A Mini Project

On

Face Recognition System Using Cascade With OpenCV

for the award of the degree of Bachelor of Technology

In

Computer Science and Engineering

By

Gaurav Kumar Verma

(2004920100021)

Aditya Pandey

(2004921530001)

Pratyush Harsh

(2004920100035)

Under the guidance of

Mr. Balak Ram, Asst Professor/Asso Prof/Prof

Dept of Computer Science

Department of Computer Science and engineering

KCC INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(Affiliated to Dr. A.P.J. Abdul Kalam Technical University, Approved by AICTE)

Knowledge Park-III, Greater Noida, Uttar Pradesh 201306

KCC INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(Affiliated to Dr. A.P.J. Abdul Kalam Technical University, Approved by AICTE)
Knowledge Park-III, Greater Noida,
Uttar Pradesh 201306

Department of computer science and Engineering

This is to certify that the project entitled “Face Recognition System using Cascade Classifier With OpenCV” being submitted by Gaurav Kumar Verma bearing the Hall Ticket number 2004920100021, Aditya Pandey bearing the Hall Ticket number 2004921530001 and Pratyush Harsh bearing the Hall Ticket number 2004920100035 in partial fulfilment of the requirements for the award of the degree of the Bachelor of Technology in Computer Science and Engineering to KCC Group of Institutions is a record of bonafide work carried out by them under my guidance and supervision from September 2022 to December 2022.

The results presented in this project have been verified and found to be satisfactory. The results embodied in this project report have not been submitted to any other or University for the award of any other degree diploma.

Internal Guide

Mr. Balak Ram
(Asst. Professor, Dept of CSE)

External Examiner

Dr Sanjay kumar,

Professor and Head, Dept. of CSE

ACKNOWLEDGEMENT

It is our privilege and pleasure to express a profound sense of respect, gratitude and indebtedness to our Mr. Balak Ram, Assistant Professor, Dept. of Computer Science and Engineering, KCC Group of Institutions for his/her indefatigable inspiration, guidance, cogent discussion, constructive criticisms and encouragement throughout this dissertation work.

We express our sincere gratitude to Dr Sanjay, Associate Professor & Head, Department of Computer Science and Engineering, KCC Group of Institutions, for his suggestions, motivations and co-operation for the successful completion of the work.

We extend our sincere thanks to Mr. Deepak Gupta, Chairman, KCC Group of Institutions for his encouragement.

Gaurav Kumar Verma – 2004920100021

Aditya Pandey - 2004921530001

Pratyush Harsh - 2004920100035

DECLARATION

We hereby declare that the project work entitled “Face Recognition System using Cascade Classifier With OpenCV” submitted to the KCC Group of Institutions in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology (B.Tech) in Computer Science and Engineering is a record of an original work done by us under the guidance of Guide Name, Assistant Professor and this project work have not been submitted to any other university for the award of any other degree or diploma.

Gaurav Kumar Verma – 2004920100021

Aditya Pandey - 2004921530001

Pratyush Harsh - 2004920100035

CONTENTS

Face Recognition System using Cascade Classifier with OpenCV

Mr. Balak Ram, Gaurav Kumar Verma, Aditya Pandey, Pratyush Harsh
[*]Asst. Professor, B.Tech Student
KCC ITM, Greater Noida, Uttar Pradesh

ABSTRACT

While humans can recognize faces without much effort, facial recognition is a challenging pattern recognition problem in computing. Facial recognition systems attempt to identify a human face, which is three-dimensional and changes in appearance with lighting and facial expression, based on its two-dimensional image. To accomplish this computational task, facial recognition systems perform four steps. First face detection is used to segment the face from the image background. In the second step the segmented face image is aligned to account for face pose, image size and photographic properties, such as illumination and grayscale. The purpose of the alignment process is to enable the accurate localization of facial features in the third step, the facial nature extraction. Features such as eyes, nose and mouth are pinpointed and measured in the image to represent the face. The so established feature vector of the face is then, in the fourth step, matched against a database of faces.

INTRODUCTION

Face recognition is the technique in which the identity of a human being can be identified using ones individual face. Such kind of systems can be used in photos, videos, or in real time machines. The objective of this article is to provide a simpler and easy method in machine technology. With the help of such a technology one can easily detect the face by the help of dataset in similar matching appearance of a person. The method in which with the help of python and OpenCV in deep learning is the most efficient way to detect the face of the person. 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.

LITERATURE SURVEY

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past years. At least two reasons account for this trend: the rest is the wide range of commercial and law

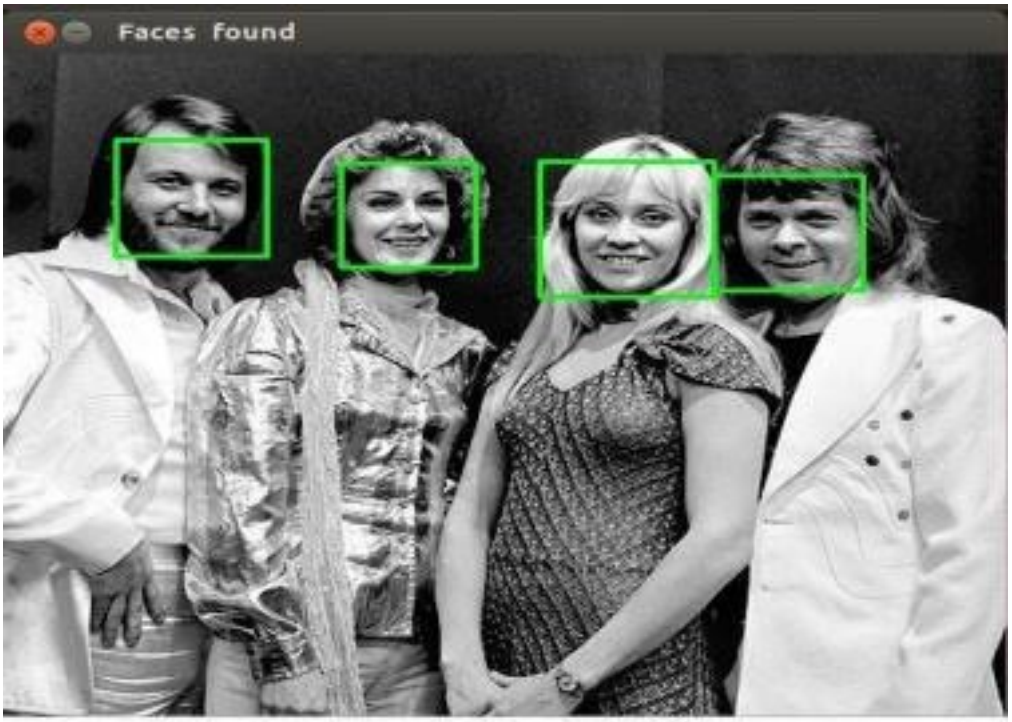
enforcement applications, and the second is the availability of feasible technologies after 30 years of research. Even though current machine recognition systems have reached a certain level of maturity, their success is limited by the conditions imposed by many real applications. For example, recognition of face images acquired in an outdoor environment with changes in illumination and/or pose remains a largely unsolved problem. In other words, current systems are still far away from the capability of the human perception system. This

