Face Recognition Based Attendance System Using Deep Learning

Yalagaboyna Mamatha[1], Kamari Pavani[2] ,Ramadi Revathi[3], Dr.T.S.Mastan Rao[4]

[1,2,3]B.Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

[1]Yalagaboynamamatha@gmail.com, [2]197r1a05e5@cmrtc.ac.in, [3]197r1a05g0@cmrtc.ac.in

[4]Associate Professor, Department of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad Telangana, India,

[4]mastan1061@gmail.com

Abstract- working on a biometric attendance management project. Using a Deep Learning-based Convolutional Neural Network algorithm for face recognition is a powerful tool to accurately identify individuals, and using Flask for building a user interface is an excellent choice to make your project more user-friendly. However, when working with biometric data, it is essential to consider the ethical implications of using such data. It is important to ensure user privacy and obtain informed consent before collecting and using biometric data. You should follow all necessary legal and regulatory requirements to protect the privacy of the individuals whose data you are collecting and storing. Here are some tips to consider when working with biometric data: Make sure that the user is aware that their biometric data is being collected and stored. Provide clear information on how the data is being used and stored. Store the data securely, and make sure that only authorized personnel have access to it.

1.INTRODUCTION

Proper biometric use is very application dependent.. Different biometric technologies have different strengths and weaknesses in terms of convenience and security, and the choice of biometric technology depends on the specific use case and the level of security and convenience required. For example, fingerprint recognition is a widely used biometric technology that offers a good balance of convenience and security. It is easy to use and widely available, but it also provides a relatively high level of security as fingerprints are unique to each individual and difficult to fake. However, some applications may require even higher levels of security, such as facial recognition or iris recognition. These biometric technologies offer a higher degree of security but may be less convenient to use, requiring specialized hardware or software.

On the other hand, some biometric technologies may prioritize convenience over security, such as voice recognition or gesture recognition. While these technologies may be easier to use, they may not provide a high level of security and are more susceptible to spoofing or false positives. Ultimately, the choice of biometric technology depends on the specific use case and the balance between convenience and security that is required No single biometric will meet

all the requirements of every possible application. Biometrics are physical or behavioral characteristics that can be used to verify the identity of an individual. There are many different types of biometrics, including fingerprints, facial recognition, iris recognition, voice which uses the unique features of a person's face to identify them. It has the advantage of being non-invasive and can be used at a distance, but it can also be affected by changes in lighting conditions or facial hair. The recognition of iris is a biometric technology that relies on the distinctive characteristics of the iris, which is the colored region of the eye.. It is very accurate and difficult to fake, but it requires specialized equipment and may not be suitable for all applications. Voice recognition is also a biometric technology that is based on the unique characteristics of a person's voice, such as their pitch and tone. It can be used for remote identification, but it can be affected by factors such as background noise and changes in a person's voice due to illness or aging. Gait recognition is a relatively new biometric technology that identifies people based on their unique walking patterns. It has the advantage of being non-invasive and can be used at a a distance, but it may not be as accurate as other biometric technologies and can be affected by changes in a person's gait due to injury or other factors. In summary, each biometric technology has its own strengths and weaknesses, and the choice of which biometric to use depends on the specific requirements of the application. It may also be necessary to use multiple biometric technologies in combination to achieve the desired level of accuracy and security.

