Should Face Recognition be used for Automating Attendance System?

Snigdha Morais Raj haramshi
Guide: Dr. Divya Premchandran
Keraleeya Samajam’s
Model College, Khambalpada Road
Thakurli, Dombivli (East), Kanchangaon, Maharashtra

Abstract
When managing attendance using conventional techniques, such as calling out roll calls and requiring a student’s signature, it can be a laborious task. Due to the lecture’s unusually high number of students, there will always be a possibility of proxy attendance. Conventional techniques of attendance marking have been difficult to implement. The issue of automatic attendance marking has recently received a lot of attention thanks to the widespread use of common biometrics like fingerprints and RFID tags, etc. However, the aspect of dependability is absent from these methods. In this proposed project, an automated attendance system is proposed by making use of face recognition. A rising problem in face recognition is the increasing demand for effective, automatic methods of recording attendance. Due to their distinctive facial traits, individuals can be identified only by their faces. Systems for face recognition come in handy for a variety of real-world uses. By keeping their facial photos along with a special ID, all pupils will initially be enrolled in the proposed system. Real-time images will be captured during the event, and the faces in those images will be compared to the faces in the pre-trained dataset.

Keywords—conventional techniques, face recognition, pre-trained dataset, real-time images.

1. Introduction
The field of facial recognition is now quite interesting and is yet in its infancy. Facial recognition technologies are quickly outpacing other biometrics because they use a set of characteristics unique to one person (such as fingerprints, RFID, etc.). This project can be used to create an attendance system that makes use of the traditional facial recognition method. Face recognition has a wide range of uses, and we decided that exploring this field for our project would be valuable and fascinating because it would help us hone our talents and better prepare for the challenges that lay ahead.

2. What is face recognition?
Facial recognition is a technique for identifying someone or confirming their identity by using their face. Facial recognition technology can identify people in real time as well as in still photos and movies. Face recognition is a subtype of biometric security. Additional biometric software kinds include those that recognises the voice, fingerprints, retina, or iris of the eye. Despite growing interest in using the technology in other industries, security and law enforcement remain account for the majority of its uses.

3. Advantages of Face Recognition
In addition to unlocking your smartphone, facial recognition offers the following advantages:

1. Increased Security
Facial recognition technology can be used by governments to track down terrorists and other criminals. On a personal level, facial recognition can be utilised as a security method for locking down mobile devices and home security cameras.

2. Reduced Crime
Face recognition makes it easier to locate trespassers, thieves, and robbers. Even just knowing that a facial recognition technology is in place can reduce crime, especially minor offences. Along with physical security, there are benefits to cybersecurity. Face recognition technology can be used by businesses to access computers without passwords. Theoretically, because there is nothing to steal or alter, as there is with a password, the technology cannot be hacked.

3. Removing bias from stop and search
Public complaints about illegal stops and searches have given rise to police issues; facial recognition technology could simplify the process. Face recognition technology could help reduce potential discrimination and reduce stops and searches on law-abiding people by automatically identifying suspects amid crowds rather than by employing a human approach.

4. Greater convenience
Customers won’t need to use their credit cards or cash to make purchases in stores as the technology becomes more widely used. This might shorten wait times at the register. Because facial recognition doesn’t require physical contact, like fingerprinting or other security measures, it offers a speedy, automatic, and seamless verification process—important in the post-COVID context.
5. Faster Processing

Facial recognition has advantages for the businesses that utilise it because it can identify faces in under a second. Businesses desire both secure and efficient solutions in an era of advanced hacking tools and cyberattacks. Quick and effective identity verification is made possible by facial recognition.

6. Integration with other technologies

Facial recognition systems are compatible with the vast majority of security software. Integration is actually rather straightforward. There are therefore few additional resources needed to put it into practise.