paper provides an up-to-date critical survey of still- and video-based face recognition research. The accuracy of the system will be tested via recognition of three peoples with multiple times at different locations, mainly to test how light

intensity affect the accuracy of the system. The accuracy is verified using confusion matrix. The calculation is based on (1). ((TN + TP) / Total) x 100% (1) where TN is true negative while TP is true positive.

METHODOLOGY

To do face recognition, there must be an input to be detected and verified. Hence, an image sensor or typically a camera has to be set up for recording or capturing images. The camera should be compatible with the software used. The next step is the input image. The input can be images and recorded video or real-time video. After the input is provided, faces in the images or videos are to be detected. When the classifier is trained, it can be utilized to start to recognition work. It can be used in either video or image to recognize one or more person. Different set of python scripts are provided to run the different type of recognition. The python script will import the classifier that is trained in previous step in order to carry out the recognition for the person from the camera or from an image.

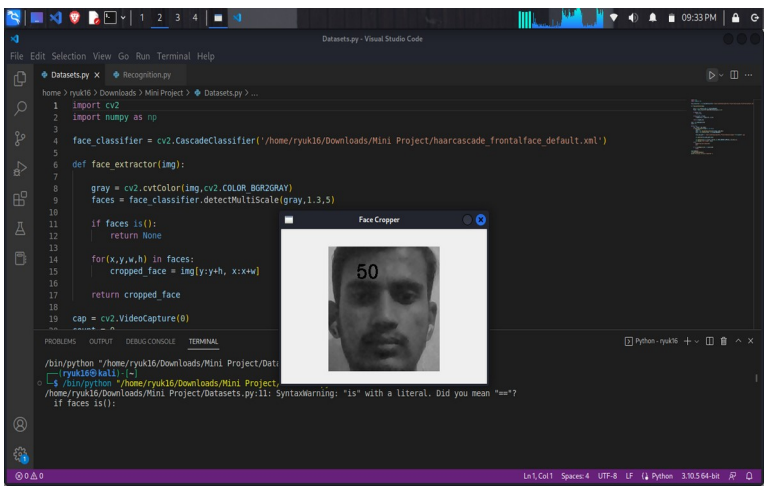


Source Code

Datasets :

```
import cv2
import numpy as np
face_classifier = cv2.CascadeClassifier('/home/ryuk16/Downloads/Mini
Project/haarcascade_frontalface_default.xml')
def face_extractor(img):
gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)
faces = face_classifier.detectMultiScale(gray,1.3,5)
if faces is():
return None
for(x,y,w,h) in faces:
cropped_face = img[y:y+h, x:x+w]
return cropped_face
cap = cv2.VideoCapture(0)
count = 0
while True:
ret, frame = cap.read()
if face_extractor(frame) is not None:
count+=1
face = cv2.resize(face_extractor(frame),(200,200))
face = cv2.cvtColor(face, cv2.COLOR_BGR2GRAY)
file_name_path = '/home/ryuk16/Downloads/Mini Project/Datasets/Images/'+str(count)
+'.jpg'
cv2.imwrite(file_name_path,face)
cv2.putText(face,str(count),(50,50),cv2.FONT_HERSHEY_COMPLEX,1,(0,255,0),2)
cv2.imshow('Face Cropper',face)
else:
print("Face Not Detected")
pass
if cv2.waitKey(1)==13 or count==100:
break
cap.release()
cv2.destroyAllWindows()
print('Prototype Colletion Completed ')
```

Output :