Fingerprint recognition is widely used and can be relatively inexpensive. It is also highly accurate and can be used in a variety of settings. However, it may not be suitable for individuals with certain types of skin conditions or injuries that affect their fingerprints.
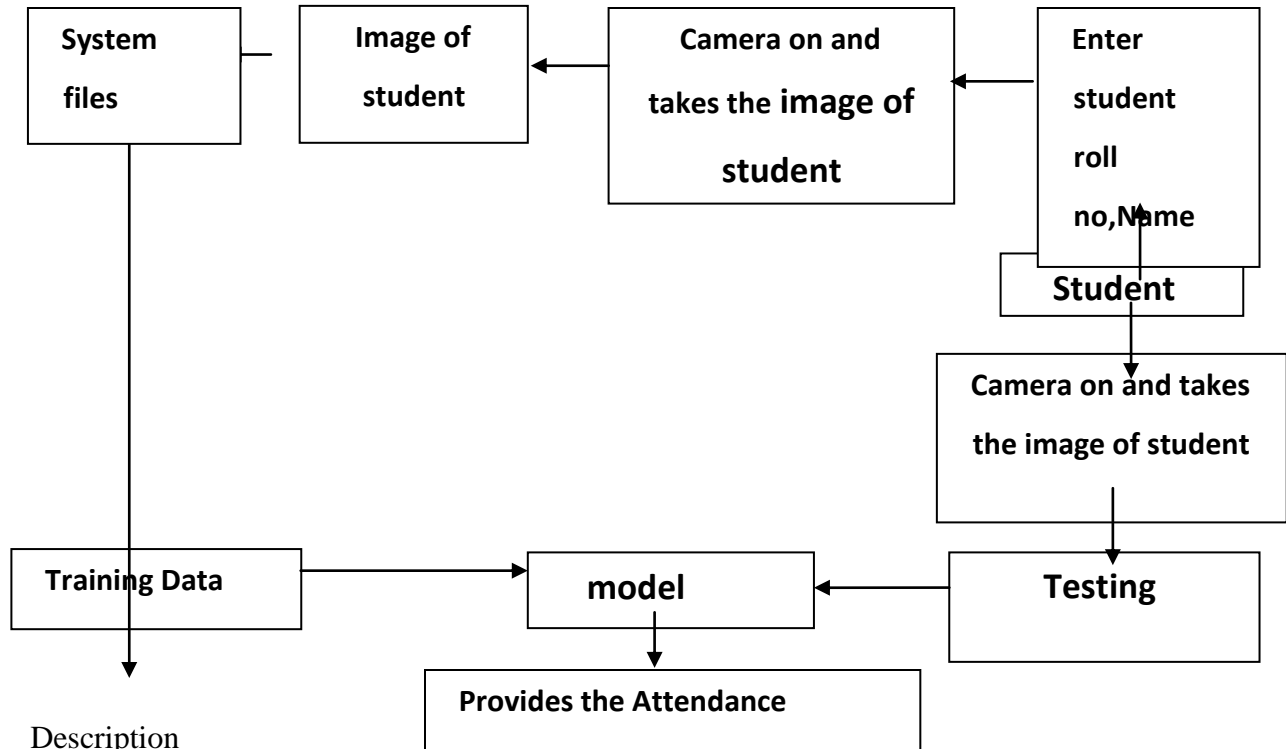
Vein recognition is a relatively new technology that is highly accurate and difficult to spoof. It can be used for both identity verification and access control. However, it can be more expensive and may require more specialized hardware than other biometric technologies. environmental noise and changes in voice due to illness or other factors. Overall, it is important to consider the specific requirements of each application when selecting a biometric in verification (or authentication) mode the system performs a one-to-one comparison of a describing a process of biometric authentication, where a person's biometric data (such as their fingerprint, face, or iris) is captured and then compared against a stored template in a biometric database to verify their identity. The process typically works like this: first, the person's biometric data is captured using a biometric sensor, such as a fingerprint scanner or facial recognition camera. The sensor then converts the biometric data into a digital template, which is a mathematical representation of the unique features of the person's biometric. This digital template is then stored in a biometric database along with other information about the person, such as their name or identification number. When the person wants to authenticate themselves, they submit their biometric data again, and it is compared against the stored template in the database. If the biometric data matches the stored template within a certain threshold of accuracy, the person is granted access or authentication. If there is not a match,

the person may be denied access or asked to provide additional forms of identification. Biometric authentication can be a useful tool for security and access control, as it provides a highly accurate and difficult-to-forge means of verifying a person's identity. However, it's important to ensure that the biometric data is collected and stored securely, and that the system is designed to protect against potential attacks or vulnerabilities.the second step, the person's biometric information, such as fingerprint, facial features, or iris patterns, is collected and compared to the stored reference model. This is done to ensure that the person is who they claim to be. In the final step, the system evaluates the degree of similarity between the collected biometric information and the stored reference model. If the degree of similarity is high enough, the system will verify the individual's identity. It's important to note that the verification process may vary depending on the specific application and the level of security required. For example, a high-security facility may require multiple forms of biometric authentication, while a simple mobile app may only require a fingerprint scan. Overall, biometric verification is becoming increasingly popular as a secure and convenient way to authenticate a person's identity. However, it's also important to consider privacy concerns and ensure that biometric data is stored securely and used responsibly.

