Sigma J Eng Nat Sci, Vol. 43, No. 1, pp. 168−188, February, 2025

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2024.00030

Research Article

Smart attendance monitoring system using multimodal biometrics

Samatha J[1,*], Madhavi GUDAVALLI[2]

[1]*Department of Computer Science & Engineering, Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, 533003 India*
[2]*Department of Computer Science & Engineering, University College of Engineering Narasaraopet, JNTUK Kakinada, Andhra Pradesh,522601, India*

ARTICLE INFO

Article history
Received: 30 October 2023
Revised: 16 December 2023
Accepted: 15 January 2024

Keywords:
Binarization; Face Recognition; Local Extreme; Minutiae; Multimodal Biometrics

ABSTRACT

The trajectory of a person's career is significantly influenced by attendance. The conventional register-based attendance system is tedious, time-consuming, and generally uninteresting. These age-old methods, being laborious and time-intensive, warrant a more efficient alternative. In this paper, we introduce a Bimodal Attendance system implemented through biometrics. We delve into the examination of key physical characteristics of a human being, such as the face and fingerprints. User enrollment involves collecting essential user information, including facial and fingerprint data. A web camera is employed to capture live facial biometrics, while the Mantra Fingerprint sensor (MFS100) is utilized for the acquisition of the user's fingerprint image. The collected facial images undergo preprocessing to reduce noise, and facial recognition is accomplished by detecting facial landmarks. Implementation of Convolutional Neural Network-based facial recognition is executed using the Dlib package. Additionally, we propose a methodology for fingerprint verification utilizing Scale Invariant Feature Transformation (SIFT). Distinctive SIFT feature points are extracted in scale space based on texture information around the feature points, facilitating effective matching. In this multimodal attendance system, real-time attendance marking is achieved by capturing facial images. The fingerprint image is subsequently captured and verified if the recognized face corresponds to a registered user. Attendance records are updated in the database, ensuring accuracy surpassing 70% identification.

Cite this article as: Juluri S, Gudavalli M. Smart attendance monitoring system using multimodal biometrics. Sigma J Eng Nat Sci 2025;43(1):168−188.

INTRODUCTION

Today, institutions place a high value on student attendance and are concerned about it.Attendance is an important aspect of a student's academic life. Importance of attendance as follows:

- Academic Success: Attendance is a key factor in academic success. Students attending classes regularly are likelier to perform well in exams and assignments. Regular attendance also ensures that students do not miss important lectures, discussions, and presentations.
- Accountability: Attendance helps build accountability among students. Regular attendance instills discipline, responsibility, and a sense of commitment to their studies.

***Corresponding author.**
*E-mail address: samathajuluri@gmail.com

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey

- Participation: Attendance is important for student participation in class activities. Students who attend classes regularly are more likely to participate in discussions, ask questions, and engage in group activities.
- Time Management: Regular attendance helps students manage their time effectively. It helps them plan their schedules, prioritise their tasks, and ensure they have enough time to complete their assignments.
- Preparation: Attendance helps students prepare for exams and assignments. Students who attend classes regularly have access to important course material, notes, and presentations that help them prepare effectively.
- Attendance Policies: Many educational institutions have attendance policies that require students to attend a certain number of classes to pass the course. Regular attendance is, therefore, necessary to meet these requirements.

Due to the fact that student attendance in general affects their academic success[1]. Manually taking attendance in a classroom is a tedious process.Faculty must keep accurate attendance records. The manual system of maintaining attendance records is inadequate and takes longer to collect information and determine each student's average attendance [2]. As a result, a system to tackle the problems of student attendance record and student average attendance computation is required [3].

The other solution for monitoring attendance is using RFID cards. This system is fully automated no human is involved in collecting data, but if the student forgets the card, then attendance should be taken manually. And also, there is a chance for proxy attendance using another person's card [4,5].

Here are some key reasons why an attendance monitoring system is important:

- Accuracy: An attendance monitoring system provides accurate and reliable attendance data. The system automatically records attendance data, eliminating the need for manual data entry and reducing the risk of errors.
- Efficiency: An attendance monitoring system is efficient and saves time. It eliminates the need for teachers or staff to take attendance manually, allowing them to focus on other tasks and responsibilities.
- Real-Time Data: An attendance monitoring system provides real-time attendance data. This allows teachers and administrators to monitor attendance data in real time and take action if necessary.
- Automated Notifications: An attendance monitoring system can send automated notifications to parents or guardians if their child is absent or late to class. This improves communication between educators, students, and parents and helps to ensure that students are attending classes regularly.
- Analysis and Reporting: An attendance monitoring system can analyze attendance data and generate reports. This allows educators and administrators to identify patterns and trends in attendance, monitor student progress, and make informed decisions to improve student outcomes.
- Compliance: An attendance monitoring system can help educational institutions comply with attendance policies and regulations. It ensures that attendance data is accurate and up-to-date, reducing the risk of non-compliance and penalties [6].

This paper is motivated by a commitment to enhance security, accuracy, and efficiency in attendance tracking. Through the integration of facial recognition and fingerprint verification, the system aims to provide an elevated level of security, mitigating risks associated with identity fraud and unauthorized access. The study is driven by a desire to overcome the inherent inaccuracies in manual or card-based attendance methods, thereby offering a more reliable and automated solution. The focus on a user-friendly experience aims to streamline processes, saving time for both administrators and attendees. Real-time monitoring capabilities facilitate prompt interventions, contributing to improved attendance management. The adaptability of the system to diverse environments and its potential to maintain data integrity and organized record-keeping further underscore the comprehensive motivation behind this paper [7,8].

Biometrics has become increasingly vital in today's digital age due to the following reasons:

- Enhanced Security: Biometric authentication provides a high level of security as it is based on the unique physiological or behavioural characteristics of an individual that cannot be easily replicated or shared. This helps prevent identity theft, fraud, and unauthorised access to sensitive information and resources.
- Improved Convenience: Biometric authentication is convenient as it eliminates the need for passwords, PINs, or other authentication methods that are easily forgotten, lost, or stolen. Biometric authentication is also faster and more efficient than traditional authentication methods.
- Reliable Identification: Biometric identification is highly accurate and reliable as it is based on the unique physical or behavioural characteristics of an individual. This ensures that the identification process is less prone to errors or falsification.
- Customizable Security: Biometric authentication can be customized to meet specific security needs by using multiple biometric traits for identification. This makes it difficult for unauthorized individuals to gain access to sensitive information or resources.
- Versatile Applications: Biometrics has versatile applications in various fields such as law enforcement, healthcare, banking, education, and transportation. It can be used for identification, verification, access control, and attendance tracking, among other things.

Figure 1 highlights a few additional benefits of biometrics.

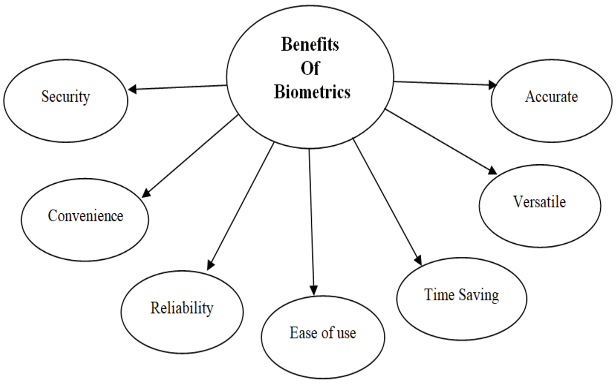


Figure 1. Benefits of biometrics.

Biometric traits can be broadly classified into two categories [9,10] as shown in Figure 2:

- Physiological Biometrics: These biometric traits are based on physiological characteristics of a person's body, such as their fingerprints, face, iris, retina, hand geometry, DNA, and voice.
- Behavioral Biometrics: These biometric traits are based on behavioral characteristics of a person, such as their typing rhythm, signature, gait, and even their behavior patterns like mouse movement or keystrokes.

Types of Biometric Traits

Below are several prevalent categories of biometric characteristics [11,12]:

- Fingerprint: Fingerprint biometrics is one of the most commonly used and recognized types of biometric technology. It analyzes the unique patterns and ridges on the surface of the fingertip.
- Face: Face biometrics uses facial recognition software to identify unique features on a person's face, such as the distance between the eyes, the shape of the jawline, or the curve of the lips.
- Iris: Iris biometrics uses the patterns in the colored part of the eye to identify a person. It is highly accurate and secure, but also requires a special camera to capture the iris image.
- Retina: Retina biometrics uses the unique patterns of blood vessels in the back of the eye to identify a person. This technology is highly accurate but requires a more invasive scanning process.
- Voice: Voice biometrics uses a person's unique voiceprint to identify them. It analyzes characteristics like pitch, tone, and pronunciation.
- Hand Geometry: Hand geometry biometrics uses the unique shape and size of a person's hand to identify them. It analyzes factors like the length of the fingers, the width of the palm, and the thickness of the hand.
- DNA: DNA biometrics uses a person's genetic code to identify them. This technology is still in the experimental stages and is not widely used.
- Signature: Signature biometrics uses the unique way a person signs their name to identify them. It analyzes factors like the speed, pressure, and angle of the signature.
- Keystroke Dynamics: Keystroke dynamics biometrics uses a person's typing rhythm and style to identify them. It analyzes factors like the speed, rhythm, and pressure of the keystrokes.
- Gait: Gait biometrics uses the unique way a person walks to identify them. It analyzes factors like the length of the stride, the angle of the foot, and the motion of the arms.
- Finger-Vein: Finger vein biometrics is a biometric recognition method that inspects the blood vessel patterns that are visible from the skin's surface of the fingers. This technique depends on shining a near-infrared light on a person's fingers to take pictures of the veins inside their hand. The presence of blood in the veins during recognition verifies the person is real and alive rather than an impostor.
- Review of various biometrics is as given below Table1

Table 1. Review of various biometrics

Biometric	Review
Face	Easy to use, but facial recognition accuracy decreases with age.
Fingerprints	Fingerprints are constant throughout life and do not change with time or age.
Iris	According to performance analysis, Iris offers high performance
Ear	Ear is recognized for its outlook. Easy to use but can't achieve the best. It leads to safety and personal identity.
Palm	Palm can be used to achieve higher security, performance, privacy, and accuracy.Because fingerprints can be collected without a person's knowledge.
Voice	It is easier to use and more versatile. Disadvantages include privacy issues and poor accuracy.
Gait	The accuracy of gait recognition can be affected by factors such as physical condition, clothing, carrying objects, and changes in walking style due to injury or fatigue.
Finger Vein	Provides high accuracy and pattern does not change for life.
Signature	Signatures can change over time due to factors such as age, injury, or illness, which may affect the accuracy and reliability of the system.
Keystroke Dynamics	Susceptible to spoofing attacks, such as using a device to simulate the typing patterns of an authorized user.