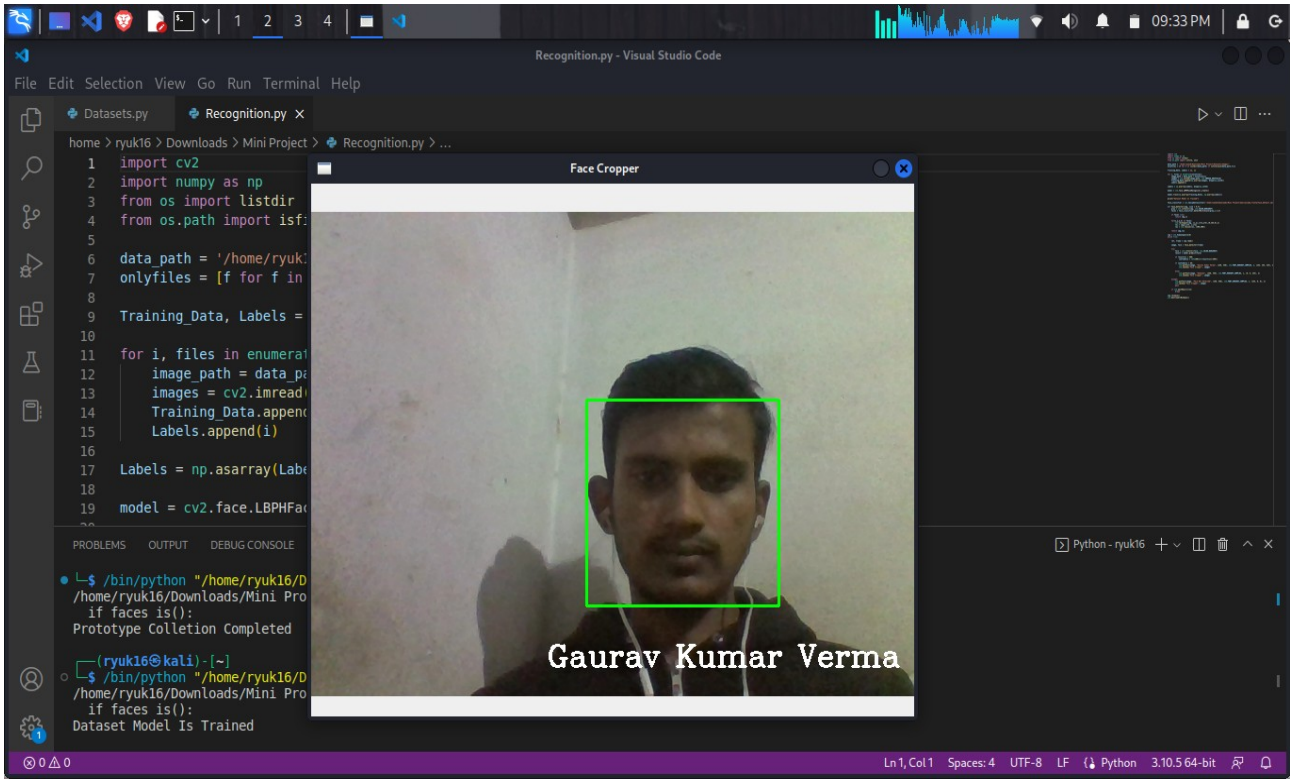


Recognition :

```
import cv2
import numpy as np
from os import listdir
from os.path import isfile, joi
data_path = '/home/ryuk16/Downloads/Mini Project/Datasets/Images/'
onlyfiles = [f for f in listdir(data_path) if isfile(join(data_path,f))]
Training_Data, Labels = [], []
for i, files in enumerate(onlyfiles):
image_path = data_path + onlyfiles[i]
images = cv2.imread(image_path, cv2.IMREAD_GRAYSCALE)
Training_Data.append(np.asarray(images, dtype=np.uint8))
Labels.append(i)
Labels = np.asarray(Labels, dtype=np.int32)
model = cv2.face.LBPHFaceRecognizer_create()
model.train(np.asarray(Training_Data), np.asarray(Labels))
print("Dataset Model Is Trained")
face_classifier = cv2.CascadeClassifier('/home/ryuk16/Downloads/Mini
Project/haarcascade_frontalface_default.xml')
def face_detector(img, size = 0.5):
gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
faces = face_classifier.detectMultiScale(gray,1.3,5)
if faces is():
return img,[]
for(x,y,w,h) in faces:
cv2.rectangle(img, (x,y),(x+w,y+h),(0,255,0),2)
roi = img[y:y+h, x:x+w]
roi = cv2.resize(roi, (200,200))
return img,roi
cap = cv2.VideoCapture(0)
while True:
ret, frame = cap.read()
image, face = face_detector(frame)
try:
face = cv2.cvtColor(face, cv2.COLOR_BGR2GRAY)
result = model.predict(face)
if result[1] < 500:
confidence = int(100*(1-(result[1])/300))
if confidence > 86:
cv2.putText(image, "Gaurav Kumar Verma", (250, 450),
cv2.FONT_HERSHEY_COMPLEX, 1, (255, 255, 255), 2)
cv2.imshow('Face Cropper', image)
else:
cv2.putText(image, "Unknown", (250, 450), cv2.FONT_HERSHEY_COMPLEX, 1, (0, 0,
255), 2)
cv2.imshow('Face Cropper', image)
```

```
except:
cv2.putText(image, "Face Not Detected", (250, 450), cv2.FONT_HERSHEY_COMPLEX,
1, (255, 0, 0), 2)
cv2.imshow('Face Cropper', image)
pass
if cv2.waitKey(1)==13:
break
cap.release()
cv2.destroyAllWindows()
```

Output :



Advantages of face recognition

Aside from unlocking your smartphone, facial recognition brings other benefits:

1. Increased security :

On a governmental level, facial recognition can help to identify terrorists or other criminals. On a personal level, facial recognition can be used as a security tool for locking personal devices and for personal surveillance cameras.

2. Reduced crime :

Face recognition makes it easier to track down burglars, thieves, and trespassers. The sole knowledge of the presence of a face recognition system can serve as a deterrence, especially to petty crime. Aside from physical security, there are benefits to cybersecurity as well. Companies can use face recognition technology as a substitute for passwords to access computers. In theory, the technology cannot be hacked as there is nothing to steal or change, as is the case with a password.

3. Removing bias from stop and search :

Public concern over unjustified stops and searches is a source of controversy for the police — facial recognition technology could improve the process. By singling out suspects among crowds through an automated rather than human process, face recognition technology could help reduce potential bias and decrease stops and searches on law-abiding citizens.

4. Greater convenience :

As the technology becomes more widespread, customers will be able to pay in stores using their face, rather than pulling out their credit cards or cash. This could save time in checkout lines. Since there is no contact required for facial recognition as there is with fingerprinting or other security measures – useful in the post-COVID world – facial recognition offers a quick, automatic, and seamless verification experience.

5. Faster processing :

The process of recognizing a face takes only a second, which has benefits for the companies that use facial recognition. In an era of cyber-attacks and advanced hacking tools, companies need both secure and fast technologies. Facial recognition enables quick and efficient verification of a person’s identity.

6. Integration with other technologies :

Most facial recognition solutions are compatible with most security software. In fact, it is easily integrated. This limits the amount of additional investment required to implement it.

Disadvantages of face recognition

While some people do not mind being filmed in public and do not object to the use of facial recognition where there is a clear benefit or rationale, the technology can inspire intense reactions from others. Some of the disadvantages or concerns include:

1. Surveillance :

Some worry that the use of facial recognition along with ubiquitous video cameras, artificial intelligence, and data analytics creates the potential for mass surveillance, which could restrict individual freedom. While facial recognition technology allows governments to track down criminals, it could also allow them to track down ordinary and innocent people at any time.

2. Scope for error :

Facial recognition data is not free from error, which could lead to people being implicated for crimes they have not committed. For example, a slight change in camera angle or a change in appearance, such as a new hairstyle, could lead to error. In 2018, Newsweek reported that Amazon’s facial recognition technology had falsely identified 28 members of the US Congress as people arrested for crimes.

3. Breach of privacy :

The question of ethics and privacy is the most contentious one. Governments have been known to store several citizens' pictures without their consent. In 2020, the European Commission said it was considering a ban on facial recognition technology in public spaces for up to five years, to allow time to work out a regulatory framework to prevent privacy and ethical abuses.

4. Massive data storage :

Facial recognition software relies on machine learning technology, which requires massive data sets to “learn” to deliver accurate results. Such large data sets require robust data storage. Small and medium-sized companies may not have sufficient resources to store the required data.

How Facial Recognition Works

First, some basic definitions:

1. AI applies algorithms to vast amounts of data to accelerate information processing and decision making.

2. AI-based facial recognition technology is software that can quickly search large databases of faces and compare them to a face or faces that have been detected in a photo or video.