4. Disadvantages of Face Recognition

When facial recognition technology is used in situations where there is a clear advantage or justification, some people may not mind being videotaped in public and do not object to its use. However, the technology can elicit strong reactions from others. Several of the negatives or problems are:

1. Surveillance

Some people are concerned that the widespread use of facial recognition technologies, together with video cameras, artificial intelligence, and data analytics, raises the possibility of mass monitoring, which would limit personal freedom. Governments can hunt down criminals using facial recognition technology, but they could also track down regular people at any time.

2. Scope for error

Facial recognition data can contain errors, which may result in false accusations against innocent people. For instance, a minor adjustment to the camera position or a modification to one’s look, such as a new hairstyle, could result in inaccuracy. Newsweek reported in 2018 that 28 members of the US Congress were mistakenly flagged as suspects in criminal activity by Amazon’s facial recognition software.

3. Breach of privacy

The most contentious topic is one involving ethics and privacy. Several people’s photos have been stored by governments without their consent. A legal framework to prevent privacy and ethical breaches would need to be developed before facial recognition technology may be used in public places for up to five years, according to a 2020 statement from the European Commission.

4. Massive data storage

Facial recognition software is built on machine learning, which requires a vast quantity of data in order for it to "learn" and deliver accurate results. Such massive data sets demand strong data storage. It’s possible that small and medium-sized firms lack the equipment needed to keep the required data.

How does facial recognition works?

FaceID, which is used to unlock phones, has made face recognition technology widely known (however, this is only one application of face recognition). Facial recognition typically identifies and recognises one person as the single owner of the device, limiting access to others, rather than relying on a large database of images to determine an individual’s identification. Beyond just unlocking phones, facial recognition technology matches the faces of people passing by special cameras to images of people on a watch list. The images on the watch lists might come from everywhere, including our social media accounts. Facial recognition technology is also used to match faces at border security checkpoints and in places like schools, colleges, offices, and other public places to take attendance. Facial recognition technology is used in numerous other ways as well. Despite the fact that facial technology systems can vary, they generally work as follows:

Step 1: Face Detection

The camera can recognise and pinpoint a face whether it is present by itself or with other individuals. The subject may be portrayed either in profile or facing forward.

Step 2: Face Analysis

The following stage is to take and examine a face image. Most facial recognition technology use 2D rather than 3D photographs because it is simpler to compare a 2D image with previously taken photos or those in a database. The software is able to read the geometry of your face. Important features include the distance between your eyes, the depth of your eye sockets, the distance
between your forehead and chin, the contour of your cheekbones, and the appearance of your lips, ears, and chin. The objective is to identify the facial characteristics that set your face apart.

**Step 3: Converting the image to data**
The face capture process transforms analogue information (a face) into a collection of digital information based on the subject’s facial characteristics (data). Your face’s evaluation can essentially be expressed as a mathematical formula. The faceprint is a coded number. Each person has a unique faceprint, similar to how each thumbprint is unique.

**Step 4: Finding a match**
Then, your faceprint is compared to a database of other recognised faces. For instance, the FBI has access to up to 650 million photographs that are taken from different state databases. Facebook adds any image that has been given a name tag to their database, which also has facial recognition software. If your faceprint matches a photo in a facial recognition database, a decision is made. Facial recognition is thought to be the most natural biometric assessment of all. This makes intuitive sense given that we frequently identify ourselves and other people by looking at their faces rather than their thumbprints or iris. According to estimations, the majority of people in the globe regularly use facial recognition software.

6. **How Facial Recognition is used?**
A multitude of uses exist for the technology. These consist of:

1. Unlocking phones
   Many phones, including the most current iPhones, use face recognition as a feature to unlock the phone. The technology ensures that sensitive data remains inaccessible in the event that the phone is stolen and offers a robust solution to protect personal information. Apple estimates that one in a million times, a random face will unlock your phone.

