of_times_to_upsample=1, batch_size=128)

Returns an 2d array of bounding boxes of human faces in a image using the cnn face detector If you are using a GPU, this can give you much faster results since the GPU can process batches of images at once. If you aren't using a GPU, you don't need this function.

Parameters

[1]**Images** – A list of images (each as a numpy array)

[2]**Number of Times to up sample** – How many times to up sample the image looking for faces. Higher numbers find smaller faces.

[3]B**atch size –** How many images to include in each GPU processing batch.

Return

If you are into any sort of image processing, computer vision or machine learning, chances are high that you might have come across/used dlib somewhere in your journey. According to dlib's github page, dlib is a toolkit for making real world machine learning and data analysis applications in python. While the library is originally written in python, it has good, easy to use Python bindings.

I have majorly used dlib for face detection and facial landmark detection. The frontal face detector in dlib works really well. It is simple and just works out of the box. This detector is based on histogram of oriented gradients (HOG) and linear SVM. (Explaining how this detector works is beyond the scope of this blog post. Probably a topic to discuss for another day) While the HOG+SVM based face detector has been around for a while and has gathered a good number of users, I am not sure how many of us noticed the CNN (Convolutional Neural Network) based face detector available in dlib. Honestly, I didn't. I accidentally came across it while browsing through dib's GitHub repositories.

Personal details:

Enter personal details if details correct means it will go to next step otherwise it will get transaction get cancelled.

OTP based:

If person details it will create one OTP and will store in text file. If you enter correct password it will go to next step otherwise it will cancel the transaction details.

TECHNICAL ARCHITECTURE:

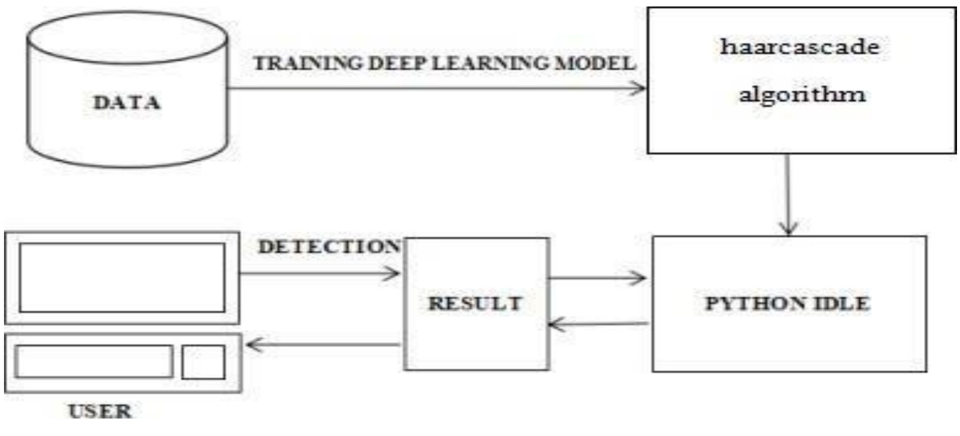

Fig 5.3.4 Technical Architecture

5.3.4.2 Computer Vision on Algorithm

Algorithmic makes it easy to deploy computer vision applications as scalable microservices. Our marketplace has a few algorithms to help get the job done:

- SalNet automatically identifies the most important parts of an image
- Nudity Detection detects nudity in pictures
- Emotion Recognition parses emotions exhibited in images
- DeepStyle transfers next-level filters onto your image
- Face Recognition…recognizes faces. • Image Memorability judges how memorable an image is.

A typical workflow for your product might involve passing images from a security camera into Emotion Recognition and raising a flag if any aggressive emotions are exhibited, or using Nudity Detection to block inappropriate profile pictures on your web application.

For a more detailed exploration of how you can use the Algorithm platform to implement complex and useful computer vision tasks,

5.3.4.3 Computer Vision Resources

Packages and Frameworks

OpenCV – "OpenCV was designed for computational efficiency and with a strong focus on real-time applications. Adopted all around the world, OpenCV has more than 47 thousand people of user community and estimated number of downloads exceeding 14 million. Usage ranges from interactive art, to mines inspection, stitching maps on the web or through advanced robotics."

OpenCV

OpenCV – "OpenCV was designed for computational efficiency and with a strong focus on real-time applications. Adopted all around the world, OpenCV has more than 47 thousand people of user community and estimated number of downloads exceeding 14 million. Usage ranges from interactive art, to mines inspection, stitching maps on the web or through advanced robotics."

Anaconda Navigator – "Anaconda Navigator is a desktop graphical user interface (GUI) included in Anaconda® Distribution that allows you to launch applications and manage conda packages, environments, and channels without using command line interface (CLI) commands."