A widely accepted definition of facial recognition as introduced to the U.S. Congress:

FACIAL RECOGNITION TECHNOLOGY:

The term “facial recognition technology” means the automated or semiautomated process that assists in identifying or verifying an individual based on the characteristics of an individual’s face.

It must be noted that people often conflate “facial recognition technology” with other types of software. For instance, the National Human Genome Research Institute uses “face analysis technology” to detect a rare genetic disease. This application would not be considered FRT because no identification component is used during the facial analysis process. There are other examples, but the above definition will be applied for this publication.

Technology Can Be a Two-Edged Sword

As history has demonstrated, technology can be a two-edged sword for minorities, and this is especially true when it comes to FRT. For example:

1. As the accuracy of FRT systems continues to improve, the potential for errors in high-risk uses to affect disadvantaged communities must be reduced.

2. The lack of workforce diversity and inclusivity has resulted in many advances in technology being used to harm or disadvantage minorities, especially Black Americans. There are multiple layers of racial equity dilemmas regarding technology, but two of the areas that need the most significant overhaul include:

° The general workplace inclusion
° The fair use of the technology in the field.

The use of facial recognition technology is growing exponentially, and it has provided many benefits. But unless technology industry leaders and stakeholders find a way to eliminate bias and increase diversity at all levels, the benefits of facial recognition will be stifled and calls to ban the technology will continue.

The facial recognition market is substantial, estimated to be $5.01 billion in 2021, and researchers expect it to grow to $12.67 billion by 2028. It is used in many ways, such as allowing you to:

° Go through security at the airport
° Unlock your phone
° Purchase products at stores

Facial recognition has many benefits, especially regarding security and law enforcement. These benefits are crucial for Black, Hispanic and indigenous communities where the number of missing children and unsolved murders is tragically high. The uses of FRT in many cases and the resulting benefits are lawful, ethical and nondiscriminatory, such as:

° Detecting identity fraud
° Preventing potential terrorist attacks
° Helping find and rescue human sex trafficking victims

Law enforcement agencies use the technology to uncover criminals or find missing children or seniors. In New York, police apprehended an accused rapist using facial recognition technology within 24 hours of an incident where he threatened a woman with rape at knifepoint. Additionally, proper use of the technology can reduce the interpersonal interaction of minorities with police and law enforcement, reducing the chances for adverse consequences.

Airports are increasingly adding facial recognition technology to security checkpoints; the U.S. Department of Homeland Security predicts that 97% of travelers will use FRT to authenticate their travel documents by 2023. Also, in cities with soaring crime rates, business owners have installed facial recognition systems to alert staff when individuals known to be involved in organized retail crime enter their places of business.

And further, there are many real-world examples of how it has been beneficial:

° Taylor Swift, the entertainer, used the technology to identify her stalkers as they came through the gate at her Rose Bowl concert in May 2018
° New York City Police used FRT to identify a potential terrorist suspect who left a pair of rice cookers in a subway station
° A nonprofit group used FRT to help rescue 15,000 children and identify 17,000 sex traffickers

Facial Recognition Security

While biometric data is generally considered one of the most reliable authentication methods, it also carries significant risk. That's because if someone's credit card details are hacked, that person has the option to freeze their credit and take steps to change the personal information that was breached. What do you do if you lose your digital 'face'?

Around the world, biometric information is being captured, stored, and analyzed in increasing quantities, often by organizations and governments, with a mixed record on cybersecurity. A question increasingly being asked is, how safe is the infrastructure that holds and processes all this data?

As facial recognition software is still in its relative infancy, the laws governing this area are evolving (and sometimes non-existent). Regular citizens whose information is compromised have relatively few legal avenues to pursue. Cybercriminals often elude the authorities or are sentenced years after the fact, while their victims receive no compensation and are left to fend for themselves.

As the use of facial recognition becomes more widespread, the scope for hackers to steal your facial data to commit fraud — increases.

A comprehensive cybersecurity package is an essential part of protecting your online privacy and security. We recommend Kaspersky Security Cloud which provides protection for all your devices and includes antivirus, anti-ransomware, mobile security, password management, VPN, and parental controls.

Biometric technology offers very compelling security solutions. Despite the risks, the systems are convenient and hard to duplicate. These systems will continue to develop in the future — the challenge will be to maximize their benefits while minimizing their risks.

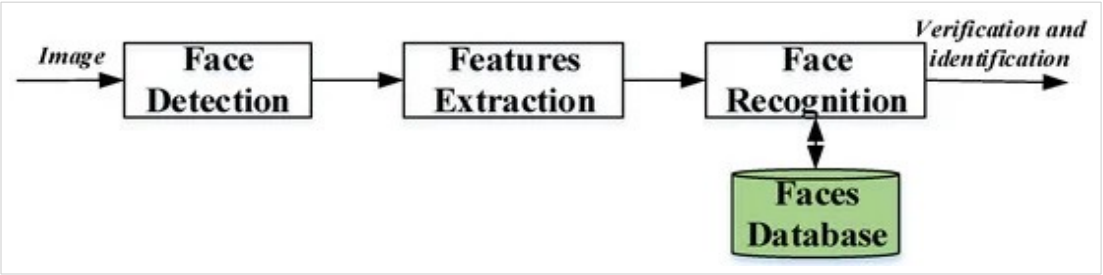
Systems Survey

Before detailing the techniques used, it is necessary to make a brief description of the problems that must be faced and solved in order to perform the face recognition task correctly. For several security applications, as detailed in the works of, the characteristics that make a face recognition system useful are the following: its ability to work with both videos and images, to process in real time, to be robust in different lighting conditions, to be independent of the person (regardless of hair, ethnicity, or gender), and to be able to work with faces from different angles. Different types of sensors, including RGB, depth, EEG, thermal, and wearable inertial sensors, are used to obtain data. These sensors may provide extra information and help the face recognition systems to identify face images in both static images and video sequences. Moreover, three categories of sensors that may improve the reliability and the accuracy of a face recognition system by tackling the challenges include illumination variation, head pose, and facial expression in pure image/video processing.

The first group is non-visual sensors, such as audio, depth, and EEG sensors, which provide extra information in addition to the visual dimension and improve the recognition reliability, for example, in illumination variation and position shift situation. The second is detailed-face sensors, which detect a small dynamic change of a face component, such as eye-trackers, which may help differentiate the background noise and the face images.