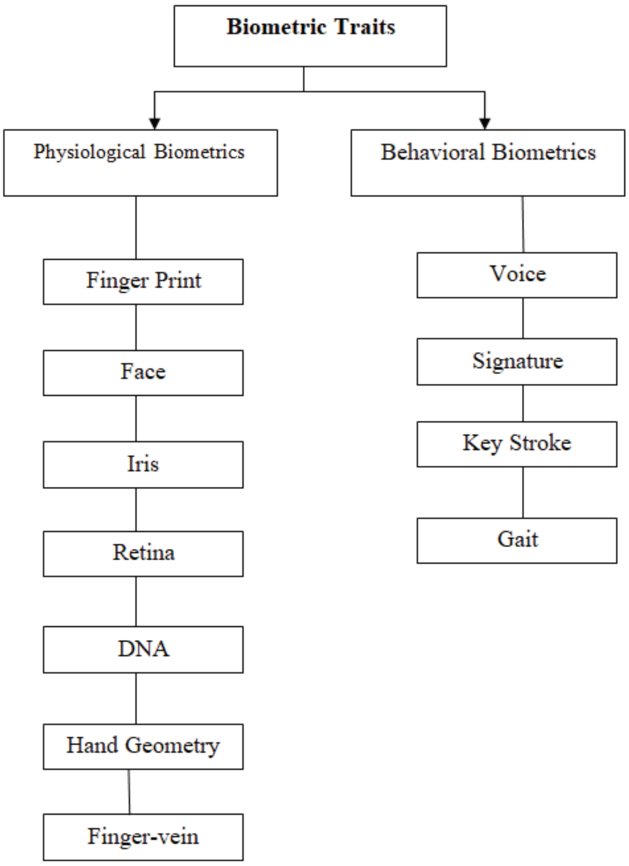


Figure 2. Classification of Biometric Traits.

Most of the current biometric attendance solutions are unimodal. Issues with unimodal systems are noise, intra class variation, interclass similarities, non-universality and spoof attacks [13]. These limitations can be overcome by using multi modal biometrics system which incorporates many biometric traits [14,15,16,17]. This paper proposes a paradigm for the student attendance system that considers fingerprint and facial biometric characteristics.

When a student enters a classroom, the system captures an image of their face, which is then compared to a database of pre-registered images to verify their identity. Face detection involves two steps: the first is the detection of faces, and the second is the recognition of those identified face images with the current database of images [18]. The face detection process involves several steps, including face localization, alignment, normalization, and feature extraction. Face localization involves identifying the face region in the image or video stream, while alignment ensures that the face is in a consistent position for comparison [19-21]. Normalization involves adjusting the image to account for variations in lighting and other factors, and feature extraction involves extracting key features of the face, such as the distance between the eyes and the shape of the jawline [22].

Once the system has detected and recognized a student's face, it can record their attendance and store it in a database for later retrieval and analysis. This process is typically faster and more accurate than traditional methods of attendance tracking, such as manual roll call. Additionally, it provides an additional layer of security by ensuring that only registered students are allowed access to the designated location.

Fingerprint detection is another component of attendance systems that use biometric technology. The system uses algorithms to capture and recognize the unique patterns and ridges of a student's fingerprint to verify their identity.The fingerprint detection process begins by capturing an image of a student's fingerprint using a fingerprint scanner. The scanner then analyzes the fingerprint to identify the unique pattern of ridges and furrows that are specific to each individual. This pattern is then compared to a pre-registered database of fingerprints to verify the student's identity.

The fingerprint detection process involves several steps, including image acquisition, pre-processing, feature extraction, and matching [23]. Image acquisition involves capturing a clear and accurate image of the student's fingerprint, while pre-processing involves enhancing the image to improve the quality of the fingerprint image. Feature extraction involves identifying unique features of the fingerprint, such as the number of ridges or the distance between them, and matching involves comparing the features of the student's fingerprint with those in the pre-registered database. The extraction of these unique characteristics produces great identification accuracy for fingerprints [24]. Once the system has successfully detected and recognized a student's fingerprint, it can record their attendance and store it in a database for later retrieval and analysis.

Limitations of Multimodal Biometric Systems [25]

1 They are more expensive and require more resources to compute and store compared with unimodal biometric systems.
2 Multimodal systems often take longer to register and verify, causing some inconvenience to users.
3 Combining evidence from different modalities is pending increasing accuracy. But if proper technique is not followed to combine the evidence provided by different methods, the accuracy of the system decreases as compared to the monomial system.

The following sections of this paper are arranged in the following manner. Section II reviews various proposals and methodologies of previous papers. Followed by Scale Invariant Feature Transform Algorithm. Section III describes facial recognition using various features and structures of fingerprints and the implementation of SIFT on fingerprints. Then the methodology of the proposed system is described in section IV. The results are reported to evaluate the performance of our proposed approach in Section V. At last, conclusions are given.

LITERATURE SURVEY

Albert Mayan J. et al. [26] proposes a mobile phone application to manage employee registration and attendance. Staff need not enter login register or biometric they just need to login to the application management can track staff members using GPS latitude, longitude, and IMSI numbers and attendance will be updated.

A. Charity et al. [27] propose a bimodal biometrics student attendance system to improve accuracy over a unimodal biometric system. For student attendance, the authors used face and fingerprint biometrics. Faces were captured using a webcam, and the PCA algorithm was used to extract features from the processed images, while SVM was used for classification. A scanner is used to capture fingerprints, and minutiae are extracted from the scanned prints. The MATLAB GUI was used as an interface between the database and the bimodal biometric system, and it achieved 87.3% accuracy.

A. Yadav et al. [28] used Haar cascade algorithm to build a class attendance system using face recognition. Face ID was used in the system to track attendance. The images for detection were captured using a webcam.

P. Wagh et al. [29] proposes a method that effectively addresses the issue of fraudulent attendance in class using facial recognition. Used principle component analysis, viola and Jones algorithm to overcome light intensity problems. Face images are detected and compared to student faces in a database.

A. Bhat et al. [30] suggests a system that uses facial biometric traits for marking student attendance. System uses class group photo to get the list of presentee. The proposed model used a one shot algorithm for facial recognition on the LFW dataset and obtained an accuracy of 97%.

L. Agarwal et al. [31] proposed a face identification system using HOG and SVM classifiers for marking attendance. The system has identified the faces accurately.

A. F. S. Moura et al. [32] proposed a facial recognition technology for the video monitoring system. The system used the FaceNet approach with labelled faces and used an SVM classifier from machine learning to classify the images to achieve an accuracy of 90%.

Kacker et al. [33] proposes an effective system for attendance monitoring by using facial biometrics.Covnets and dimensionality reduction techniques are used to identify faces, possibly by comparing them to a database.

Some authentication systems use fingerprints for identification. But the image produced by the scanner may produce different results for each scan, which is the major drawback of the existing biometric identification systems. S.Singh et al. [34] proposed a neural network based attendance monitoring system using fingerprints. The proposed system is implemented on the Raspberry Pi with suitable interfacing modules. The backend system includes image acquisition and processing to create a suitable database. The hardware model is created in MATLAB and then deployed in the Raspberry Pi-3 module to create a standalone system.

According toP. Sivakumar et al. [35], unimodal systems are fast-use biometrics and are applied to various real-time applications as it is difficult to steal like traditional password based systems. But also protecting the biometrics database is also a challenge. To reduce the error rate and increase accuracy, multimodal biometric systems are proposed. The author proposed a deep hashing secure framework for protecting multimodal biometrics. Finger and finger-vein biometric image data is collected and applied VGG19 algorithm for feature extraction and recognition. The system obtained an accuracy of 95%.

For HR personnel to use with corporate employees, V. Garget al. [36] presented an attendance management system. The technology has produced reliable and precise results. Also, the approach saved time and money.

N. Dhanalakshmi et al. [37] presented a GSM-based wireless fingerprint terminal-based attendance tracking system for recording students' actual attendance (WFTs). Student verification uses a unimodal trait fingerprint. For the verification procedure, the author suggested two techniques. One verifies using the database server, while the other does so using the Aadhar Central Identification Repository (CIDR). The image of the fingerprint was captured using a wireless fingerprint terminal. If the ward is irregular with the organization, parents are informed.

Hamami et al. [38] indeed presented a multimodal view of fusion structures.Facial biometrics with iris features for feature-level merging. This assessment uses several methods.Integrate extraction and support vector machines, apply quotes for customer review, and give accuracy up to 98.6%

A review article led by AI-Waisey et al. [39] presented a multimodal biometrics framework for client-perceptible evidence called the Iris Conv Net. It uses a combination of positioning levels to integrate the iris of both the right and left eye. The framework quickly identified the iris pattern in the eye image and then recognized its location incorporated into the neural network solution. The framework has achieved 100% success.

A similar study by another reviewer, AI-Waisy et al. [40] Facilitate biometrics to differentiate frames of evidence in terms of left and right eye facial images and iris patterns. Face ID, the Locale technology used for face identification, and the Deep Belief Network (DBN) have been inserted. The Iris Conv Net was used as proof of iris identification. Various strategies were used to merge matching values, and the accuracy of the presented framework was 99.9%.

Himanshuet al. [41] proposes a useful feature-level fusion technique for multimodal biometric systems. The four main steps of the proposed method are preprocessing, feature extraction, optimal feature-level fusion, and recognition. Geometry highlights were isolated using a modified district development calculation and surface elements were removed using HMSB Administrator. In addition, relevant features were selected by applying optimization techniques. The ideal components were selected using OGWO + LQ calculations. On the positive side, multipart support vector machine (MKSVM) estimation was used for confirmation. Evaluate the implementation of the proposed strategy using measures such as responsiveness, specificity, and accuracy. The proposed strategy outperforms other techniques in terms of recognition, specificity and accuracy, as shown by experimental results and similar studies. As a result, multimodal biometric systems can greatly benefit from the efficiency of the proposed method. Individual validations show that using Convolution Brain Networks is an effective way to attach a multimodal biometric framework to the device. Carrying out the proposed work on CNN will be a future effort [42].