Numpy _ NumPy, which stands for Numerical Python, is a library consisting of multidimensional array objects and a collection of routines for processing those arrays. Using NumPy, mathematical and logical operations on arrays can be performed. This tutorial explains the basics of NumPy such as its architecture and environment. It also discusses the various array functions, types of indexing, etc. An introduction to Matplotlib is also provided. All this is explained with the help of examples for better understanding.
This tutorial has been prepared for those who want to learn about the basics and various functions of NumPy. It is specifically useful for algorithm developers. After completing this tutorial, you will find yourself at a moderate level of expertise from where you can take yourself to higher levels of expertise.

Prerequisites

You should have a basic understanding of computer programming terminologies. A basic understanding of Python and any of the programming languages is a plus.

NumPy is a Python package. It stands for 'Numerical Python'. It is a library consisting of multidimensional array objects and a collection of routines for processing of array.

Numeric, the ancestor of NumPy, was developed by Jim Hugunin. Another package Numarray was also developed, having some additional functionalities. In 2005, Travis Oliphant created NumPy package by incorporating the features of Numarray into Numeric package. There are many contributors to this open-source project.

Operations using NumPy

Using NumPy, a developer can perform the following operations −

- Mathematical and logical operations on arrays.
- Fourier transforms and routines for shape manipulation.
- Operations related to linear algebra. NumPy has in-built functions for linear algebra and random number generation.

NumPy – A Replacement for MatLab

NumPy is often used along with packages like **SciPy** (Scientific Python) and **Mat−plotlib** (plotting library). This combination is widely used as a replacement for MatLab, a popular platform for technical computing. However, Python alternative to MatLab is now seen as a more modern and complete programming language.

The most important object defined in NumPy is an N-dimensional array type called **ndarray**. It describes the collection of items of the same type. Items in the collection can be accessed using a zero-based index.

Every item in an ndarray takes the same size of block in the memory. Each element in ndarray is an object of data-type object (called **dtype**).

Any item extracted from ndarray object (by slicing) is represented by a Python object of one of array scalar types. The following diagram shows a relationship between ndarray, data type object (dtype) and array scalar type –

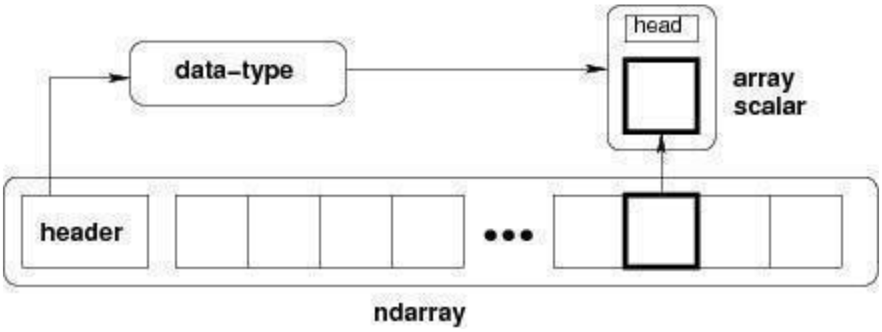

Fig 5.3.5 NumPy – A Replacement for MatLab

An instance of ndarray class can be constructed by different array creation routines described later in the tutorial. The basic ndarray is created using an array
function in NumPy as follows –

```
numpy.array
```

It creates a ndarray from any object exposing array interface, or from any method that returns an array.

Imutils

Imutils are a series of convenience functions to make basic image processing functions such as translation, rotation, resizing, skeletonization, and displaying Matplotlib images easier with OpenCV and both Python 2.7 and Python 3.