The last is target-focused sensors, such as infrared thermal sensors, which can facilitate the face recognition systems to filter useless visual contents and may help resistance illumination variation.

Three basic steps are used to develop a robust face recognition system: (1) face detection, (2) feature extraction, and (3) face recognition. The face detection step is used to detect and locate the human face image obtained by the system. The feature extraction step is employed to extract the feature vectors for any human face located in the first step. Finally, the face recognition step includes the features extracted from the human face in order to compare it with all template face databases to decide the human face identity.



● *Face Detection:*

The face recognition system begins first with the localization of the human faces in a particular image. The purpose of this step is to determine if the input image contains human faces or not. The variations of illumination and facial expression can prevent proper face detection. In order to facilitate the design of a further face recognition system and make it more robust, pre-processing steps are performed. Many techniques are used to detect and locate the human face image, for example, Viola–Jones detector, histogram of oriented gradient (HOG), and principal component analysis (PCA). Also, the face detection step can be used for video and image classification, object detection, region-of-interest detection, and so on.

● *Feature Extraction:*

The main function of this step is to extract the features of the face images detected in the detection step. This step represents a face with a set of features vector called a "signature" that describes the prominent features of the face image such as mouth, nose, and eyes with their geometry distribution. Each face is characterized by its structure, size, and shape, which allow it to be identified. Several techniques involve extracting the shape of the mouth, eyes, or nose to identify the face using the size and distance. HOG, Eigenface, independent component analysis (ICA), linear discriminant analysis (LDA), scale-invariant feature transform (SIFT), gabor filter, local phase quantization (LPQ), Haar wavelets, Fourier transforms, and local binary pattern (LBP) techniques are widely used to extract the face features.

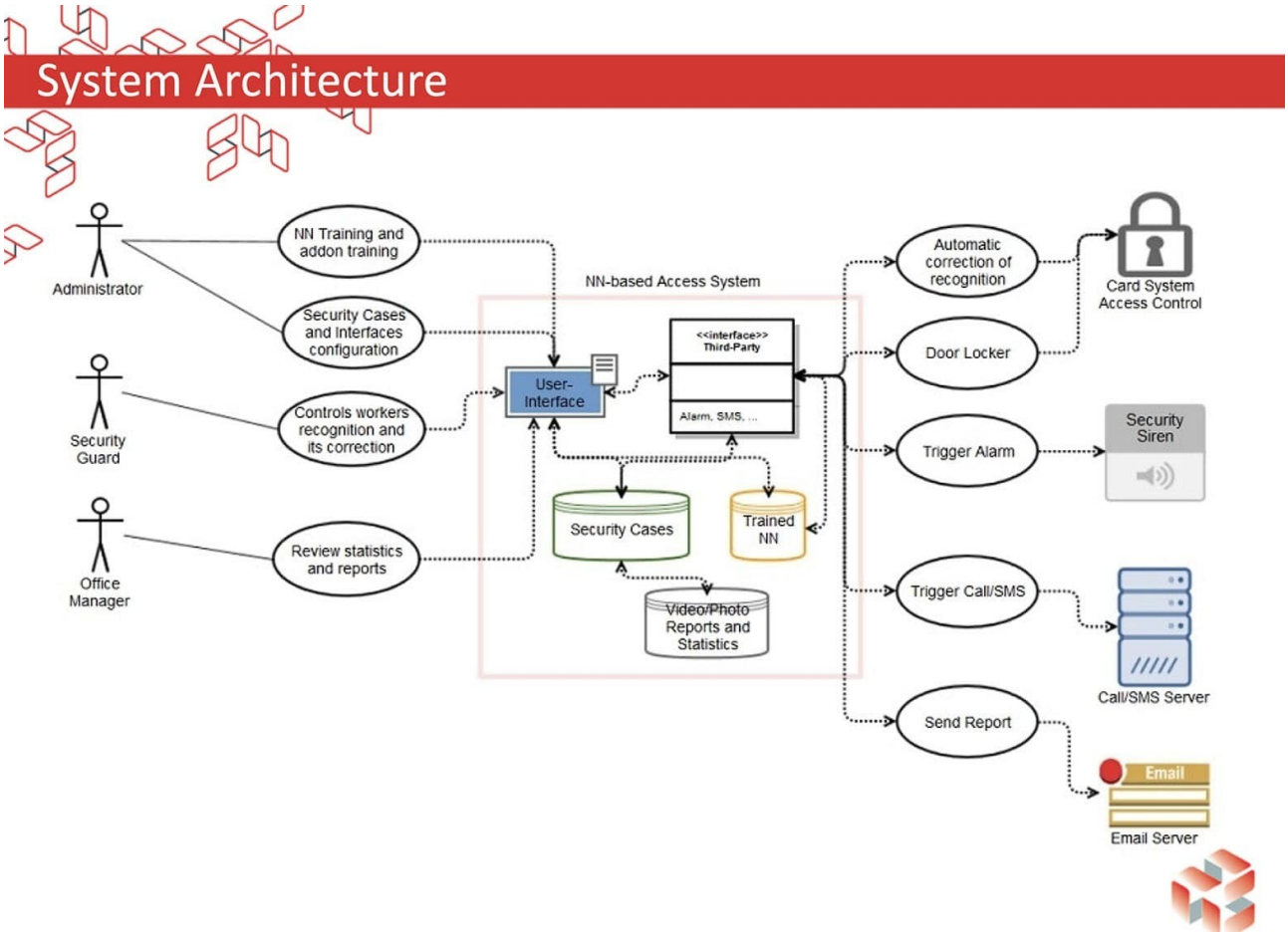
● *Face Recognition:*

This step considers the features extracted from the background during the feature extraction step and compares it with known faces stored in a specific database. There are two general applications of face recognition, one is called identification and another one is called verification. During the identification step, a test face is compared with a set of faces aiming to find the most likely match. During the identification step, a test face is compared with a known face in the database in order to make the acceptance or rejection decision. Correlation filters (CFs), convolutional neural network and also k-nearest neighbor (K-NN) are known to effectively address this task.

Proposed Work

The proposed system gives an approach to mark an individual's user using their facial features. It functions through frame by frame processing of live feed obtained from a camera to find a face. Upon face detection, the area in frame occupied by face is considered as the region of interest, and various operation like color-correction and face alignment is done to obtain better results followed by feature extraction. Collected features are then processed by the trained model which yields the result subjected to the confidence score. An Illustration of the proposed architecture is given in Figure. The proposed system uses MTCNN (Multi-Task Cascaded Convolutional Neural Networks).