According to Joseph et al. [43]. Application security cannot be guaranteed without authentication. Cloud computing is a model for utilizing the Internet to provide IT-related services to various end-users. Cloud services are becoming easier to use over time due to the greater degree of freedom for users. It also raises concerns about information security. Inherent biological patterns in multimodal biometric systems increase the robustness of the authentication mechanism. Captured design accurately separates individuals and their characteristics. Moreover, this concept can be applied in various ways to harden the system. This includes but is not limited to, safeguarding health information and the human genetic code for future reference through digital ledger management and EHR management. In this work, a multimodal biometric authentication scheme is proposed to enhance cloud-based data security. It uses MD-5 hash calculations to combine elements removed from unique fingerprints, irises, and palmprints in multiple stages to produce a hash of the enigmatic key's strings and digits. Protected data is encrypted with one of three symmetric key encryption algorithms (DES, AES, or Blowfish) using the private key. AES outperforms the other two algorithms in terms of performance in terms of the strength of the encryption process, while DES takes less time to run. This model demonstrated the robustness of data security due to the amalgamation of human modalities in security mechanisms.

Shraddha Arya and Arpit Agarwal [44] proposed a method to create and implement a face recognition system that can authenticate full or partial facial images. The process involves several steps, including pre-processing of the images, implementation of LDA algorithm, and the use of a neural network. During pre-processing, the facial image is partitioned into multiple facial parts. The LDA algorithm is then applied to reduce the dimensions of the facial images while preserving as much information as possible for recognition. Finally, a neural network is used to train the extracted features in the database, and the trained model receives the input image to compute the input faces for authentication.

Prashant Ksambe, Akash Upadhyay, Anushka Waingankar, Nevil Poonawalla, and Ruchi Shah [45] proposed a mobile-based attendance system that utilizes machine learning-based face recognition techniques. The system employs a mobile application to mark attendance by recognizing the faces of the individuals. The study shows that the proposed system is capable of dealing with variations in face poses and lighting conditions. The face recognition method relies on deep learning and solves the problem of illumination by converting the original image into a HOG representation that captures major image features, irrespective of brightness. The approach also involves considering local facial landmarks for further processing, followed by encoding the faces to generate 128 measurements. Finally, the optimal face recognition is achieved by matching the encoding with the person's name. The authors have claimed a high accuracy of 98.3% for the system.

Shama S, Karthikeyan Shanmugasundaram, and Satees Kumar Ramasamy [46] proposed a deep learning-based face recognition system that uses a Convolutional Neural Network (CNN). The system utilizes the Dlib library for face alignment, recognition, and implementation of the FAREC algorithm, written in C++ for computer vision. The authors explain how CNN and Dlib assist in facial recognition. The system compares input images with those in the database and achieves maximum accuracy through the use of trained feature models. The system has a low false acceptance ratio (FAR) of 0.1 and an accuracy of 96%. The application is designed to open the webcam to capture a photograph of the user, and CNN using Dlib algorithms recognizes the face. The image is then compared with the database, and attendance is marked if the image matches the database.

S. Asadi et al. [47] propose a multimodal biometric recognition system based on the fusion of face and voice modalities. Deep Belief Networks are used to extract features from both modalities and combine them using a weighted sum approach. The proposed system achieves high accuracy on a database of face and voice samples.

N. N. Brahmbhattet al. [48] propose a multimodal biometric authentication system that combines face and speech recognition. Linear Discriminant Analysis and Support Vector Machine classifiers are used to fuse the information from the two modalities. The system is tested on the XM2VTS database and achieves an accuracy of 98.34%.

M. Arun et al. [49] propose a multimodal biometric authentication system that combines fingerprint, face, and iris recognition. A weighted score level fusion approach is used to combine the results from each modality. The proposed system achieves high accuracy on a database of fingerprints, faces, and irises.

T. Liuet al. [50] propose a multimodal biometric authentication system that combines facial and palmprint features. The system uses a combination of feature level and score level fusion approaches to combine the results from each modality. The proposed system achieves high accuracy on a database of facial and palmprint samples.

Leghari, et al. [51] propose a CNN-based deep learning model for the feature-level fusion of online fingerprints and signatures. For convolutional and fully connected layers, early and late feature fusion techniques have been developed that combine features from both biometric modalities. Fingerprint images have a fixed size of 150x150x1 and online signature files are 17x17 pixels. The signature was resized to 1 x 17 x 1 before being sent to the online signature network to combine the online signature and fingerprint properties. Various systems have attempted to integrate elements of web-based signatures with unique fingerprint images. However, setting the component vector width of the web-based mark to 1 did not affect the accuracy or other properties of other scores in the proposed framework. This issue has been resolved by adding two layers of zero padding to the signature network to improve the system's accuracy and the value of other metrics. Additional zeros were added to at least the top, bottom, left, and right of the element vector using this zero fading strategy. As a result, the dimensions of the final feature vector increased to 4 x 4. Similarly, the final feature vector for fingerprints was 4 x 4. These features were concatenated and passed through fully connected layers to extract and classify features in a more abstract way. The model was trained and tested on a new dataset. The system had an accuracy of 99.10% in the early fusion mode and an accuracy of 98.35% in the late fusion mode.

In this study, we collected facial and fingerprint data through the utilization of a web camera and the Mantra fingerprint scanner. The real-time data obtained was employed both for training and testing the model. Additionally, attendance was recorded in the portal, and an Excel sheet report was generated for comprehensive record-keeping, offering an extra benefit in comparison to prevailing systems.

Introduction to Sift

Scale-Invariant Feature Transform, or SIFT, was initially introduced by D. Lowe [52] of the University of British Columbia in 2004. The SIFT algorithm is a technique for extracting unique, invariant features from images. It may also be used to match several viewpoints of an image. SIFT is a robust algorithm that can handle a wide range of image transformations, including scaling, rotation, and illumination changes. It has been widely used in various computer vision applications, such as object recognition, image stitching, and 3D reconstruction.

Key Benefits of Sift

- Locality: Features are local, making them resistant to occlusion and clutter.
- Uniqueness: Certain features may be compared to a vast database of images.
- Quantity: Even small images can create a large number of features.
- Efficiency: an accurate performance that is nearly real-time
- Extensibility: Easily extensible to a variety of distinct feature types, each of which improves robustness [53].

Sift Algorithm

The SIFT algorithm consists of the following steps:

- Scale-space extrema detection: The first step involves building a scale space pyramid of the input image, where each level in the pyramid corresponds to a different scale. At each level, the difference of Gaussians is computed to identify potential interest points that are both scale and spatially invariant.
- Keypoint localization: In this step, potential interest points are refined and filtered to improve their stability and repeatability. The algorithm eliminates points with low contrast or that are located on edges or corners.
- Orientation assignment: At each interest point, a dominant orientation is assigned based on local gradient orientations. This step makes the algorithm invariant to rotation.
- Keypoint description: In this step, a local image descriptor is generated for each interest point based on the gradient magnitudes and orientations in its surrounding region. The descriptor is robust to scale, rotation, and illumination changes.
- Keypoint matching: The final step involves matching key points between different images using their respective descriptors. A common approach is to use a nearest-neighbor algorithm to find the closest match between key points in two images.

Scale-space extrema detection:

Real world elements are significant only at a definite scale. The multi-scale nature of elements is fairly frequent in nature. And a scale space tries to reproduce this concept on digital images.

The scale space of an image is characterized as a function, L(x, y, σ), that is formed fromthe convolution of a variable-scale Gaussian, G(x, y, σ), with an input image, I(x, y):

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

where ∗ is the convolution operation in x and y, and

$$G(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)}$$

To efficiently perceive stable keypoint locations in scale space, it is suggested using scale-space extrema in the difference-of-Gaussian function convolved with the image, D(x, y, σ), which can be calculated from the difference of two close by scales separated by aconstant multiplicative factor k:

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y)$$

$$= L(x, y, k\sigma) - L(x, y, \sigma)$$

For every octave of scale space, the initial image is repetitively convolved with Gaussians to create the set of scale space images shown on the left. Neighboring Gaussian images are subtracted to generate the Difference-of-Gaussian images on the right as illustrated in Figure 3. After each octave, the Gaussian image is down-sampled by a factor of 2, and the procedure is continued.

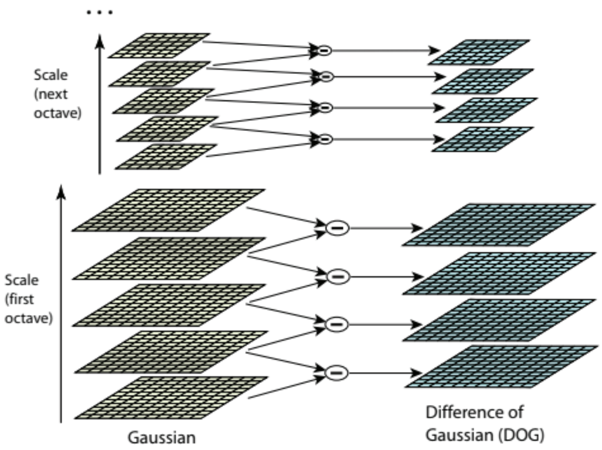


Figure 3. Gaussian & difference of gaussian.

Now to find the keypoints, i.e., maxima and minima, of the difference of gaussian images by comparing a pixel with 8 neighbours and 9 pixels in the next scale and 9 pixels in previous scales as represented in Figure 4. So a total of 26 comparisons are done. If it is a local extrema, it is a potential keypoint.

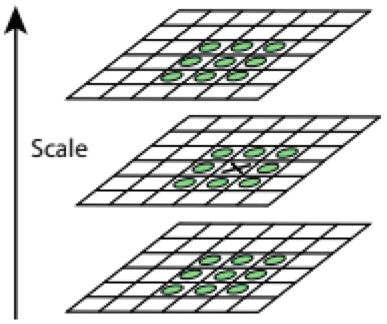


Figure 4. Comparing neighbouring pixels to find key points.

Keypoint Localization

After identifying keypoints by comparing a pixel to its neighbours, the next action is to do a thorough fit to the close by data for location, scale, and ratio of principal curvatures. It permits the points to discarded that have low contrast or are weakly localised along an edge.

The Taylor series is used to obtain a more precise location of extrema, and if the intensity at this extrema is less than a threshold value (0.03), it is discarded. DoG has a higher response for edges, so edges also need to be removed.