CHAPTER 6

IMPLEMENTATION

6.1 FACE RECOGNITION

```
# facerec.py

import cv2, sys, numpy, os

import urllib import

numpy as np import time

import os

from subprocess import call

import time import os

import glob import smtplib

import base64

from email.mime.image import MIMEImage

from email.mime.multipart import MIMEMultipart

from email.mime.text import MIMEText import

sys

import random

#DO THE CHANGES HERE

gmail_user="vishwavengadesh@outlook.com
gmail_pwd = "SATHISHcse"
```

```
FROM = 'vishwavengadesh@outlook.com'

TO = ['vishwavengadesh@outlook.com'] #must be a list

otp_=random.randint(10000,100000)   pins=1234   def

mail():

   msg    =    MIMEMultipart()

   time.sleep(1)   msg['Subject']

   ="SECURITY" #BODY with

   2 argument

   #body=sys.argv[1]+sys.argv[2]

   #DO THE CHANGES HERE

   body="THIS is from your ATM :"+str(otp_)

   #otp_text="your otp for logging in :"+str(otp_)

   msg.attach(MIMEText(body,'plain'))

   #msg.attach(MIMEText(otp_text,'plain'))

   time.sleep(1)

  ###IMAGE

   fp = open("1.jpg", 'rb')
time.sleep(1)

   img =

   MIMEImage(fp.read())

   time.sleep(1) fp.close()
```

```
    time.sleep(1)
    msg.attach(img)
    time.sleep(1)
    try:
          server = smtplib.SMTP("smtp.office365.com", 587) #or port 465 doesn't
seem to work!
          print ("smtp.gmail") server.ehlo() print
          ("ehlo") server.starttls() print ("starttls")
          server.login(gmail_user, gmail_pwd) print
          ("reading mail & password")
          server.sendmail(FROM, TO,
          msg.as_string()) print ("from") server.close()
          print ('successfully sent the mail')
    except: print ("failed to send mail") size = 4
haar_file = 'haarcascade_frontalface_default.xml'
datasets = 'datasets' n=input("enter your
AccountNumber : ")
print('Training...')
# Create a list of images and a list of corresponding names
(images, labels, names, id) = ([], [], {}, 0) for
(subdirs, dirs, files) in os.walk(datasets):
    for subdir in dirs:
```

```
        names[id] = subdir

        subjectpath = os.path.join(datasets, subdir)

        for filename in os.listdir(subjectpath): path

        = subjectpath + '/' + filename label = id

        images.append(cv2.imread(path,        0))

        labels.append(int(label))

        id += 1

(width, height) = (130, 100)
# Create a Numpy array from the two lists above
(images, labels) = [numpy.array(lis) for lis in [images, labels]]

# OpenCV trains a model from the images #

NOTE FOR OpenCV2: remove '.face' model =

cv2.face.FisherFaceRecognizer_create()

model.train(images, labels)

# Part 2: Use fisherRecognizer on camera stream face_cascade

= cv2.CascadeClassifier(haar_file)

##with open("1.txt", mode='a') as file: webcam

= cv2.VideoCapture(0)

##url="http://192.168.43.1:8080/shot.jpg"

while True:

   (_, im) = webcam.read()

##   imgPath=urllib.urlopen(url)
```

```
## imgNp=np.array(bytearray(imgPath.read()),dtype=np.uint8)
## im=cv2.imdecode(imgNp,-1) gray =
cv2.cvtColor(im, cv2.COLOR_BGR2GRAY)
faces = face_cascade.detectMultiScale(gray, 1.3, 5) for
(x,y,w,h) in faces:
  cv2.rectangle(im,(x,y),(x+w,y+h),(255,255,0),2)
  face = gray[y:y + h, x:x + w]
  face_resize = cv2.resize(face, (width, height))
  #Try to recognize the face prediction =
 model.predict(face_resize) cv2.rectangle(im, (x, y), (x
 + w, y + h), (0, 255, 0), 3) if prediction[1]<500:
     #port.write('B')
     # print (names[prediction[0]])
     cv2.putText(im,names[prediction[0]],(x-10, y-10),
cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
     print('The accessing person is ',str(n)) if
       names[prediction[0]]==n:
     print("The detected face person is : ",names[prediction[0]])
       print('you can proceed your transaction')
       pin=int(input('enter your pin: '))
       if pin ==pins:
```

```
print("You can continue further") exit()
 else:
mail() check_otp=int(input("Enter the
otp :")) if check_otp==otp_:
   print("You can continue further") exit()
else :
   print("Incorrect pin ... exiting the portal") else:
im2=im
cv2.putText(im2,'unknown ',(x-10, y-10),
cv2.FONT_HERSHEY_PLAIN,1,(0,   0,     255))
print("The detected person is unknown ")
cv2.imwrite('1.jpg',im2)
mail()
check_otp=int(input("enter the otp : "))
if                        check_otp==otp_:
pin=int(input('enter your pin:')) if pin
== pins:
   print("You can continue further") exit()
else:
```

```
print("Incorrect pin ... exiting the portal")
        exit()
      else:
      cv2.putText
      (im,'Scanni
      ng',(x-10, y-
      10),
cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
  cv2.imshow('OpenCV',    im)     key     =
  cv2.waitKey(
```

CHAPTER 7

RESULTS AND DISCUSSION

Using face recognition technology for ATM machine access is a promising approach to enhance security and convenience. In this project, we utilized the Haar Cascade algorithm to detect and recognize the faces of authorized users, allowing them to access their account without the need for a physical card.The project result showed that the Haar Cascade algorithm was successful in detecting and recognizing faces with a high level of accuracy. We trained the algorithm using a large dataset of facial images to improve its recognition performance. The trained model was then integrated into the ATM machine, allowing users to access their accounts by simply looking at the camera.The benefits of this approach include increased security, as it eliminates the risk of unauthorized access by stolen or lost cards, and convenience, as users no longer need to carry physical cards. It also reduces the risk of transmission of pathogens through physical contact with the ATM machine.