2. Law Enforcement
   The use of facial recognition in law enforcement is common. According to a recent NBC article, police enforcement agencies in the US and other countries are using technology more and more. Following an arrest, police collect mug pictures from the suspects and compare them to facial recognition databases at the federal, state, and local levels. A photograph of an arrested person will be taken, stored in databases, and reviewed each time police undertake a new criminal investigation. Additionally, mobile face recognition enables law enforcement personnel to take a picture of a driver or a pedestrian on the street using smartphones, tablets, or other portable devices, and then instantaneously compare that picture to one or more face recognition databases to try to identify the person.
3. Airports and Border Control

Today, facial recognition technology is widely used in several airports all around the world. More travellers are using biometric passports, which allow them to skip the frequently long lines and head straight to the gate by going through an automated ePassport control. Using facial recognition technology at airports could improve security and reduce wait times. By 2023, 97% of travellers will be subject to face recognition, according to the US Department of Homeland Security. Airports, border crossings, and major events like the Olympics all use the technology to increase security.

4. Finding missing persons

Facial recognition technology can be used to find people who have gone missing and victims of human trafficking. Consider a database that has been enlarged to include absent individuals. In that case, law enforcement can be notified as soon as they are recognised by face recognition, whether they are in an airport, supermarket, or other public space.

5. Banking

Biometric online banking is another benefit of facial recognition technology. Customers can authorise transactions by looking at their smartphone or computer rather than requiring onetime passwords. There are no passwords to compromise with facial recognition technology. ‘Liveless’ detection, a method for determining if the source of a biometric sample is a living human being or a phoney representation, should, in theory, stop hackers from utilising your photo database for impersonation. Debit cards and signatures might become obsolete as a result of face recognition.

6. Marketing and advertising

Facial recognition has being utilised by marketers to improve customer experiences. For instance, in a 2017 marketing effort, the frozen pizza firm DiGiorno used facial recognition to scan partygoers’ facial expressions to gauge how they felt about the food. The media industry also employs facial recognition to determine the most effective times to air advertising and how consumers respond to TV pilot characters and movie trailers. Brands can trigger customised adverts on billboards that use face recognition technology, such as those at Piccadilly Circus in London.

7. Healthcare

In hospitals, facial recognition is utilised to help in patient care. Healthcare organisations are experimenting with the use of facial recognition to access patient records, speed up patient registration, identify specific genetic illnesses, and even assist patients express emotion and pain. AiCure has developed a facial recognition-based software to ensure that patients take their medication as prescribed. As costs decrease, more biometric technology usage in the healthcare sector is projected.

8. Monitoring gambling addictions

The level of client protection provided by gaming enterprises can be increased with facial recognition. In crowded, enormous facilities like casinos, it might be difficult for human staff to keep an eye on persons entering and departing gaming sections. Face recognition technology allows businesses to identify those who are classified as gambling addicts and records their gameplay so that employees can advise when it’s time to stop. If gamblers on voluntary exclusion lists are found gaming, casinos risk severe fines.

7. What Are the Risks of Face Recognition Technology?

Hackers reportedly compromised Apple’s iPhone FaceID user authentication in just 120 seconds in 2019. To keep your personal information secure, it is crucial to weigh the risks and drawbacks of facial recognition technology despite its many advantages.

1. It may be an invasion of personal and society privacy

One serious drawback of facial recognition technology is the potential threat to individual privacy. People dislike having their faces taken down and kept in a database for a hypothetical future use.

2. It leads to data security issues

There is a chance that facial recognition data stored in databases will be compromised. Hackers have gained access to databases that house facial scans that have been gathered and used by banks, police forces, and defense companies.

3. It offers opportunities for fraud and other illegal behaviour

Facial recognition technology can be used by criminals to commit crimes on defenceless people. To commit identity fraud, they can gather personal information about people, including images and videos taken from facial scans and stored in databases. With this knowledge, a thief could create a criminal record using the victim’s identity or open bank or credit card accounts in the victim’s name.

4. Technology has flaws

Inaccurate facial recognition exists. For instance, compared to white males, it is less good in identifying women and people of colour. Algorithms are used by the technology to match faces. Because the databases include more information on white men, the algorithms are more reliable for them than for women and people of colour. The algorithms get biased unintentionally as a result.