Orientation Assignment

Now we have stable keypoints. and we also know the scale at which keypoints were perceived. So it is scale invariance. The next step is to allot an orientation to each keypoint to make them orientation invariant.

The scale of the keypoint is used to select the Gaussian smoothed image, L, with the closest scale, so that all computations are performed in a scale-invariant manner. For each image sample, L(x, y), at this scale, the gradient magnitude, m(x, y), and orientation, θ(x, y), is precomputed using pixel differences:

$$m(x,y)=\sqrt{}(L(x+1,y)-L(x-1,y))^2+((L(x,y+1)-L(x,y-1))^2$$

$$\theta(x,y) = tan^{-1}\frac{L(x,y+1)-L(x,y-1)}{L(x+1,y)-L(x-1,y)}$$

An orientation histogram is produced from the gradient orientations of sample points within a region around the keypoint. The orientation histogram has 36 bins covering the 360 degree range of orientations. Every sample added to the histogram is weighted by its gradient magnitude and by a Gaussian-weighted circular window with a σ that is 1.5times that of the scale of the key point. Peaks in the orientation histogram correspond to dominant directions of local gradients. The highest peak in the histogram is perceived, and then any other local peak that is within80% of the highest peak is used to also create a keypoint with that orientation as illustrated in Figure 5.

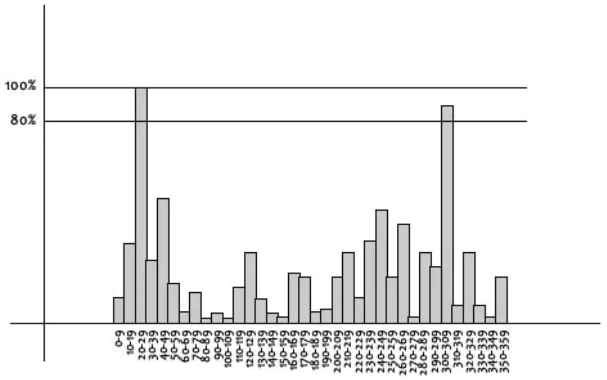


Figure 5. Histogram Representation.

Keypoint Description

Currently, each keypoint has a location, scale, and orientation. The next step is to calculate a descriptor for the local image region regarding each keypoint that is extremely unique and invariant as well as probable to variations such as changes in viewpoint and illumination[53].

A keypoint descriptor is formed by first calculating the gradient magnitude and orientationat every image sample point in a region around the keypoint location, as shown on the left of Figure 6. These are weighted by a Gaussian window, designated by the overlaid circle. These samples are then accumulated into orientation histograms briefing the contents over 4x4 subregions, as shown on the right of Figure 6, with the length of each arrow equivalent to the sum of the gradient magnitudes close to that direction within the region. The Figure 6 shows a 2x2 descriptor array computed from an 8x8 set of samples.

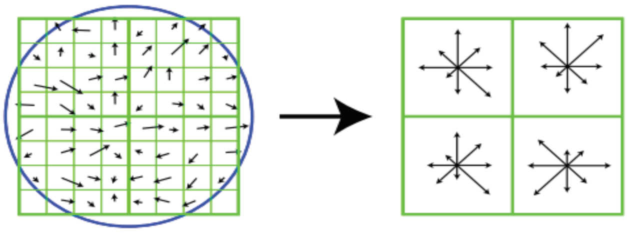


Figure 6. Image gradients-Keypoint Descriptor.

Keypoint Matching

The best candidate match for each keypoint is found by recognizing its nearest neighbor in the database of keypoints from training images. The nearest neighbour is defined as the keypoint with the minimum Euclidean distance. But in some cases, the second closest-match may be very close to the first. It might occur due to noise or some other reason. In that case, the ratio of the closest-distance to the second-closest distance is taken. If it is greater than 0.8, they are rejected.

RELATED WORK

Taking attendance of students in class is a time-consuming and tedious task in traditional systems. To address this issue, a unimodal biometric system is introduced. To mark attendance, unimodal systems use either fingerprint or facial recognition. However, there are some issues with unimodal, such as noise in collected data, nonuniversality, similarity in collected data, and so on [54].

Multi Modal Biometrics

The problems of a unimodal system are reduced by multimodal biometrics[55]. It takes into account more than one biometric trait when recognising a person and recording attendance. The system compares all biometrics to match the person with the existing database, improving accuracy over unimodal systems [56][57]. In this paper, we use face and finger print recognition as biometric traits to identify students and record attendance [58].

Technology for Facial Recognition

The features of the face image are captured using a web camera. Individual facial features are compared with the database to authenticate the user [59] as illustrated in Figure 7.

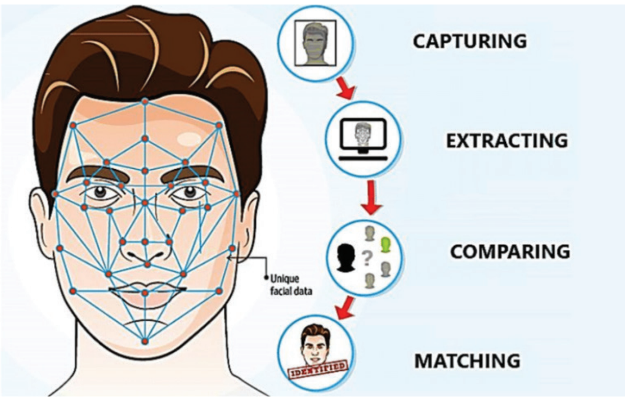


Figure 7. Face recognition steps using various features.

The multiple features in the face image are used to recognize the authorized user [60]. Distances between the various features of the face image are measured. These measurements are stored in a database and used during verification as a basis for comparison.Some of the facial measurements are as follows:

- The space between the eyes
- The nose's width
- Dimensions of the cranial-orbital region
- Contour of the cheekbones
- Width of the jaw bone

Above measurements are captured, and a face print (numerical code) is created and preserved in the database. This code is crucial for recognizing the facial image accurately.

One big benefit of facial recognition technology is that it is non-intrusive [61]. Without a person's knowledge, they can be taken from a considerable distance. Facial biometrics eliminates the problems associated with biometric systems that rely on characteristics that require the user to touch [62].

Technology for Finger Print Recognition

The fingerprint structure is depicted in Figure 8 along with illustrations of crossovers, cores, bifurcations, ridge endings, islands, deltas, and pores.

The whorl, loop, and arch are the three chief fingerprint ridge patterns. As a ridge enters a finger from one side, it rises in the middle to form an arch before leaving the finger from the opposite side. A loop occurs when the ridge enters

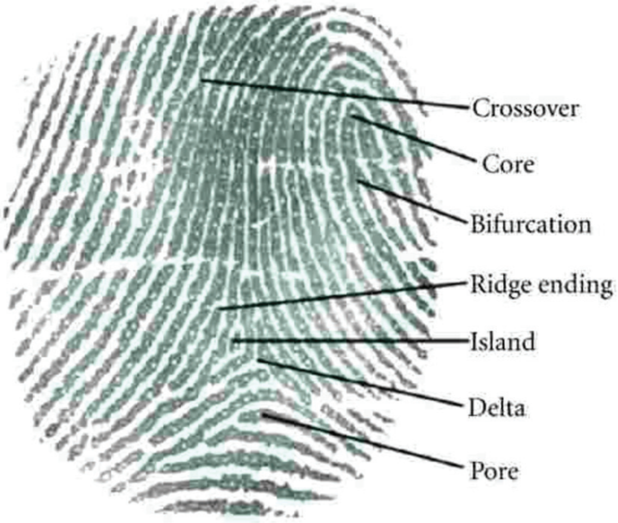


Figure 8. Structure of finger print.

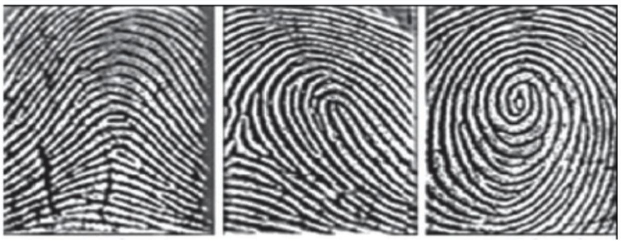


Figure 9. Types of finger prints: Arch, loop, whorl.

the finger from one side, curves, and then departs the finger from the same side. The most frequent pattern seen in fingerprints is a loop. Last but not least, a whorl isthe pattern that results from ridges forming in a circle around a central point.For illustrations of each pattern, view Figure 9.

Fingerprint biometrics contain minutiae scores. Minutiae are the precise points in a fingerprint. The ridge ending, bifurcation and dot are the primary features of minutiae. The ridge ending is the mark where ridge ends. A bifurcation is the mark where ridge divides into two ridges. Dots are the shorter ridges.By comparing minutiae scores, fingerprints can be recognized.

The SIFT operator is used to extract features from the fingerprints. Using the descriptors that each feature point is represented by, SIFT identifies consistent feature points in an image and compares them.

Construction of Scale Space

An image's scale space is produced by applying a variable-scale Gaussian operator to it. Images made using Difference of Gaussian (DOG) are created by subtracting the scales after each octave. DOG pictures and images that have been smoothed with a Gaussian filter make up an octave. By down sampling the source image several times, such octaves are produced. The use of 5 and 6 scales and octaves is necessary for SIFT to function.

Local Extreme

Every point in the DOG space picture is observed in order to identify local extremes.When the value of a point is smaller or larger by a specific margin than the values of all of its adjacent neighboring points, it is determined to be a local minimum or maximum.

Assigning Descriptor

Each local extreme is compared to the other using the linked descriptors to perform matching. Consider the scenario where we wish to compare two pictures IM1, IM2. A characteristic point pt11 in IM1 is given, and the distances dt1 and dt2 between it and its closest points, pt21 and pt22, are determined from characteristic points in IM2. When dt1/dt2 is sufficiently small, pt11 and pt21 are regarded as matches. The number of similarity points and geometric configurations of the two images can be used to calculate the similarity score between the two images.

Implementing SIFT on Fingerprint Images

1) Distinctive fingerprint feature points:Ridge ends and bifurcation points are used to precisely specify minutiae points. As a result, there are only about 100 tiny points that may be seen in a fingerprint image. Although there are many feature points, Number of factors, including the number of octaves and scales, have an impact on the number of SIFT feature points. A normal fingerprint contains close to a few thousand SIFT feature points.A comparison of SIFT feature points and minutiae points on the identical fingerprint image is shown in Figure 11. Although there are just 36 minutiae points, 2,020 SIFT feature points are recorded, as seen in Figure 10. The SIFT parameters were 4 octaves, 5 scales, 3 as the width of the Gaussian kernel, and an initial standard deviation value of 1.8.