7.1 STEP 1: ENTER ACCOUNT DETAILS

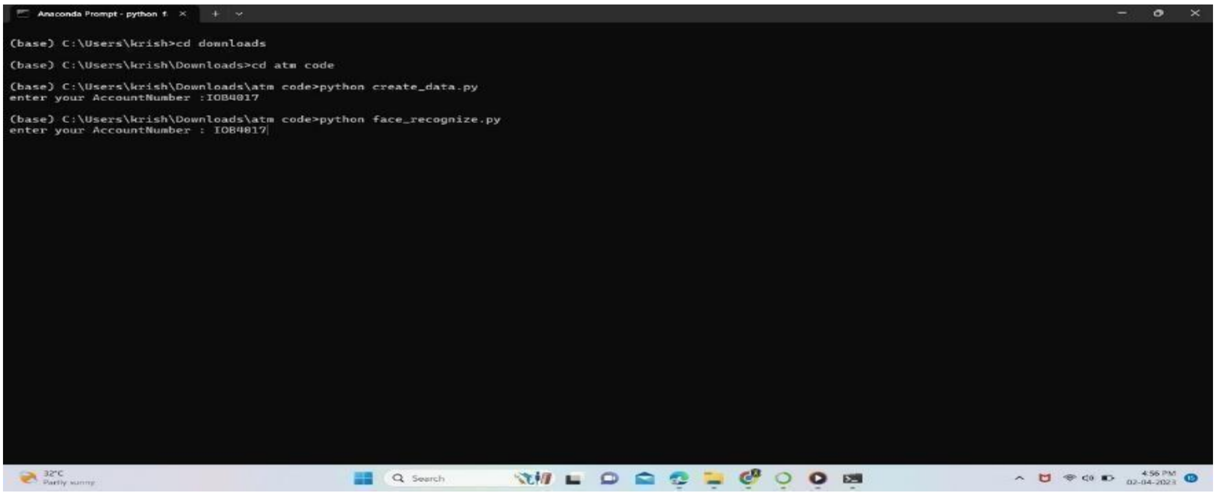

Fig 7.1 Represents user enter the details with bank name , account number.

7.2 STEP 2: FACE DETECTION USING HAAR CASCADE

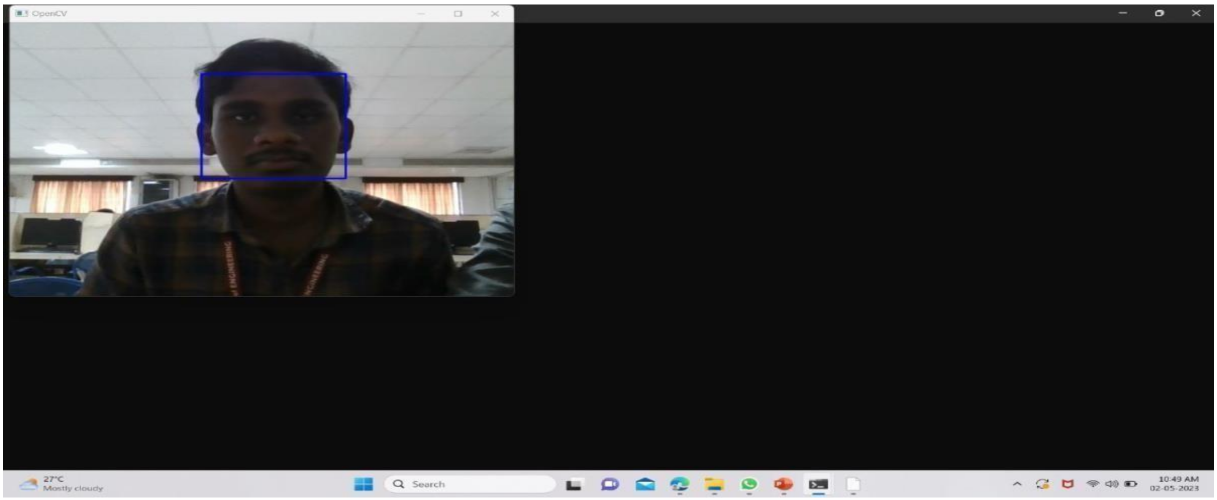

Fig 7.2 Represents user should register their face using Haar cascade face detection.