5. Technology is fallible

Other elements, such as camera angles, lighting conditions, and image or video quality, can influence the technology’s capacity to recognise faces. Using disguises or marginally altering one’s appearance can also fool facial recognition software.
The adoption of FRT has many advantages, but there are also a number of security issues that come with it, according to Ping Identity. Both users and developers should use prudence while thinking about the technology. From tracking individuals who have not provided consent and the breach of privacy to hackers finding ways to infiltrate the newly emerging software. Ping Identity claims that weak passwords, such as your date of birth, full name, or readily guessed phrases, make it simple for hackers to access systems and networks. The retrieval of unique genetic information is caused by the replication of this issue in biometrics. Businesses should think about using biometric technologies like FRT in conjunction with other security measures like passwords and MFA, the report recommends. As a result, systems will be able to validate several components rather than just one, enhancing security and lowering the risk of attacks. Although facial recognition technology (FRT) has shown to be more difficult to penetrate, hackers are already exploring for ways to reproduce people’s looks. Cybercriminals have found it easier to breach voice and fingerprint recognition security.

8. What can you do?
Be cautious about who you give access to your face at all times.

![Avoid Facial Identity Fraud](image)

9. Research Methodologies

Hybrid Model
Both descriptive and analytical elements may be present in a model. To reason about a system, logical relationships in a descriptive model can be investigated and inferences made. The results of logical analysis, however, are very different from those of a quantitative chemical examination of system attributes. We first conducted a poll of people utilising an online form creator and data collection service to acquire information regarding people’s awareness.

10. Public Survey
We deployed our data gathering utility, often known as a survey bot, to a variety of people and collected information on various facets of their understanding of face recognition.

10.1. Questionnaire
How likely do you think proxy attendance is marked?
Would it be wise to abandon the conventional approaches to attendance?
Which method of attendance do you prefer? Modern (Artificial Intelligence) or Traditional?
Do you believe that taking attendance should be done using face recognition?
Do you believe that face recognition technology is accurate and trustworthy?
Can the burden of taking attendance be lessened by utilizing a facial recognition system for the attendance system?
Do you believe the issue of proxy attendance can be solved by using contemporary attendance solutions (such as artificial intelligence)?
Should face recognition attendance systems be used in all settings, including businesses, schools, and colleges?

10.2. Results
We conducted some public research by asking people questions for our project. The observed response chart shows how respondents responded when asked how probable they thought proxy attendance was marked:
About 75% of respondents who were asked if it would be wise to stop using the traditional methods of attendance agreed that it would be, while 25% thought that the traditional methods should be kept up.

90% of respondents who were asked which way they would want for the attendance system answered they would like it to be modern (using artificial intelligence), while the remaining respondents chose the traditional technique.

94% of respondents agreed that facial recognition should be used to take attendance, while the other 23% disagreed.

The observed answer chart for the question of whether respondents believed face recognition is reliable and accurate is as follows:
When asked if using a facial recognition system for the attendance system could ease the strain of taking attendance, the observed response was as follows:

92% of respondents said they thought the problem of proxy attendance could be resolved with modern attendance technologies (such artificial intelligence), while the remaining respondents disagreed.

The observed response is as follows when asked if they thought face recognition attendance systems should be employed in all contexts, including businesses, schools, and colleges:

11. Hypothesis Testing
In order to draw conclusions about a population parameter or probability distribution, statistical reasoning known as hypothesis testing involves analysing data from a sample. A hypothesis is first formulated with relation to the parameter or distribution. The shorthand for this is the null hypothesis, or $H_0$. The null hypothesis is then contrasted with the alternative hypothesis (designated $H_a$), which is the complete opposite. The hypothesis-testing method decides if $H_0$ can be rejected based on sample data. The alternative hypothesis $H_a$ is valid if $H_0$ is disproved, according to the statistical result.