2.PROPOSED SYSTEM

In this project, we have created a model that which can take the attendance of student in the allotted times by the face recognition if student not recognized I the allotted attendance taken time they will be given attendance as late coming. The manual method of attendance management, which is time-consuming and challenging to maintain, is expected to be replaced by automatic attendance management. Among the various biometric processes available, face recognition is considered the most effective. The proposed solution employs computer vision, a branch of deep learning that facilitates camera reading and writing, and utilizes Flask to develop a user-friendly graphical interface.

```
┌──────────┐   ┌──────────┐      ┌──────────────┐      ┌──────────┐
│ System   │───│ Image of │ ←──  │ Camera on and│ ←──  │ Enter    │
│ files    │   │ student  │      │ takes the    │      │ student  │
│          │   │          │      │ image of     │      │ roll     │
└──────────┘   └──────────┘      │ student      │      │ no,Name  │
                                 └──────────────┘      └──────────┘
                                                          Student
```

Camera on and takes the image of student

Training Data → model ← Testing

Provides the Attendance

Description

Face recognition based attendance using deep learning is an easy way to mark attendance, first the we need to train the model with the student face and their details ,when the web cam capture the image of the students then captured face test with the trained model and register the attendance in the database. If we want to check the attendance of the student we need to login through webpage .where we have to login and enter into that we need to check the attendance.

CNN training process is configured in 7 layers consisting of input, convolution, pooling, and activation functions. In the first layer, input is provided consisting of feature vector size in the second layer for the convolution purposes dimensions are decided for the matrix convolution, 3rd layer pooling is performed and max pooling is done, 4th layer stack to line conversion is done after that in remaining layers activation function are used like sigmoid function. The

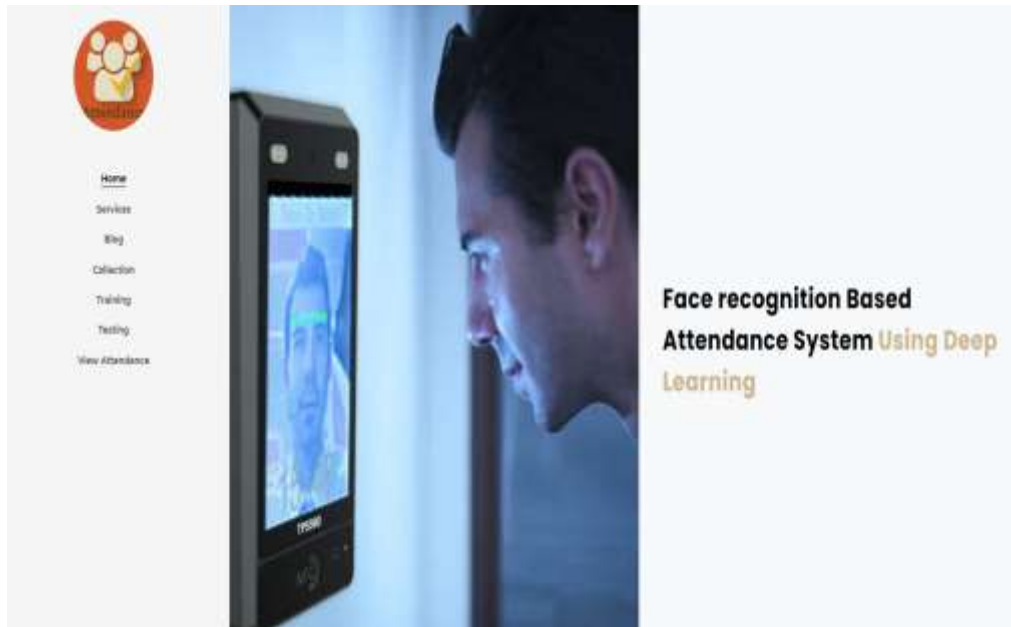activation function is used for minimizing the error at the output. The weight and
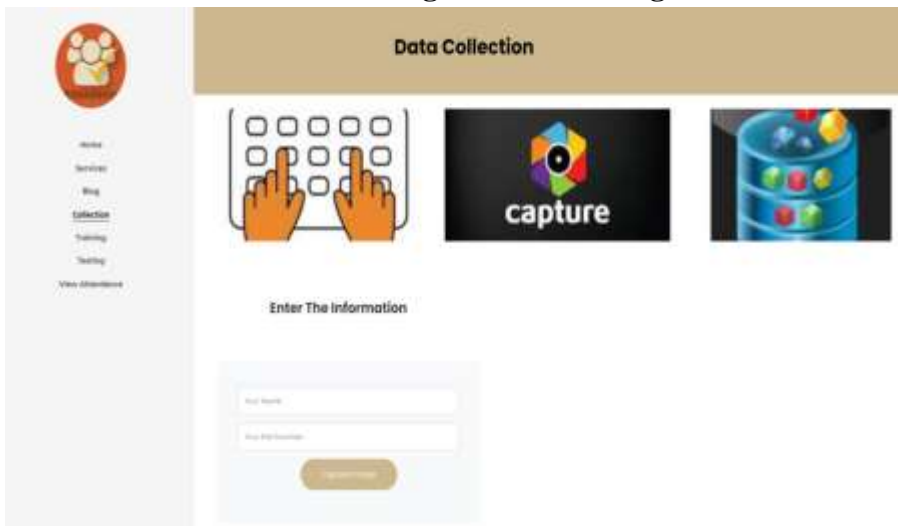