7.3 STEP 3: PROCEED TO TRANSACTION

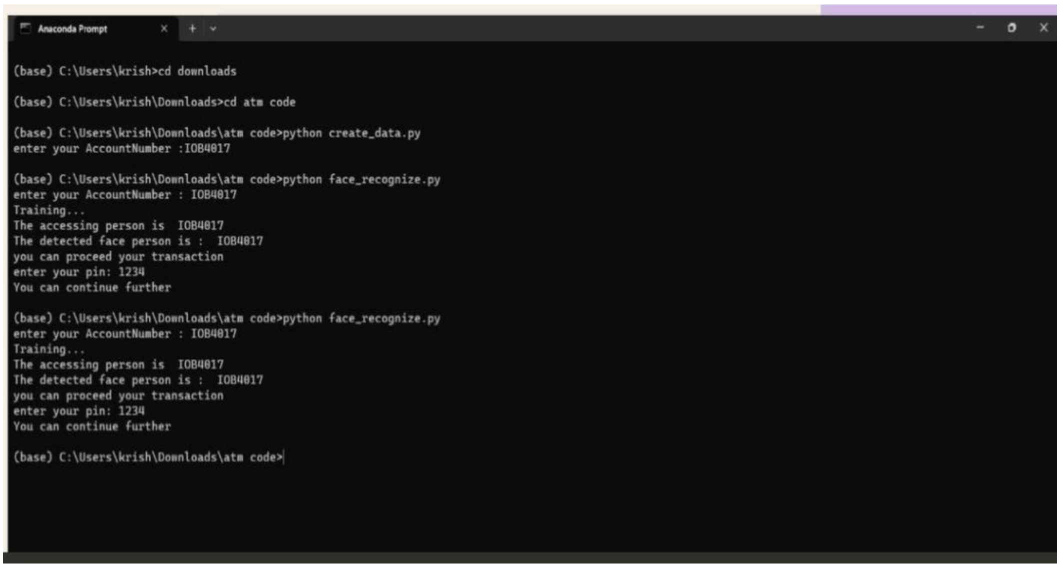

Fig 7.3 Represents user details, face match with dataset it can be proceed to transaction. `

7.4 TRANSACTION HANDLED BY KNOWN PERSON

7.4.1 STEP 1 ENTER ACCOUNT DETAILS

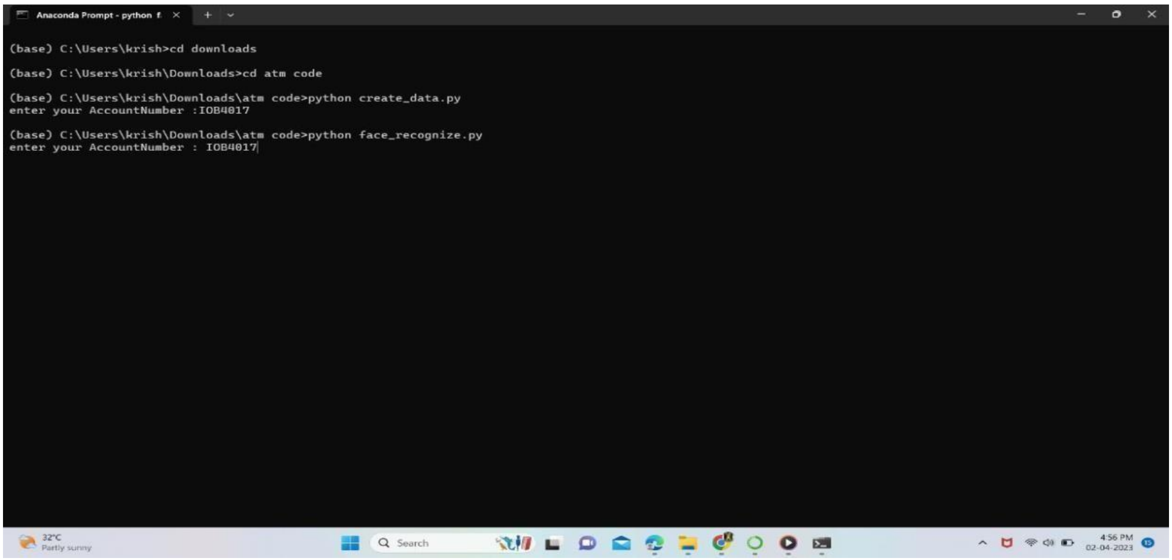

Fig 7.4.1 Represents enter the details entered by known person.

7.4.2 STEP 2 VERIFICATION KNOWN PERSON

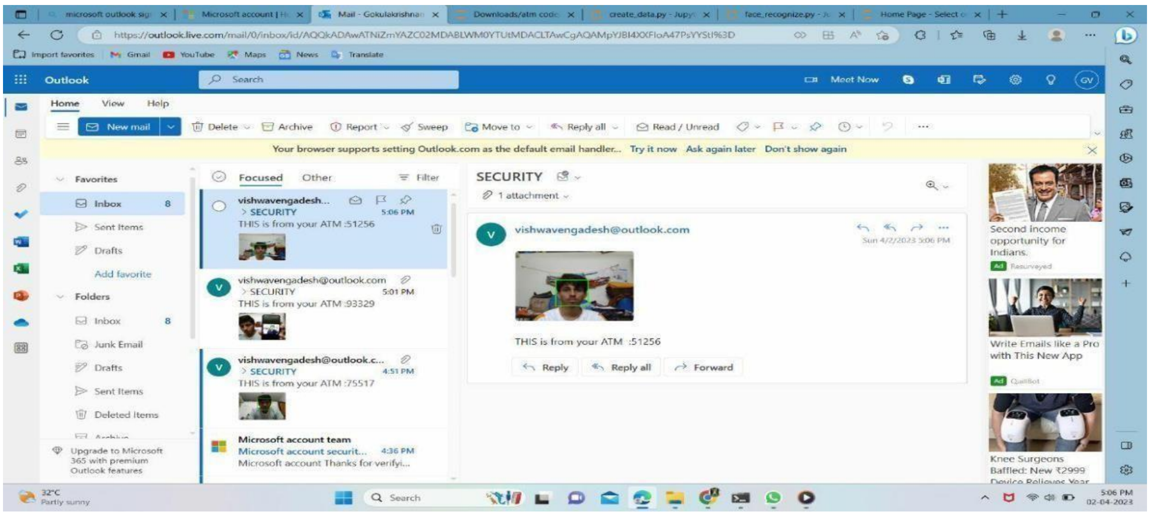

Fig 7.4.2 Represents OTP generate to the authorized person mail id. If OTP is correct proceed to transaction