2) SIFT Processing-based fingerprint verification*:* A few preprocessing procedures are included in order to improve the matching performance of the SIFT operator [63]. Two steps make up the pre-processing: (i) altering the greylevel

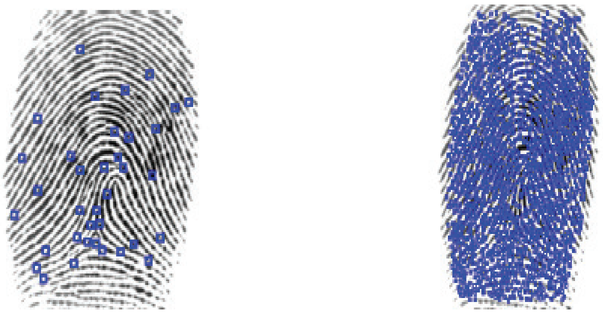


Figure 10. Extraction of minutiae and SIFT feature points from a single image. First image shows 36 Minutia points second image shows SIFT feature points.

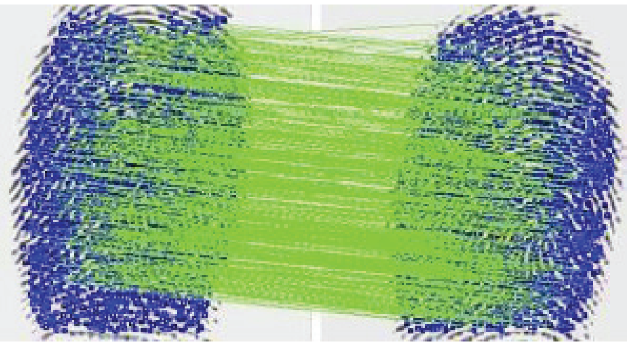


Figure 11. An explanation of the SIFT operator's fingerprint matching technique.

pattern, and (ii) deleting unwanted SIFT feature points. Performance is expected to improve when fingerprintphotos have a comparable texture since SIFT employs texture information for both extracting feature points andmatching.To enhance comparison performance, unwanted SIFT feature points are deleted for the same reason.

First, we assess the picture intensity in the fingerprint's centre region and update the histogram to correct certain apparent variations in gray level distributions. Second, because they are local extrema, feature points in a fingerprint's boundary area are always picked up. Even for the same finger, the boundary area varies for each fingerprint imprint. As a result, false matches frequently emerge from feature locations on the fingerprint boundary. To avoid unwanted feature points from appearing at the border, we generate a binary mask that only comprises the inner component of a fingerprint and apply it there. Green samples of binary masks are presented in figure.

3) Point-by-Point Comparison:As shown in Figure 11, The first step in point-by-point comparison is to match each feature point using the Euclidian distance as the distance measurement metric..

4) Eliminating Incorrect Matches:The false acceptance rate rises as a result of certain inaccurate matching points produced by point-wise matching. Therefore, when two fingerprint photos are put side by side and similar lines are formed, all genuine matches appear as parallel lines of approximately the same length[14]. Based on this observation, we determine the majority direction and length and maintain the matched pairs that meet these criteria.

MATERIALS AND METHODS

The overall system architecture, shown in Figure 14, encompasses two main modules: a web interface for accessing the system for enrolling the student using fingerprint and facial image data, and a verification module for comparing the database to confirm the authorized student.

The fingerprint pictures are collected utilizing Mantra MFS scanner as shown in Figure 12. The MFS100 USB fingerprint sensor is a high-quality option for desktop or network security fingerprint authentication. MFS100 depends on optical detecting innovation which effectively perceives low quality fingerprints too. MFS100 can be utilized for validation, ID and check works that let your unique finger impression carry on like computerized passwords that cannot be lost, neglected, or taken. Scratches, impacts, vibration, and electrostatic shock are all prevented by a hard optical sensor. Attachment and play USB 2.0 rapid point of interaction upholds numerous gadgets taking care of. 500 dpi optical finger impression sensor scratch free sensor surface.

The face pictures are gathered utilizing zebronics Zeb-Gem Genius webcam as shown in Figure 13. A USB-powered web camera with a 3P lens and clear videos is the Zeb-Crystal Pro. It has night vision, a clip-on design for easy mounting, and a built-in microphone. 30 frames per second, 640 x 480 video resolution, and 1.2 meters of cable. The webcam can be used directly without the need for drivers.

In enrolment phase dataset is created with basic details of the student along with facial and finger print images.

Figure 12. Mantra finger print scanner.

Figure 13. Webcamera.

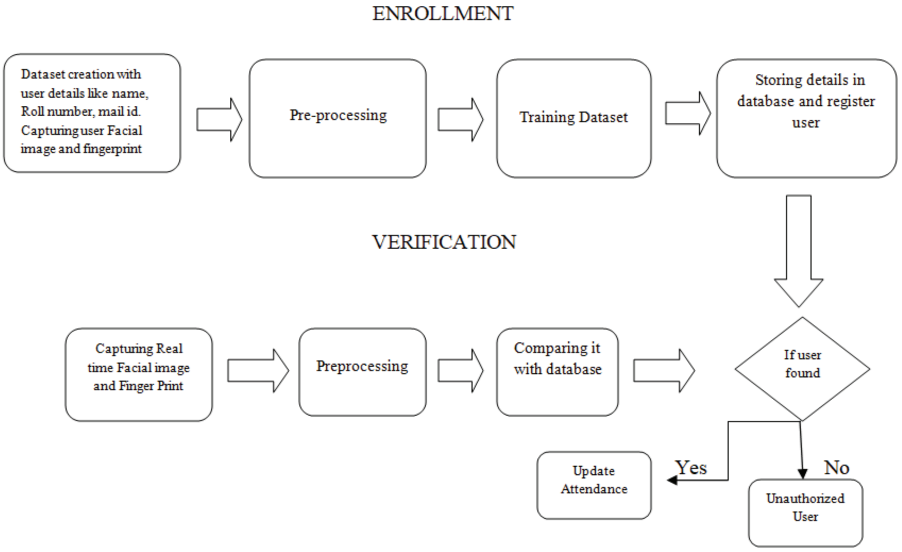

ENROLLMENT
Dataset creation with user details like name, Roll number, mail id. Capturing user Facial image and fingerprint
Pre-processing
Training Dataset
Storing details in database and register user
VERIFICATION
Capturing Real time Facial image and Finger Print
Preprocessing
Comparing it with database
If user found
Yes
No
Update Attendance
Unauthorized User

Figure 14. Architecture of attendance system.

After collecting data facial and fingerprint data need to be pre-processed for removal of any unwanted or noisy data. After pre processing, the database is updated and the student is registered. The system is trained with the existing data base.

At the time of attendance monitoring, verification module gets enabled. Before updating the attendancesheet student facial and finger print images are captured, are preprocessed and compared with the existing registered student data. If the data is matched or found, the student will be considered as an authorized user and attendance is updated in the excel sheet else considered as unauthorized user and an error message is popped.

The system was built using the Python programming language. GUIs can be easily created in Python using the Tkinter package. Tkinter is the only GUI framework that is part of the Python Standard Library among a variety of GUI frameworks. The GUI of the student attendance system in our model was created using Tkinter and is depicted in Figure 15.

We used OpenCV for image database. OpenCV is a library where there are lots of image processing functions are available. This is very useful library for image processing.

OpenCV is a video and image processing library and it is used for image and video analysis, like facial detection, license plate reading, photo editing, advanced robotic vision, and many more. OpenCV is the huge open-source library for the computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today’s world.

A Convolutional Neural Network (CNN)[64] is a Deep Learning algorithm which can take in an input image, assign importance (learnable weights and biases) to various aspects/objects in the image and be able to differentiate one from the other.

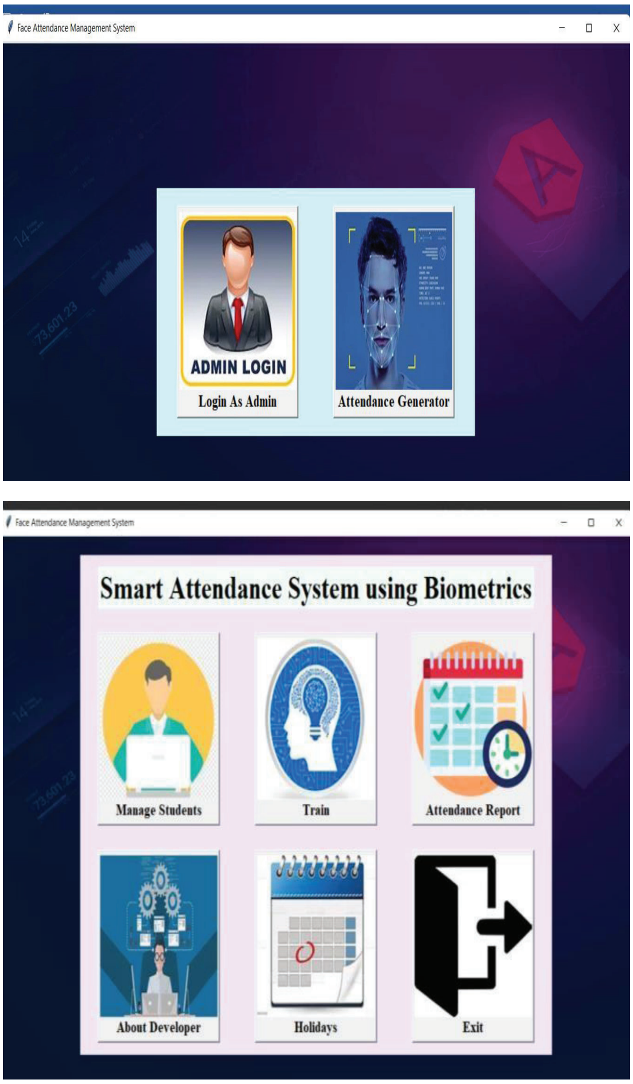


Figure 15. GUI of attendance system.