The performance and accuracy of MTCNN is state of the art and is being used in the development. The process of feature extraction from the region of interest is done using FACENET. It is developed by Google and used to extract the features from the face which is very crucial for facial recognition. The proposed system also has self-learning capability and thus it works by updating the model automatically after regular intervals to perform efficiently with changing features of the children and adults. The user data will be stored on a server and can be retrieved when required using APIs (application programming interfaces).



System Requirement

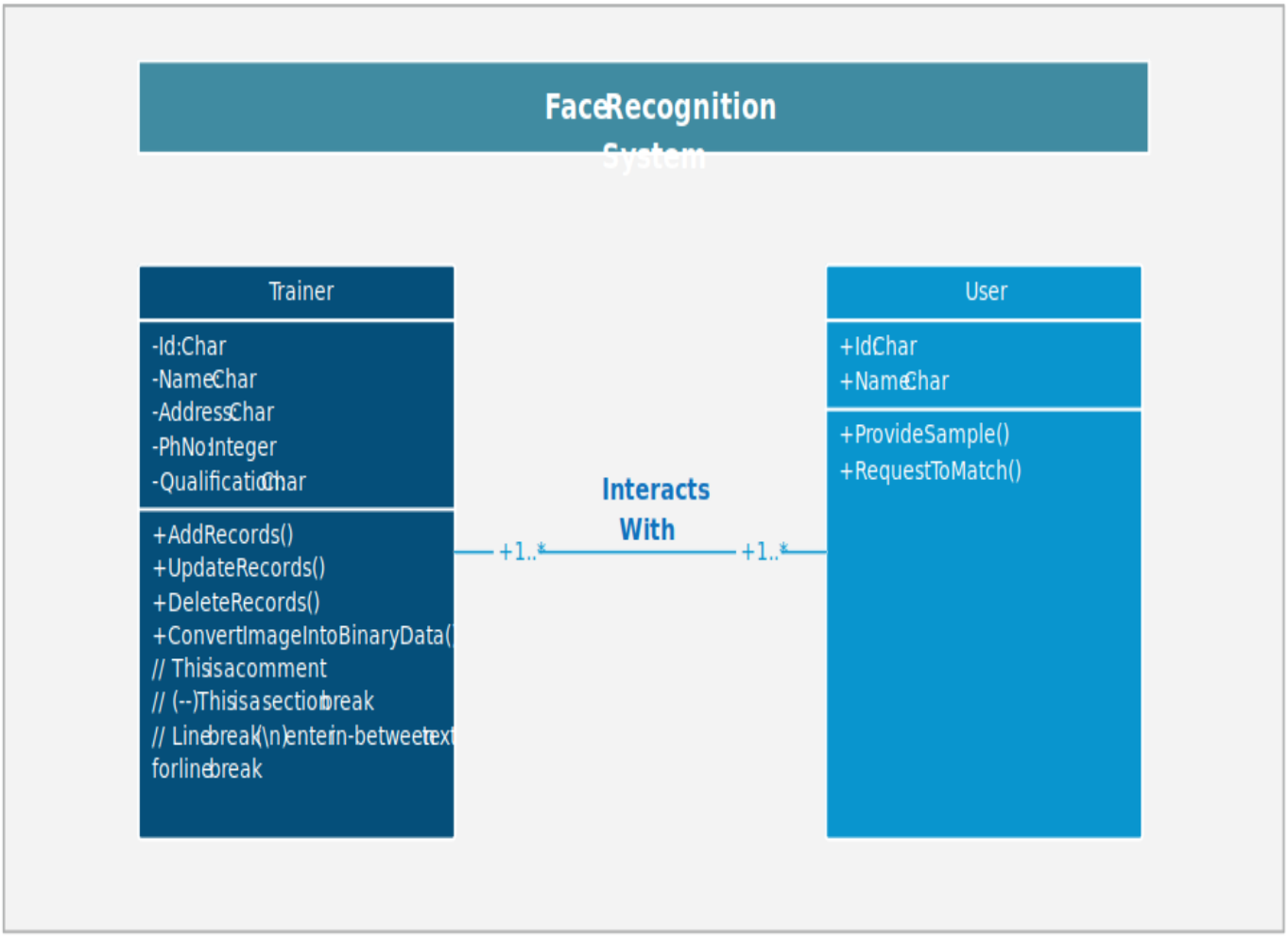
Hardware Requirements:

Processor : Intel Dual Core or Advance.
Hard Disk : Minimum 80 GB.
Display : LCD/LED Colour.
Accessories : Web Cam, Keyboard & Mouse.
RAM : Minimum 2 GB.

Software Requirements:

Operating system : Microsoft Windows 7 or Higher Versions, Linux.
Programming Language : Pycharm with Python 11.2.
Database : Cascade with OpenCV.

UML DIAGRAM



RESULTS

Face recognition systems are currently associated with many top technological companies and industries making the work of face recognition easier. The use of python programming and OpenCV makes it an easier and handy tool or system which can be made by anyone according to their requirement. The proposed system discussed in this project will be helpful for many as it is user friendly and cost_ efficient system. Hence by the use of python and OpenCV the face recognition system can be designed for various purposes.