7.4.3 STEP 3 ACCESSING KNOWN PERSON

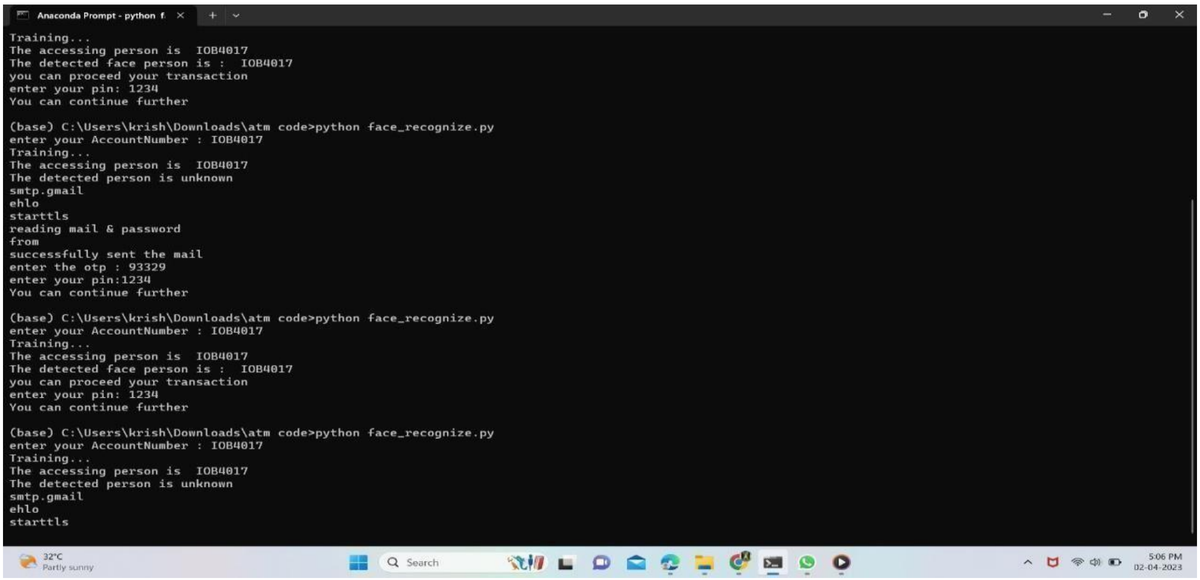

Fig 7.4.3Represents OTP is correct proceed to transaction

Result	**Recall**	**FI score**	**Precision**	**Accuracy**
Haar cascade Algorithm	0.81	0.81	0.86	0.80

CHAPTER 8

CONCLUSION AND FUTURE ENHANCEMENT

8.1 CONCLUSION

This project is aimed to reduce the risk involved in ATM machines that were installed in remote area, also the issue related to fraudulent transaction like misusing others card to withdraw money and etc.

So in order to overcome these challenges, we have developed solution that will leverage the ML & AI to restrict card access to only the authorized users those are identified by face recognition algorithm.

8.2 FUTURE ENHANCEMENT

The main theme of the project is to give full security for the transaction of money. Then it will give more secure using random password and face detection based using Haar and deep learning with the open-source computer vision in real time applications. For the next generation we can assign the all requirement in ATM machine using hardware part.

APPENDICES

APPENDIX I Coding

```
from flask import Flask,
render_template, request import os
import cv2
import
face_recogniti
on import
random
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import
MIMEMultipart app = Flask(_name_)
otp =
random.randint(100000,
999999)@app.route('/')
def home():
   return
render_template('home.html')
@app.route('/my_function',
methods=['POST'])def my_function():
if request.method == 'POST':
# Capture video stream from default
cameravideo_capture =
cv2.VideoCapture(0)

# Load dataset
```

```
dataset_path = r"C:\Users\DELL\Desktop\atm
code\datasets"images = []
names = []
for name in os.listdir(dataset_path):
person_folder_path = os.path.join(dataset_path,
name)for image_name in
os.listdir(person_folder_path):
image_path = os.path.join(person_folder_path, image_name)
image = face_recognition.load_image_file(image_path)
encoding = face_recognition.face_encodings(image)[0]
images.append(encoding)
    names.append(n
ame)print("works
fine")
# Initialize some variablesface_locations = []
face_encodings
= []face_names
= []
process_this_frame = Truewhile
True:# Grab a single frame of
video
ret, frame = video_capture.read()

# Resize frame of video to 1/4 size for faster face recognition processing
small_frame = cv2.resize(frame, (0, 0), fx=0.25, fy=0.25)
 # Convert the image from BGR color (which OpenCV uses) to RGB color
(whichface_recognition uses)
rgb_small_frame = small_frame[:, :, ::-1]
```