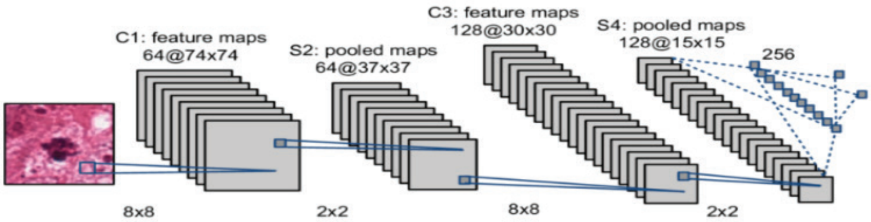


Figure 16. Architecture of CNN model.

CNN is based on the human visual cortex and is the neural network of choice for computer vision (image recognition) and video recognition. It is also used in other areas such as NLP, drug discovery, etc. As shown in Figure 16, CNN consists of a sequence of convolution and sub-sampling layers followed by a fully connected layer and a normalizing layer. The figure demonstrates the mitosis/non-mitosis classification. The series of multiple convolution layers perform increasingly more refined feature extraction at every layer moving from input to output layers. Fully connected layers perform classification by convolutional layers. Downsampling or aggregation layers are usually inserted in between each convolution layer.

CNN takes a 2D nxn pixelated image as input. Each layer consists of a set of 2D neurons called filters or kernels. Neurons in each feature extraction layer of CNN are not connected to the spatially mapped fixed-sized and partially overlapping neurons in the previous layer's input image or feature map. All neurons in a filter are connected to the same numberof neurons in the previous input layer (or feature map) and are bound to have the sameseries of weights and biases. These causes speed up the learning and reduce the memory requirements for the network. Thus, each neuron in a definite filter looks for the same pattern but in different parts of the input image. Downsampling layers reduce the size of the network.Local average or maximum/average aggregation filters are often used for downsampling. Final match CNN layers are responsible for the actual classification, where neurons between layers are fully connected.

The preprocessing required in a CNN is much lower as compared to other classification algorithms. While in primitive methods filters are hand-engineered, with enough training, CNN have the ability to learn these filters/characteristics.A CNN is able to successfully capture the Spatial and Temporal dependenciesin an image through the application of relevant filters. The architecture performs a better fitting to the image dataset due to the reduction in the number of parameters involved and reusability of weights. In other words, the network can be trained to understand the sophistication of the image better.

Dlib is a modern C++ toolkit containing machine learning algorithms and toolsfor creating complex software in C++ to solve real world problems.

DLib is much like DMTL in that it provides a generic high-performance machine learning toolkit with many different algorithms, but DLib is more recently updated and has more examples. DLib also contains much more supporting functionality.What makes DLib unique is that it is designed for both research use and creating machine learning applications in C++

dlib includes two face detection methods built into the library:

1. A HOG + Linear SVM face detector that is accurate and computationally efficient.
2. A Max-Margin (MMOD) CNN face detector that is both highly accurateand very robust, capable ofdetecting faces from varying viewing angles, lighting conditions and occlusion.

Best of all, the MMOD face detector can run on an NVIDIA GPU, making it super fast.

In this paper we are using MMOD CNN face detector.

The MMOD CNN architecture consists of multiple layers of convolutional neural networks, which learn to extract features from images. The features are then fed into a set of fully connected layers, which make predictions about the presence and location of faces in the image. The MMOD CNN is designed to handle multi-scale detection, meaning it can detect faces of different sizes in an image as shown in Figure 17.

One of the key features of the MMOD CNN is that it uses a "sliding window" approach to detect faces. This means that the network is applied to different parts of the

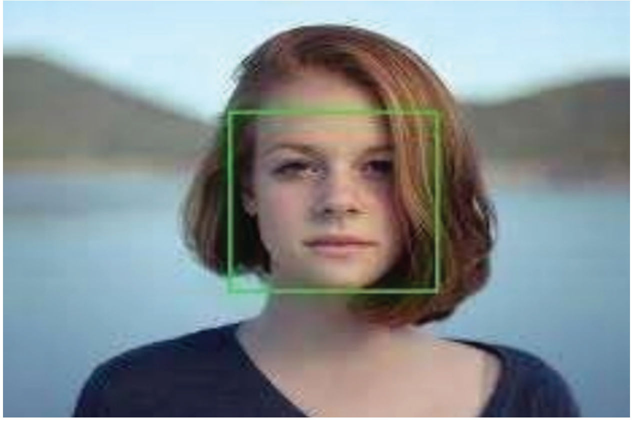
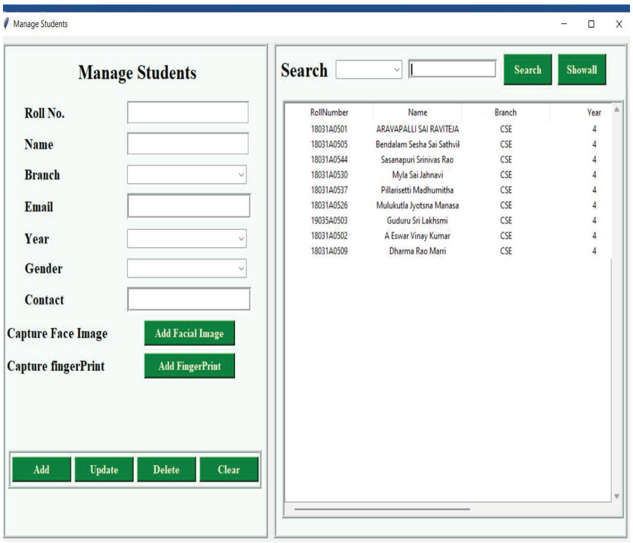
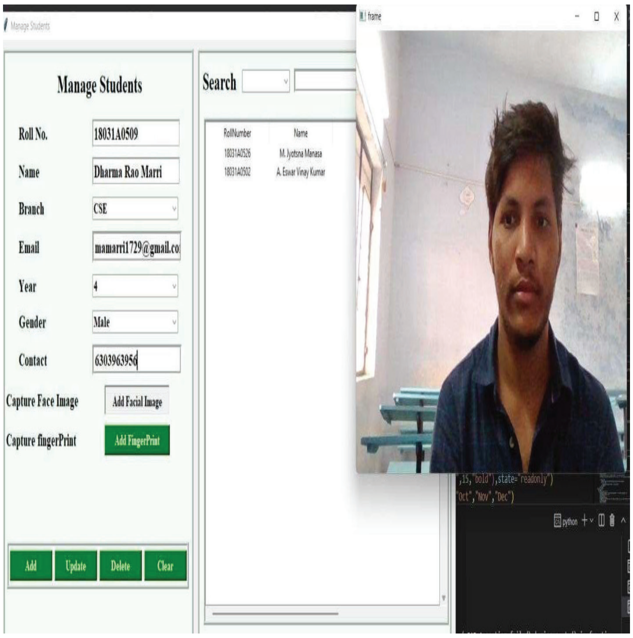


Figure 17. Face detection using dlib MMOD CNN face detector.



RollNumber	Name	Branch	Year
18031A0501	ARAVAPALLI SAI RAVITEJA	CSE	4
18031A0505	Bendalam Sesha Sai Sathvik	CSE	4
18031A0544	Sasanapuri Srinivas Rao	CSE	4
18031A0530	Myla Sai Jahnavi	CSE	4
18031A0537	Pillarisetti Madhumitha	CSE	4
18031A0526	Mulukutla Jyotsna Manasa	CSE	4
19035A0503	Guduru Sri Lakhsmi	CSE	4
18031A0502	A Eswar Vinay Kumar	CSE	4
18031A0509	Dharma Rao Marri	CSE	4

Figure 18. Manage user details page.



Roll No. 18031A0509
Name Dharma Rao Marri
Branch CSE
Email mamarri1729@gmail.co
Year 4
Gender Male
Contact 6303963956

RollNumber	Name
18031A0526	M. Jyotsna Manasa
18031A0502	A. Eswar Vinay Kumar

Figure 19. Capturing facial image.

image at different scales, allowing it to detect faces of different sizes. The network also includes a set of anchor boxes, which are used to predict the position and size of faces in the image.

The MMOD CNN is trained using a combination of positive and negative samples. Positive samples are images that contain faces, while negative samples are images that do not contain faces. During training, the network adjusts its parameters to minimize the difference between its predictions and the ground truth labels.

Dataset Creation

To manage the attendance of any student, first we have to upload all the information of the student like Name, Roll Number, E-Mail, Branch, Year, Gender, Phone Number and the Date of Birth. In order to calculate any student attendance, they have to add their profile in the database as depicted in Figure 18.

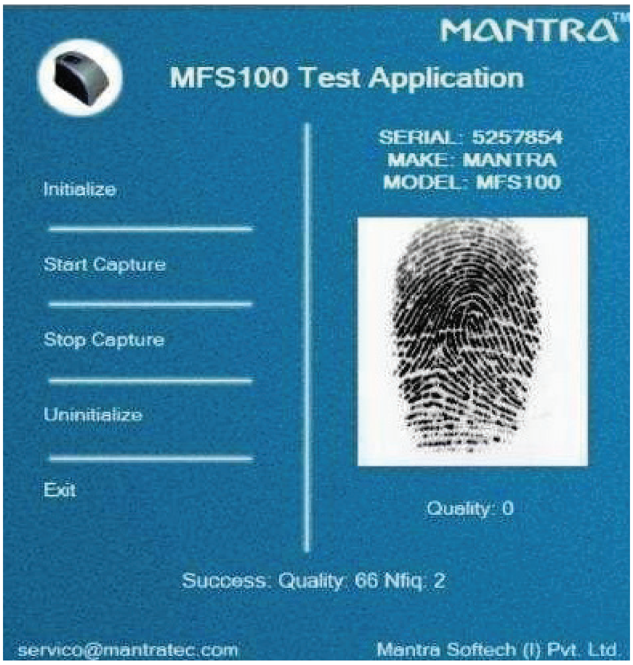
After adding all the details of the student, they have to add their profile to the database. And here we are using the roll number as the primary variable. Without roll number no one is able to add the data to the database. In the proposed methodology, students can add their data to the database by using the manage student button that is provided on the home page.The student must now provide their photo samples for the creation of the dataset for each student after filling out all the necessary information.

Image Acquisition Phase

The biometric traits must first be acquired and saved in the database in order to identify a person using those traits. The system must gather data from sensors and cross-reference it with the current database when authenticating the user.

The process of acquiring images happens during the image acquisition phase. Fingerprints and facial photographs will be recorded using a MANTRA Fingerprint Sensor (MFS100) and a web camera, respectively.