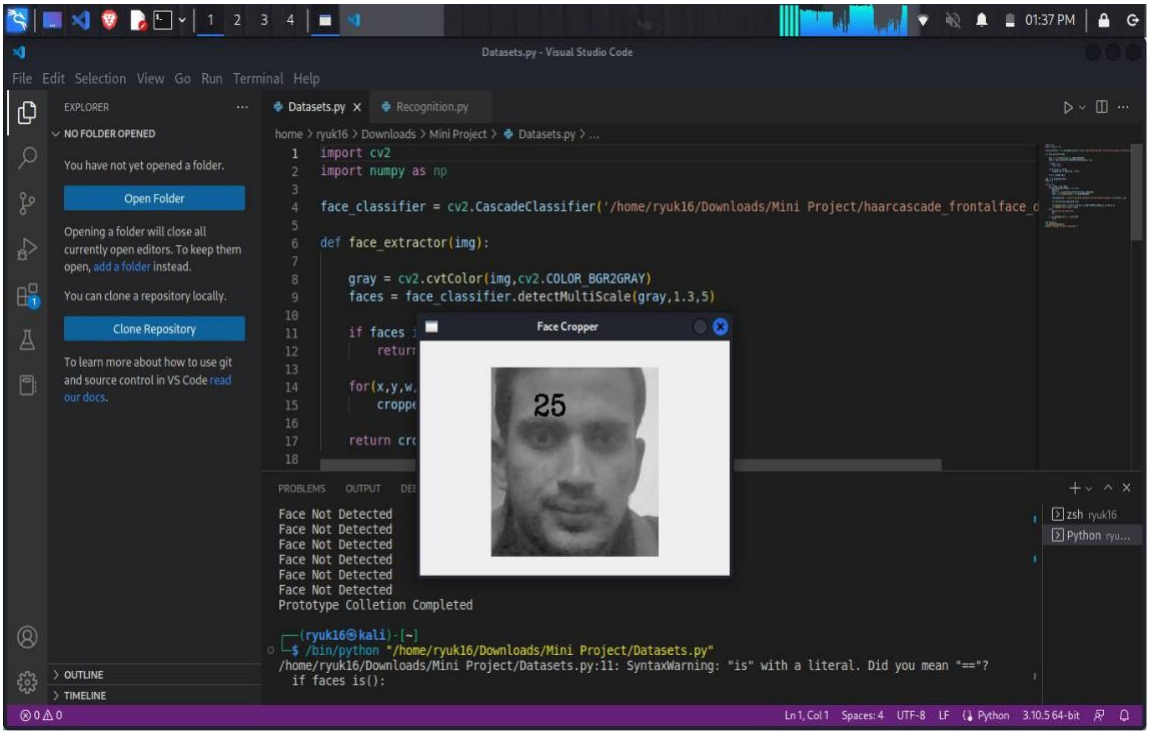


Figure 1: Collecting Samples

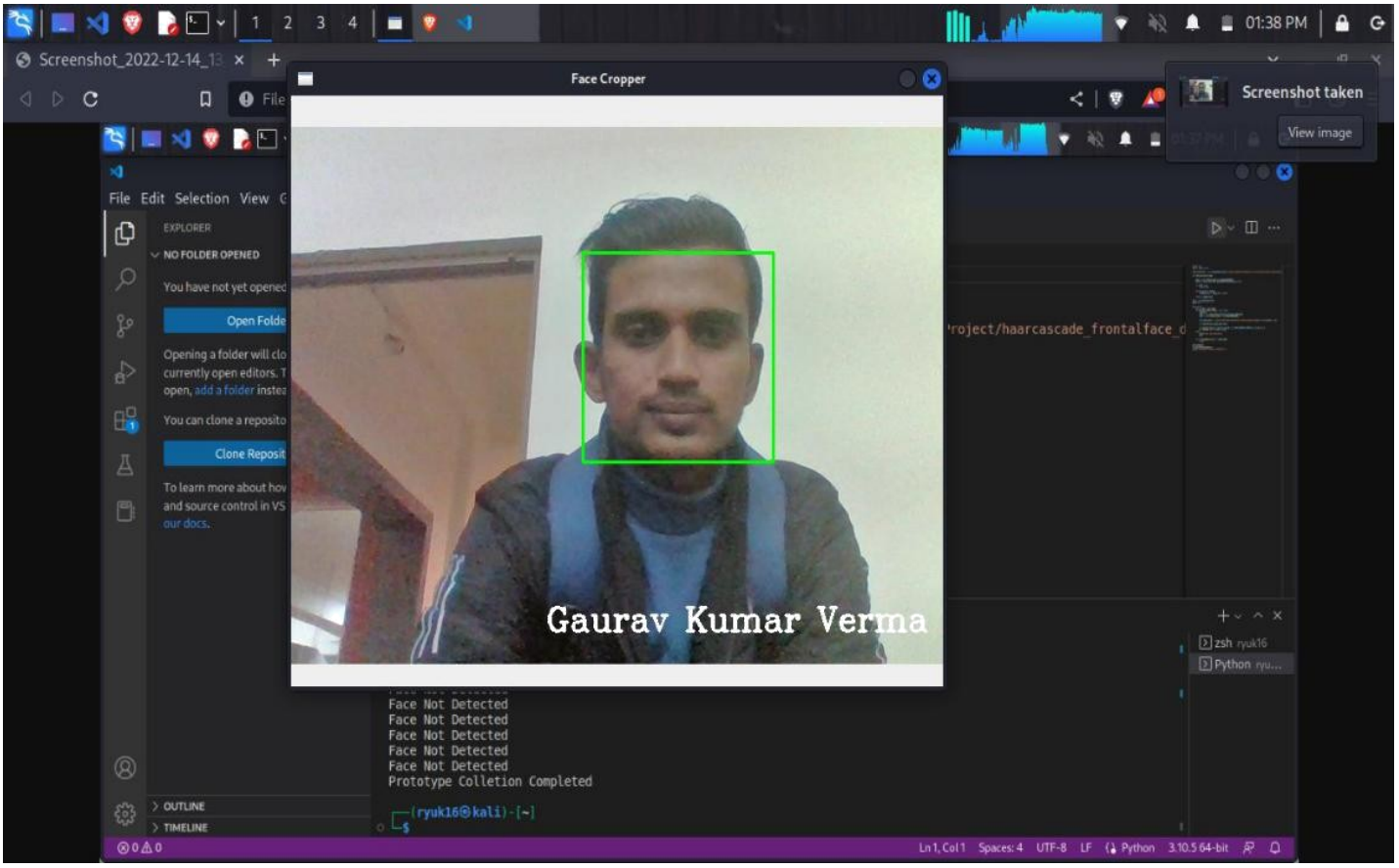


Figure 2: Face Recognition Using OpenCV

Analysis

The proposed system has been implemented and tested in python programming language and the system works fine.

The proposed system has some shortcomings though which are mentioned below:

- The system is unable to mark user in a darker room or at night. However, this problem can be fixed by having a light source mounted with the system and when the system detects dark frames it should turn the light source on automatically using.

- The system is slow and lags on the average system. However, with GPU enabled modern computers or using cloud computing this problem can easily be solved.

Table 1 : Test results analysis on face recognition with user system interface

No. of Test	No. of Person	Time for Login	No. of Frames for Recognition	Average Credibility	No. of Error Recognition
1	A	-	3	0.89	0
2	A	15	7	0.65	0
3	B	-	10	0.76	0
4	A		10	0.45	0
5	A	12	10	0.99	0
6	B	18	11	0.56	0
7	C	-	10	0.78	0
8	A		11	0.56	0
9	C	11	10	0.91	0
10	A	-	10	0.96	0
11	B	-	11	0.87	0
12	A	16	10	0.46	0
13	A		10	0.78	0
14	B	-	7	0.65	0
15	B	17	9	0.96	0
16	B	-	10	0.71	0

Table 1 : Shows the login time and error detection using user interface system. Numbers of frames are divided to calculate average credibility. Login time consumed as well as well detection area of any object, in terms of object we captured one scene and recognized from the scale of pattern.