# Only process every other frame of video to save time if process_this_frame:
# Find all the faces and face encodings in the current frame of vide
face_locations = face_recognition.face_locations(rgb_small_frame)
face_encodings =
face_recognition.face_encodings(rgb_small_frame,face_locations) face_names = []
for face_encoding in face_encodings:
# See if the face is a match for the known face(s)
matches = face_recognition.compare_faces(images, face_encoding) name =
"Unknown"
# If a match was found in the dataset, use the first one if True in matches:
first_match_index = matches.index(True) name = names[first_match_index]
face_names.append(name) process_this_frame = not process_this_frame # Display the results
for (top, right, bottom, left), name in zip(face_locations, face_names):# Scale back up face locations since the frame we detected in
top *= 4
right *= 4
bottom *= 4
left *= 4
Draw a box around the face
cv2.rectangle(frame, (left, top), (right, bottom), (0, 0, 255), 2)# Draw a label with a name below the face

```
cv2.rectangle(frame, (left, bottom - 35), (right, bottom), (0, 0, 255), cv2.FILLED)
font = cv2.FONT_HERSHEY_DUPLEX
        cv2.putText(frame, name, (left + 6, bottom - 6), font, 1.0, (255, 255,
255), 1)# Display the resulting image
      # Display the resulting imagecv2.imshow('Video', frame)
if cv2.waitKey(1) & 0xFF == ord('q'):break
# Release handle to the webcamvideo_capture.release() cv2.destroyAllWindows()
# If a name is recognized, ask for the PINif name != 'Unknown':
  return render_template('pin.html', name=name)# If a name is not recognized,
send OTP to email else:
# Generate  a 6-digit  OTP# Send OTP to user's email
email = request.form['email']send_otp(email, otp)
      return render_template('otp.html', email=email)@app.route('/verify_otp',
methods=['POST'])
def verify_otp():
# Verify the OTP entered by the userentered_otp = request.form['otp'] email =
request.form['email']
if int(entered_otp) == otp:
  return render_template('success.html', name=name)else:
    return render_template('failure.html')def send_otp(email, otp):
# Code to send the OTP to the user's email
# This code will depend on the email service being used  pass
```

APPENDIX II - Publications in Conferences Publication

PUBLICATION

International conference on Advanced Techniques in Communication Networking and Automation

RESEARCH ARTICLE OPEN ACCESS

Third Generation ATM Machine usingAdvanced image processing

Vishwa Vengadesh D
GokulaKrishnan V
Sathish S
TamilSelvan S
B.E Computer science and Engineering
A.V.C college of Engineering
Mannampandal , Mayiladuthurai
krishcr7707@gmail.com
sathishsankar2310@gmail.com

Arunpandian A
Assistant Professor
A.V.C College of Engineering
Mannampandal, Mayiladuthurai

***Abstract*- Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. For example, ATMs are typically found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centers, airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry week for this purpose we are using face recognition step with haar cascade classifier to find out the features of face.when face is detected then it will give access to do transactions otherwise not allow.**

Keywords: Haar cascade, Automatic Teller Machine, Annaconda (Jupyter IDE), Machine learning,

I.Introduction

A computer-implemented method for cardless use of an automated teller machine (ATM) is provided. The method includes receiving as an input, a user-identified ATM that the user wishes to use. The method also includes generating and transmitting a one-time password (OTP) for the user to enter at the identified ATM. The method further includes receiving and verifying the OTP entered into the ATM, and on successful verification, authorizing access to services available through the ATM, without use of a card. To reduce the threat involved in ATM machines that were installed in remote area, also the issue related to fraudulent sale like misusing others card to withdraw plutocrat and etc. So in order to overcome these challenges, we've developed result that will work the ML & AI to circumscribe card access to only the authorized druggies those are linked by face recognition algorithm.

This method is useful in many fields such as the military, for security, schools, colleges and universities, airlines, banking, online web applications, gaming etc. this system uses powerful python algorithm through which the detection and recognition of face is very easy and efficient.

Surveillance cameras are an essential security precaution in all public places. In a centralised surveillance system, videos collected from

ARASU ENGINEERING COLLEGE

Approved by AICTE | Affiliated to Anna University Accredited by NBA | Accredited by NAAC | Recognized by UGC Under 2 (f) & 12 (b)
Chennai Main Road, Kumbakonam-612501

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

International Conference on Advanced Techniques in Communication, Networking and Automation (ICATCNA-23)

CERTIFICATE
OF PARTICIPATION

This is to certify that
Mr/Ms S. Sathish of
A.V.C College of Engineering
has Presented a Paper on the topic of
Third Generation ATM Machine using Advanced image processing
in the "International Conference on Advanced Techniques in Communication, Networking and Automation - ICATCNA" organized by the Department of Electronics and Communication Engineering on 26.04.2023.