An optical fingerprint reader is used to capture an image of the fingerprint during online fingerprint identification. The fingerprint image will have a dimension of 260 by 300 pixels. Figure 19, 20 illustrates the capture of a fingerprint using MFS100.



SERIAL: 5257854
MAKE: MANTRA
MODEL: MFS100

Quality: 0

Success: Quality: 66 Nfiq: 2

Figure 20. Capturing fingerprint.

Difficulties encountered in facial recognition:

Illumination :Illumination represents changes in light. slight change in lighting conditions are controlled by automated facial recognition and it can have a big impact on your results.

Pose: The system is very sensitive to pose changes. When the pose of the face changes People's head movements and viewing angles change. Head movement different camera perspectives always change the appearance of the face, generating intra-class variations and reducing automatic face recognition rates Drastic. Changing the rotation angle makes it difficult to distinguish the real face higher. Using only the database can result in false positives or no detections There is a front view of the face.

Occlusion: Occlusion means blockage, The face is blocked and the whole face cannot be used as input image. Occlusion is considered one of the most important challenges in facial recognition systems. It occurs due to accessories applied to beards, mustaches (goggles, hats, masks, etc.), it is widely used in real-world scenarios. The presence of such components makes the automatic face recognition process very difficult due to the diversity of subjects.

Expression: The face is one of the most important biometric data due to its unique features. An important role in providing human identity and emotion. Different moods that lead to different emotions being shown and eventually changing facial expressions.

Low resolution: The minimum resolution for standard images is 16*16. Images with a resolution of less than 16*16 are called low-resolution images. These low-level images can be found on small standalone cameras such as CCTV. Street cameras, ATM cameras, and supermarket surveillance cameras. These cameras capture a small portion of the human face area. Since the camera is not very close to the face, only face areas less than 16*16 can be captured. A low-resolution image like this doesn't provide much information because most of the information is lost, it can be a big challenge during face recognition.

Aging: The appearance/texture of the face changes over time, reflecting age, This is another challenge for facial recognition systems. With aging Human facial features, shapes/lines, and other aspects also change. Resolved visual observation and image reproduction for the first time in a while. For accuracy check, a dataset was calculated for people of different age groups over a specific time period. Here, the recognition process consists of feature extraction, basic features such as wrinkles, markings, eyebrows, hairstyles, etc.

Preprocessing

1) Face image preprocessing: Here we use mainly 5 steps during the preprocessing they are as follows:

- Converting Facial image to Gray Scale Image: Grayscale images contain only shades of gray, without any color information. In contrast, colored images contain red, green, and blue (RGB) color channels, which increase the computational complexity of image processing algorithms. Converting a colored image to a grayscale image simplifies the image processing task and reduces the amount of data that needs to be processed. The conversion process involves assigning a gray value to each pixel of the image, based on the intensity of its original RGB values.

Figure 21 depicts the original image where as Figure 22 depicts the image after converting to Gray scale.

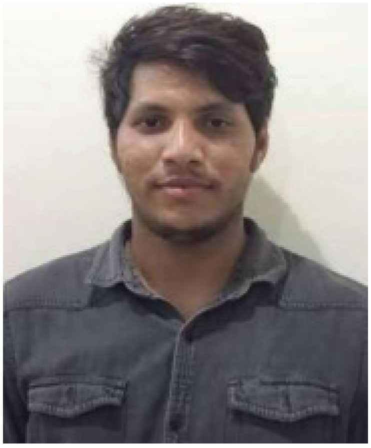


Figure 21. Original image of user.

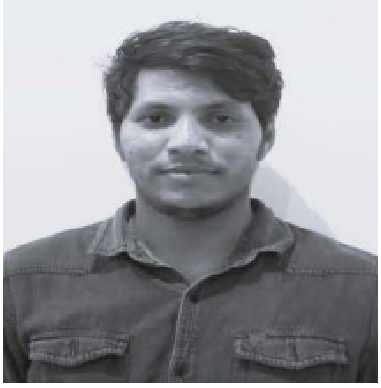


Figure 22. Gray scale image of user.

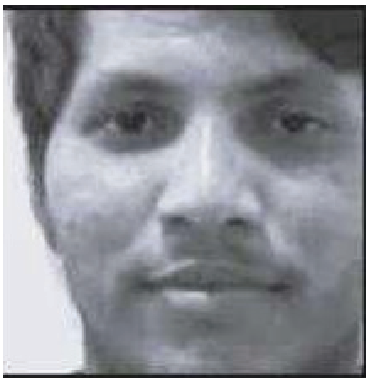


Figure 23. Face identification.

- Identifying Face locations: The process of identifying face locations, also known as face detection, is an important step in many facial recognition systems. This step involves identifying the regions within an image that contain a face, and is usually the first step in any facial recognition pipeline.CNNs use deep learning algorithms to automatically learn features that are most relevant for face detection. Figure 23 depicts the face identification.
- Removing background noise: The step of removing background noise refers to the process of removing unwanted and irrelevant information from an image that is not related to the object of interest. This can be particularly important in facial recognition systems, where the presence of background noise can negatively impact the accuracy of the system. Background noise can arise from a variety of sources, including lighting conditions, shadows, reflections, and other objects in the image that are not relevant to the face being recognized. Deep learning models such as convolutional neural networks (CNNs) can be trained to automatically remove background noise from face images.
- Extracting face landmarks: In facial recognition, extracting facial landmarks refers to identifying and locating key features of the face, such as the eyes, nose, mouth, and jawline. These landmarks are important for accurately identifying and recognizing faces, as they provide important information about the shape and structure of the face. To extract facial landmarks, the pre-trained convolutional neural network (CNN) model Dlib package was used.
- Retrieving Facial encodings: It involves extracting a set of features or unique identifiers from the preprocessed and aligned facial image. These features are then used to compare and recognize the face of the individual. Facial encoding is a process of measuring and quantifying various facial features like the distance between the eyes, the width of the nose, the shape of the lips, etc. These features are used to create a unique representation of the face that is specific to each individual. CNNs can automatically learn relevant features for face recognition from raw images through training on large datasets.Once the facial encodings have been extracted, they are compared to the encodings stored in the database for verification or identification. The similarity between the encodings is measured using a distance metric such as Euclidean distance or cosine similarity, and a threshold is set to determine whether the two encodings match or not.

2) Finger print preprocessing:

- Binarization of image: In fingerprint preprocessing, the step of "binarization of image" refers to converting the grayscale image of the fingerprint into a binary image. This is done to simplify the image and make it easier to extract features for fingerprint recognition. Binarization is done by thresholding the grayscale image, which involves setting a threshold value and assigning all pixel values below the threshold to 0 (black) and all values above the threshold to 1 (white). Figure 24 represents the fingerprint after binarization.
- Thinning of image:Thinning of an image refers to reducing the width of the ridges and valleys of the fingerprint image to a single pixel width. This is done to simplify the image and make it easier to extract features for fingerprint recognition. Thinning is performed by applying a thinning algorithm to the binary image obtained from the binarization step. Thinning algorithms work by examining the neighboring pixels of each ridge and valley pixel and removing them based on a set of rules. The process is repeated until the ridges

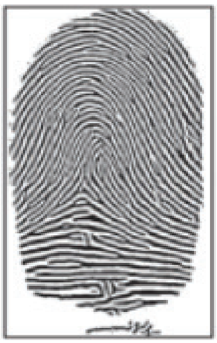


Figure 24. Finger print after binarization.

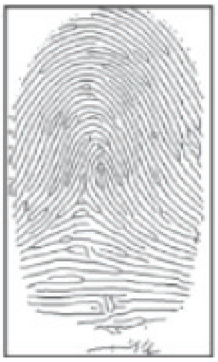


Figure 25. Finger print after thinning.

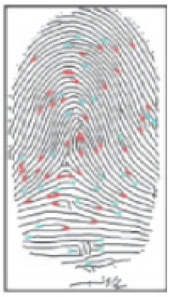


Figure 26. Minutia points extraction in finger print.

and valleys are reduced to a single-pixel width. Thinning is an important step in fingerprint recognition because it helps to reduce the computational complexity of feature extraction by simplifying the fingerprint image. It also helps to remove any noise or artifacts that may have been introduced during the binarization step. Figure 25 shows the effect of thinning on the finger print after binarization.

- Minutia points extraction: Minutiae extraction is an important step in fingerprint recognition. It involves the detection of unique characteristics or features of the fingerprint image, such as ridge endings, bifurcations, and other ridge characteristics that are used to uniquely identify an individual. The minutiae extraction process involves locating and extracting these unique features from the fingerprint image. Once the minutiae points are identified and extracted, they are used to create a template of the fingerprint, which is then used for comparison with other fingerprint templates in the database. The template contains information about the location, orientation, and type of each minutia point, which is used to determine the similarity between two fingerprints. Figure 26 shows the extracted minutia points extraction on the finger print.

Extraction of Features

The image feature extraction method is used in the output pre-processing stage. Ridge ends and bifurcations in the fingerprint are located, measured, and encoded using a fingerprint feature extraction process. The features from the fingerprint image can be extracted using a variety of techniques. The well-known technique is called the minutiae extraction algorithm, which locates the minute points and maps their relative locations on the fingerprint. Ridge ends and ridge bifurcations are two types of minutiae points. SIFT techniques are used to extract features from fingerprints. Individual face structures were localised using Dlib's facial landmark predictor.

RESULTS AND DISCUSSION

Comparison Phase

The process of comparing the acquired feature with the database template occurs during the comparison phase. The comparison phase is to verify how similar the extracted image from the user is to the image from the database. Figures 27,28 depicts detection of face and fingerprint image.

Updating Database

The proposed approach will use a webcam to find faces and then identify them. Following recognition, it will update the attendance record on the Excel sheet and designate the identified student as present, as illustrated in Figure 29.