Figure 1. Home Page
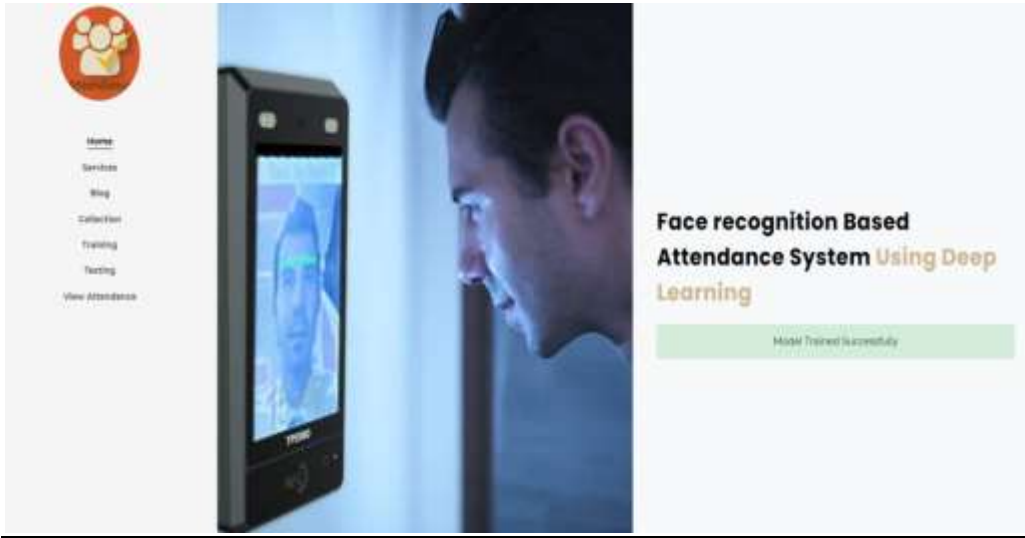

Figure 2 Data Collection

Figure 3. Model Trained Sucessfully

Figure 4 Final result

3.Data Base

providing multi-user access to a number of databases. The SQL phrase server for a Structured Query Language. Free-software-open source projects that require. Full-featured database management system often use MySQL. For commercial use, several paid editions are available, and offer additional functionality.To Applications which use MySQL database include: TYPO3,Joomla, Word Press, phpBB, Drupal .

MySQL is utilized by numerous prominent and rapidly expanding enterprises, including Wikipedia, to power their high-profile and large-scale World Wide Web offerings. The creation and development of MySQL originated in Sweden through the collaboration of two Swedish individuals and one Finnish individual.
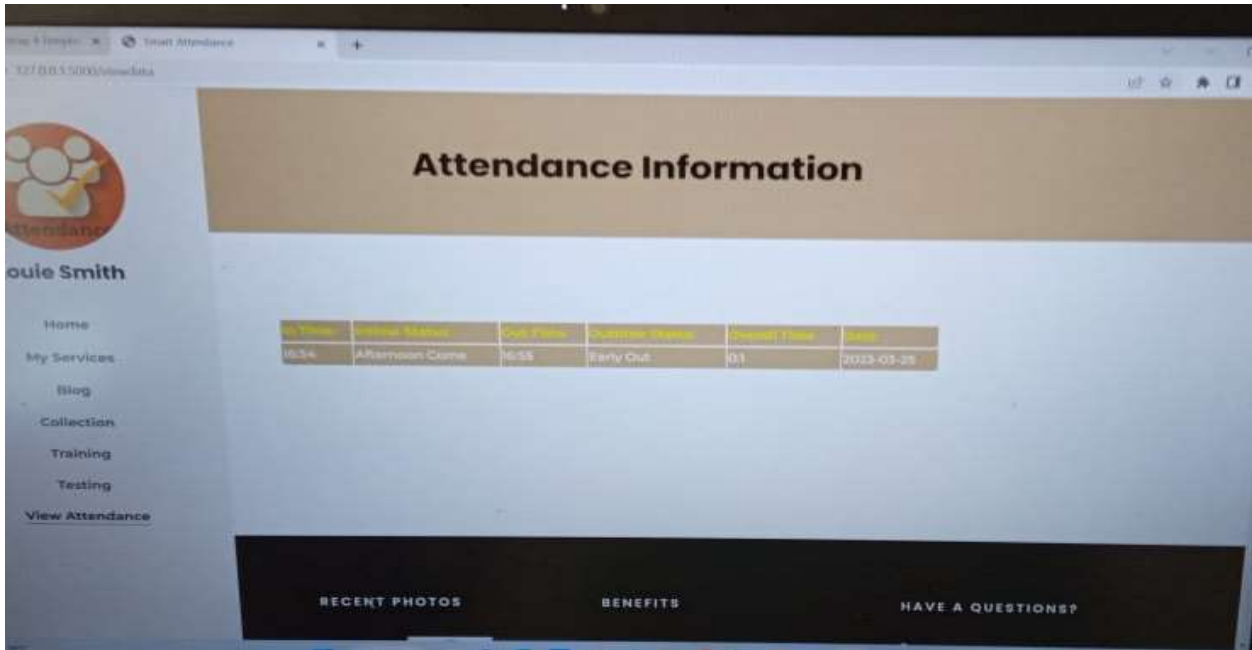