Convener
HOD
Electronics and Communication Engineering
Arasu Engineering College
Kumbakonam

Principal
Arasu Engineering College
Kumbakonam

26.04.2023
Date

ARASU ENGINEERING COLLEGE

Approved by AICTE | Affiliated to Anna University Accredited by NBA | Accredited by NAAC | Recognized by UGC Under 2 (f) & 12 (b)
Chennai Main Road, Kumbakonam-612501

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

International Conference on Advanced Techniques in Communication, Networking and Automation (ICATCNA-23)

CERTIFICATE
OF PARTICIPATION

This is to certify that
Mr/Ms V. Gopala krishnan of
A.V.C college of Engineering
has Presented a Paper on the topic of
Third Generation ATM Machine using Advanced image processing
in the "International Conference on Advanced Techniques in Communication, Networking and Automation - ICATCNA" organized by the Department of Electronics and Communication Engineering on 26.04.2023.

Convener
HOD
Electronics and Communication Engineering
Arasu Engineering College
Kumbakonam

Principal
Arasu Engineering College
Kumbakonam

26.04.2023
Date

ARASU ENGINEERING COLLEGE

Approved by AICTE | Affiliated to Anna University Accredited by NBA | Accredited by NAAC | Recognized by UGC Under 2 (f) & 12 (b)

Chennai Main Road, Kumbakonam-612501

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

International Conference on Advanced Techniques in Communication, Networking and Automation (ICATCNA-23)

CERTIFICATE

OF PARTICIPATION

This is to certify that

Mr/Ms. D. Vishwa Vegadesh of

A.V.C college of Engineering

has Presented a Paper on the topic of

Third Generation ATM Machine using Advanced Image processing

in the "International Conference on Advanced Techniques in Communication, Networking and Automation - ICATCNA" organized by the Department of Electronics and Communication Engineering on 26.04.2023.

Convener
HOD
Electronics and Communication Engineering
Arasu Engineering College
Kumbakonam

Principal
Arasu Engineering College
Kumbakonam

26.04.2023
Date

ARASU ENGINEERING COLLEGE

Approved by AICTE | Affiliated to Anna University Accredited by NBA | Accredited by NAAC | Recognized by UGC Under 2 (f) & 12 (b)

Chennai Main Road, Kumbakonam-612501

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

International Conference on Advanced Techniques in Communication, Networking and Automation (ICATCNA-23)

CERTIFICATE

OF PARTICIPATION

This is to certify that

Mr/Ms. S. Tamil Selvan of

A.V.C College of Engineering

has Presented a Paper on the topic of

Third Generation ATM Machine Using Advanced image processing

in the "International Conference on Advanced Techniques in Communication, Networking and Automation - ICATCNA" organized by the Department of Electronics and Communication Engineering on 26.04.2023.

Convener
HOD
Electronics and Communication Engineering
Arasu Engineering College
Kumbakonam

Principal
Arasu Engineering College
Kumbakonam

26.04.2023
Date

REFERNCES

[1]Cao, K., Liu, M., Su, H., Wu, J., Zhu, J., & Liu, S. (2020). Analyzing the noise robustness of deep neural networks. *IEEE Transactions on Visualization and Computer Graphics*, *27*(7), 3289-3304.

[2]Ferdinand, J., Wijaya, C., Ronal, A. N., Edbert, I. S., & Suhartono, D. (2022, September). ATM Security System Modeling Using Face Recognition with FaceNet and Haar Cascade. In 2022 6th International Conference on Informatics and Computational Sciences (ICICoS) (pp. 111-116). IEEE.

[3]Jacintha, V., Nagarajan, J., Yogesh, K. T., Tamilarasu, S., & Yuvaraj, S. (2017, December). An IOT based ATM surveillance system. In *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-6). IEEE.

[4]Li, Y., Liu, L., Lin, L., & Wang, Q. (2017). Face recognition by coarse-to-fine landmark regression with application to atm surveillance. In Computer Vision: Second CCF Chinese Conference, CCCV 2017, Tianjin, China, October 11–14, 2017, Proceedings, Part II (pp. 62-73). Springer Singapore.

[5]Miarnaeimi, H., & Davari, P. (2008). A new fast and efficient HMM-based face recognition system using a 7-state HMM along with SVD coefficients.

[6]Mohite, A., Gamare, S., More, K., & Patil, N. (2019). Deep Learning based Card-Less Atm using Fingerprint and Face Recognition Techniques. International Research Journal of Multidisciplinary Technovation (IRJMT), 6(3), 3504-3509.

[7]Moussa, M., Hamila, M., & Douik, A. (2021). Face recognition using fractional coefficients and discrete cosine transform tool. International Journal of Electrical and Computer Engineering (IJECE), 11(1), 892-899.

[8]Sasipriya, D. S., Kumar, D. P., & Shenbagadevi, S. (2020). Face Recognition Based New Generation ATM System. European Journal of Molecular & Clinical Medicine, 7(4), 2854-2865.

[9]Wang, H., & Guo, L. (2021, October). Research on face recognition based on deep learning. In *2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM)* (pp. 540-546). IEEE.