Conclusion

On referring various papers we come to understand the challenges faced in Face Detection and the various methodologies used to detect face. From this Literature Survey we have following take-aways: It is very important to remove background information. Removing irrelevant information, such as noise and non-face part would make face detection less complicated. Feature based analysis is one of the predominant methodology that most of the Detection Algorithms use in one way or another. Hence, efficient feature selection is very crucial. We must chose at-least two features for face identification. Because, depending only on one feature might result in erroneous detection. Varied Facial Expression and poses makes face detection more complicated.

Lightning conditions greatly affects face detection. Computations need to be fast and should require less main memory as majority of application are of real time in nature. When going through the cascade like methodology, re-computation of an already computed face must be avoided. It is very essential for a methodology to define its definition of face and successful face detection. As we saw that the elliptical face method did not consider ears as part of face whereas other methods did. Thus, definition of terms is important.

Different methods and approaches of face mask detection and recognition have been reviewed in this paper. In comparison, Haar-like features are digital image features used in object recognition. They owe their name to their intuitive similarity with Haar wavelets and were used in the first realtime face detector. The key advantage of a Haar-like feature over most other features is its calculation speed. Adaboost can be less susceptible to the over fitting problem than most learning algorithms. Bad feature of adaptive boosting is its sensitivity to noisy data and outliers. In real-world scenarios human faces might be occluded by other objects such as facial mask. This makes the face recognition process a very challenging task. Deep learning-based method and quantization-based technique achieves a high recognition performance.

MobileNetV2 is a very effective feature extractor for object detection and segmentation.

MobileNetV2 provides a very efficient mobile-oriented model that can be used as a base for many visual recognition tasks. For the best of our knowledge, this work addresses the problem of masked face recognition and different approaches during COVID–19 pandemic. It is worth stating that this study is not limited to this pandemic period since a lot of people are self-aware constantly, they take care of their health and wear masks to protect themselves against pollution and to reduce other pathogens transmission.

Future Enhancement

At Apple's September 2017 Apple Event, the maker of the iPhone and other ubiquitous technologies made a significant change to its flagship product: It introduced Face ID. This feature allowed users to forgo traditional fingerprint readers, instead using their faces to access their iPhones and other sensitive information, enhancing security and usability in the process.

Today, facial recognition technology is more expansive and integrated than ever before. Facial recognition has been implemented by big banks, credit card companies, technology platforms and even Major League Baseball.

It's showing up in our professional lives as well. During the pandemic, many businesses retrofitted their access control systems by replacing badge or fingerprint readers with systems harnessing facial recognition. This has become especially important in a decentralized environment where companies are responsible for enhancing worker safety and security in less populated workspaces.

Collectively, the facial recognition market is soaring. In 2020, the technology's market size approached $4 billion, a number expected to quadruple by 2030 as businesses and forward-thinking individuals look to upgrade their physical security and access control solutions in the years ahead.

While the facial recognition market is still in flux as companies, individuals and governments grapple with the implications of the technology's broad implementation, five trends will shape facial recognition in 2022 and beyond.

1. AI Enhances Capabilities :

AI-driven identity verification for access control will become more capable and accessible in the year ahead. No longer a theoretical technology, AI is more refined and actionable, ready to deliver new real-world experiences.

Therefore, access controls will be more frictionless, fast and multifaceted.

For instance, AI enables today's facial recognition systems to incorporate multifactor authentication, video authorization and other features to create a more capable access control solution.

2. Facial Recognition Heightens Convenience :

Many businesses and building owners are balancing safety and convenience, often compromising one to accommodate the other.

What's more, there is frequently a chasm between executives' intentions and actual process implementation. For example, a PwC survey found "90% of C-suite executives believe their company pays attention to people's needs when introducing new technology, but only about half (53%) of staff say the same."

When it comes to securing physical spaces, this means accounting for access control requirements. Physical authentication tools, like magnetic cards or badges, can be lost, stolen or manipulated while eroding the user experience.

In 2022, facial recognition technologies will alleviate these concerns, allowing people to access appropriate spaces with as little friction as possible.

3. Facial Recognition Protects The Home :

Doorbell cameras and home security systems are increasingly prevalent in residential dwellings, providing peace of mind and protection for people's most valuable asset.

Facial recognition will enhance these systems, allowing people to derive more functionality than ever before.

For instance, facial recognition technologies can be integrated with home-centered applications to announce front door arrivals, provide remote residential access and other access-related functionality.

4. New Information Makes More Intuitive Personal Assistants :

AI-powered personal assistants—including Siri, Alexa and Cortana—are becoming more competent at simple tasks like scheduling calendar meetings, dictating text messages or playing music.

However, when paired with facial recognition technologies, these assistants can be more personal and responsive, serving as a more realistic and responsive alternative to today's robotic iterations.

Specifically, these technologies can be trained to detect emotions and other intuitive social cues, making them more conversational and personally responsive.

5. Face As A Credential Protects People's Identities :

Facial recognition is often used to facilitate some of our most important interactions, including platform access, online payments and other secure spaces.

In a digital environment where personally identifiable information (PII) is both highly valuable and often vulnerable, facial recognition offers a solution, protecting people's identities when navigating digital or physical spaces. While passwords and other credentials are prone to theft or misuse, facial recognition remains with a person, enhancing security and privacy.

Of course, these developments will need to be paired with their own privacy standards, but the net gain to users' security is worth navigating and refining this complicated process.

REFERENCES

1. Wikipedia, Three dimensional face recognition
http://en.wikipedia.org/wiki/Threedimensional_face_recognition [2] Basu, S. 1997.

2. Wikipedia, Active appearance model,
http://en.wikipedia.org/wiki/Active_appearance_model4

3. Shervin Emami, Rotating or Resizing an Image in OpenCV,
http://shervinemami.info/imageTransfor ms.html

4. The Investment Performance of Common Stocks in Relation to their Price to Earnings.

5. Computer Vision Papers
Ratio: A Test of the Efficient Markets Hypothesis. Journal of Finance, 33(3): 663-682.

6. Wikipedia, Histogram equalization equalize+778=]]]= =]lization.

7. K. T. Talele, S. Kadam, A. Tikare, Efficient Face Detection using Adaboost, "IJCA Proc on International Conference in Computational Intelligence", 2012.