Figure 5. Attendance Information

4.TESTING

S.NO	Test cases	I/O	Expected O/T	Actual O/T	P/F
1	Login	Enter User name, password	Login successfully	Login successfully completed	P
2	Login	Enter User name, password	Login failed	Incorrect User name	F
3	Login	Enter User name, password	Login failed	Incorrect User password	F
4	Data Adding	Enter name,roll number, mobile number	Data added successfully	Data added successfully	P
5	Face	Input face image	Face recognized	Face	P

	recognition			recognized successfully	
	Face recognition	Input face image	Face recognized	Unknown person identified	F

5.CONCLUSION

In our proposed work, we have created a model that which can take the attendance of student in the allotted times by the face recognition if student not recognized I the allotted attendance taken time they will be given attendance as late coming. We have used Flask Framework, where the information about the student are stored and a model is trained and then the student picture is captured which is tested and attendance is taken to the student by the captured face image.

6.ACKNOWLEDEMENTS

7.REFERENCES

[1] Naveed Khan Balcoh, M.HaroonYousaf, Waqar Ahma and M.IramBaig, Algorithm for efficient Attendance Management: FaceRecognition Based approach, International Journal of Computer Science Issue, Vol.9, Issue 4, No 1, July 2012.

[2] NirmalayaKar, MrinalKantiDebbarma, AshimSaha, and DwijenRudraPal, Study of implementing Automated Attendance System using Implementing Automated Attendance System Using face recognition Technique, International Journal of Computer and Communication Engineering, Vol 1, No 2,July 2012.

[3] O. Shoewn, Development of Attendance Management System using Biometrics. The Pacific Journal of Science and Technology Volume 13, No 1, May 2012

[4] M. Turk and A. Pentland (1991) "Face recognition using Eigen faces". Proc.IEEE conference on computer vision and Pattern Recognition

[5] W.Zhao, R. Chellapa, P.J.Phillips and A.Rosenfld,"Face Recognition: A Literature Survey, vol. 35, No 4, Dec 2003, pp.399-458

[6] R.L. Hsu, Mottalec M.A and A.K.Jain,"Face Detection in colour images",International Conference on Image Processing, Oct 2001, pp. 1046-1049.

[7] ToufiqP. Ahmed Egammal and Anurag mittal (2006),"A Framework for featureselection for Background Subtraction", in Proceedings of IEEE computer SocietyConference on Computer Vision and Pattern Recognition.

[8] M.H.Yang, N.Ahuja and D.Kriegmao, "Face recognition using kernel Eigen faces", IEEE International Conference on Image Processing, vol.1, pp. 10-13, Sept. 2000

[9] Rekha A. L, Chethan H. K, "Automated Attendance System Management System Using Face Recognition through Video Surveillance", Volume 1, Issue 11, July-2014

[10] Anil K. Jain, Arun Ross and Salil Prabhakar, "An introduction to biometric recognition", Circuits and Systems for Video Technology, IEEE Transcations on Volume 14, Issu 1, Jan 2004 Page(s):4-20.

[11] H. M. El Barkey, "Face detection using fast neural networks and image decomposition", Neurocomputing, Vol.11, no 3, pp 1039- 1046, 2002.

[12] R. L. Hsu, Mottale M.A and A.K. Jain, "Face detection in colourimages", Proceedings International Conference on Image Processing (ICIP), Oct 2001, pp.1046-1049.

[13] Prabhjot Singh and Anjana Sharma, "Face Recognition using Principal Component Analysis in MATLAB", International Journal of Scientific Research in Computer Science and Engineering, vol.3,Issue 1, ISSN 2320-7639.