For this paper,

Null hypothesis ($H_0$): It is not advisable to take attendance using face recognition.

Alternative hypothesis ($H_a$): The best method for taking attendance is face recognition.

TEST STATISTICS
There are three tests that can be used to decide whether or not the null hypothesis should be rejected. They are:

1. Chi-squared test
2. T-student test (t-test)
3. Fisher’s Z test

A two-tailed T-student test will be used in this paper.

When comparing the means of two groups that are connected in some way, a t-test is an inferential statistic that assesses whether there is a significant difference.

Level of significance
The significance level is the likelihood that the null hypothesis will be rejected when it is confirmed (also known as alpha or $\alpha$). A significance level of 0.05, for instance, means that there is a 5% probability of discovering a difference where there is none. Lower significance levels indicate that to disprove the null hypothesis, there must be evidence.

Level of confidence
The confidence level shows the likelihood that a statistical parameter’s position is correct (such as the arithmetic mean) measured in a sample survey is also true for the entire population.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>74.8</td>
</tr>
<tr>
<td>2</td>
<td>89.6</td>
</tr>
<tr>
<td>3</td>
<td>93.9</td>
</tr>
<tr>
<td>4</td>
<td>95.7</td>
</tr>
<tr>
<td>5</td>
<td>91.3</td>
</tr>
<tr>
<td>6</td>
<td>90.5</td>
</tr>
</tbody>
</table>

Mean (x) 89.3

Standard Deviation (s) 7.455199528

Level of significance = 0.05 i.e. 5%
Level of confidence = 95%

The number of standard deviations that separate a t-score (or t-value) from the t-mean distribution. The formula to find t-score is:

\[ t = \frac{(x - \mu)}{(s/\sqrt{n})} \]

where \( x \) is the sample mean, \( \mu \) is the hypothesized mean, \( s \) is the sample standard deviation, and \( n \) is the sample size.

The p-value, also referred to as the probability value, expresses how likely it is that your data occurred under the null hypothesis. Finding the equivalent p-value is possible once we are aware of the value of t. The null hypothesis can be rejected and facial recognition software should be employed for attendance if the p-value is less than a certain alpha level (popular choices are .01, .05, and .10).

Calculating t-value:

Step 1: Identify the alternative and null hypotheses.
Null hypothesis (H0): The best method for taking attendance is face recognition.
Alternative hypothesis (Ha): It is not advisable to take attendance using face recognition.

Step 2: Find the test statistic.
The postulated mean value in this situation is taken to be 0.

\[ t = \frac{(x - \mu)}{(s/\sqrt{n})} = \frac{(89.3 - 0)}{(7.4552/\sqrt{6})} = 29.3412 \]

Step 3: Calculate the test statistic’s p-value.
The p-value is computed using the t-Distribution table with n-1 degrees of freedom. The sample size for this study is \( n = 6 \), hence n-1 = 5.
It provides a p-value when the observed value is entered into the calculator. In this case, the p-value returned is less than 0.00001. We can rule out the null hypothesis because this p-value is smaller than our selected alpha threshold of 0.05. Therefore, we have enough information to conclude that using face recognition to take attendance is the best option.

12. Conclusion
With the use of this technology, a robust facial recognition-based attendance system might be created. The suggested system will be able to track attendance by employing facial ID. It will identify them after detecting faces using a webcam. This is accomplished by utilising dlib for facial recognition and OpenCV for frame extraction. This technique will require less time to recognise several faces from a single frame and will be more accurate. After acknowledgment, the attendance record will be updated to reflect the acknowledged student’s attendance.

References
1. Journal of Cognitive Neuroscience Volume 3, Number 1, 1991 - Massachusetts Institute of Technology
7. Face recognition-based Attendance System using Machine Learning Algorithms, Radhika C. Damale, Department of Electronics and Telecommunications, Cummins College of engineering for Women, Pune, Maharashtra, India.