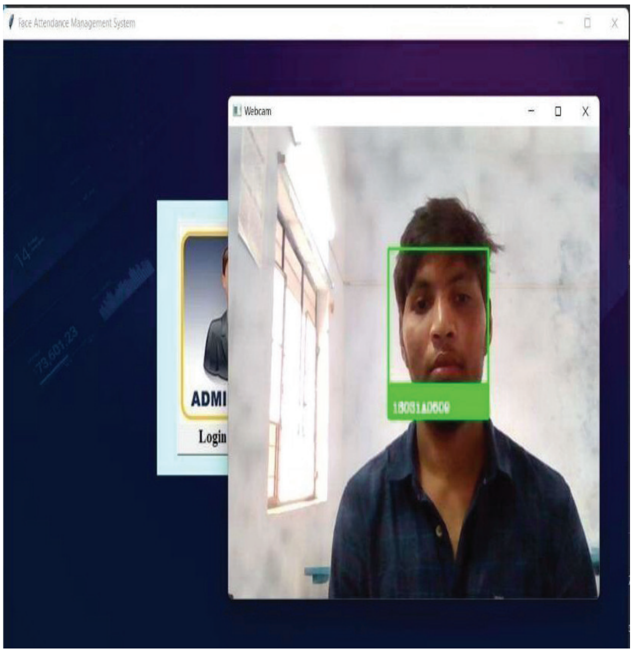
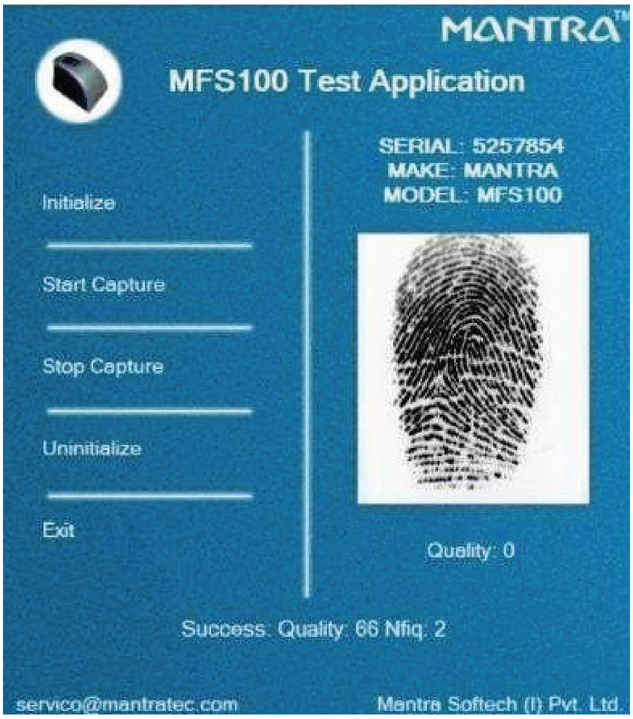


Figure 27. Face detection.



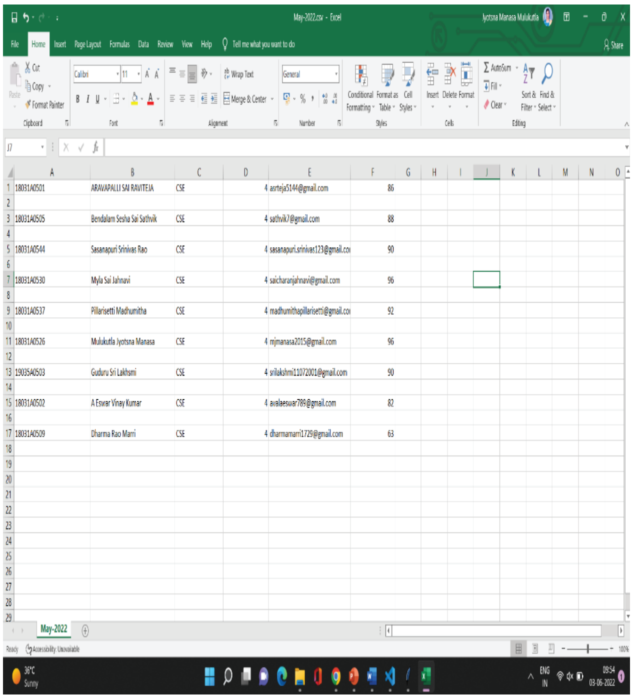
SERIAL: 5257854
MAKE: MANTRA
MODEL: MFS100

Quality: 0

Success: Quality: 66 Nfiq: 2

Figure 28. Fingerprint detection.

The automatic attendance system employing multimodal biometrics offers several advantages. Combining face and fingerprint recognition, it enhances security and reduces vulnerability to spoofing, providing a robust solution. This multimodal approach improves the accuracy and reliability of attendance tracking, minimizing errors in



	A	B	C	D	E	F
1	18031A0501	ARAVAPALLI SAI RAVITEJA	CSE	4	asrteja5144@gmail.com	86
2						
3	18031A0505	Bendalam Sesha Sai Sathvik	CSE	4	sathvik7@gmail.com	88
4						
5	18031A0544	Sasanapuri Srinivas Rao	CSE	4	sasanapuri.srinivas123@gmail.co	90
6						
7	18031A0530	Myla Sai Jahnavi	CSE	4	saicharanjahnavi@gmail.com	96
8						
9	18031A0537	Pillarisetti Madhumitha	CSE	4	madhumithapillarisetti@gmail.co	92
10						
11	18031A0526	Mulukutla Jyotsna Manasa	CSE	4	mjmanasa2015@gmail.com	96
12						
13	19035A0503	Guduru Sri Lakhsmi	CSE	4	srilakshmi11072001@gmail.com	90
14						
15	18031A0502	A Eswar Vinay Kumar	CSE	4	avalaesvar789@gmail.com	82
16						
17	18031A0509	Dharma Rao Marri	CSE	4	dharmamarri1729@gmail.com	63

Figure 29. Recording the attendance.

identification. The system's automation through a graphical user interface (GUI) streamlines processes, eliminating drawbacks associated with manual methods and enhancing overall efficiency. The user-friendly GUI encourages seamless integration into educational or organizational settings. Real-time attendance updates facilitate timely and accurate information, aiding in monitoring attendance patterns and addressing discrepancies promptly. Integration with an Excel sheet ensures structured and accessible record-keeping, simplifying administrative tasks. The system's adaptability makes it versatile for various environments, and customizable to meet the specific attendance tracking needs of different organizations. This trained model can identify students and mark attendance, achieving an accuracy of 92.23%.

CONCLUSION

An automatic attendance system will reduce the drawbacks of the traditional (manual) approach. This paper demonstrates the application of multimodal biometrics. Because unimodal biometrics are vulnerable to spoofing, multimodal biometrics provide a solution. The attendance system is the best application for multimodal recognition. The GUI acts as a conduit between the database and its users. Face images were captured using a webcam, and fingerprints were recorded using a Mantra Fingerprint Sensor (MFS100). If the extracted image matches the existing database images, the attendance system updates attendance in an Excel sheet otherwise, it ignores the image.

AUTHORSHIP CONTRIBUTIONS

J Samatha: Methodology, Writing original draft, Literature Review, Investigation, Conceptualization. G Madhavi: Review and Editing Supervision

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES

[1] Charity A, Okokpujie K, Etinosa NO. A bimodal biometric student attendance system. In: 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON); 2017 Nov; p. 464–471. IEEE. [CrossRef]

[2] Samatha J, Manjusha D, Pooja B, Usha A. Student placement chance prediction. J Emerg Technol Innov Res 2020;7:1011–1015.

[3] Juluri S, Sagar D, Reddy VP, Koundinya GS. Verification for online signature biometrics using deep learning. I-Manag J Comput Sci 2020;8.

[4] Memane R, Jadhav P, Patil J, Mathapati S, Pawar A. Attendance monitoring system using fingerprint authentication. In: 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA); 2022 Aug; p. 1–6. IEEE. [CrossRef]

[5] Demir I, Karaboğa HA. Modeling mathematics achievement with deep learning methods. Sigma J Eng Nat Sci 2021;39. [CrossRef]

[6] Selçuk ALP, Yiğit ÖE, Ersoy ÖZ. Prediction of BIST price indices: a comparative study between traditional and deep learning methods. Sigma J Eng Nat Sci 2020;38:1693–1704.

[7] Madhavi G, Samatha J. Secure data storage and access of data in cloud using elliptic curve cryptography. IEEE J 2020 May;11.

[8] Sarker DK, Hossain NI, Jamil IA. Design and implementation of smart attendance management system using multiple step authentication. In: 2016 International Workshop on Computational Intelligence (IWCI); 2016 Dec; p. 91–95. IEEE. [CrossRef]

[9] Gudavalli M, Raju SV, Babu AV, Kumar DS. Multimodal biometrics-sources, architecture and fusion techniques: an overview. In: 2012 International Symposium on Biometrics and Security Technologies; 2012 Mar; p. 27–34. IEEE. [CrossRef]

[10] Soewito B, Gaol FL, Simanjuntak E, Gunawan FE. Smart mobile attendance system using voice recognition and fingerprint on smartphone. In: 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA); 2016 Jul; p. 175–180. IEEE. [CrossRef]

[11] Ouch R, Garcia-Zapirain B, Yampolskiy R. Multimodal biometric systems: a systematic review. In: 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT); 2017 Dec; p. 439–444. IEEE. [CrossRef]

[12] Debnath S, Ramalakshmi K, Senbagavalli M. Multimodal authentication system based on audio-visual data: a review. In: 2022 International Conference for Advancement in Technology (ICONAT); 2022 Jan; p. 1–5. IEEE. [CrossRef]

[13] Siswanto ARS, Nugroho AS, Galinium M. Implementation of face recognition algorithm for biometrics-based time attendance system. In: 2014 International Conference on ICT for Smart Society (ICISS); 2014 Sep; p. 149–154. IEEE. [CrossRef]

[14] Ariffin SMZSZ, Jamil N, Kasinathan V. Image fusion for single-trait multimodal biometrics: a brief review. In: 2022 IEEE 20th Student Conference on Research and Development (SCOReD); 2022 Nov; p. 13–18. IEEE. [CrossRef]

[15] Sivakumar P, Rathnam BR, Divakar S, Teja MA, Prasad RR. A secure and compact multimodal biometric authentication scheme using deep hashing. In: 2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT); 2021 Nov; p. 27–31. IEEE. [CrossRef]

[16] Malathy EM, Sivamurugan V, Rajtilak S. Performance analysis and enhancement to biometric-based attendance system. In: 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP); 2020 Sep; p. 1–3. IEEE. [CrossRef]

[17] Nihan KAYA, Erdem F. Artificial neural network approach for lead removal from aqueous solution by agricultural waste-derived biochars. Sigma J Eng Nat Sci 2023;41:64–73. [CrossRef]

[18] Lu Y, Fu Y, Li J, Li X, Kong J. A multi-modal authentication method based on human face and palmprint. In: 2008 Second International Conference on Future Generation Communication and Networking; 2008 Dec; Vol. 2, p. 193–196. IEEE. [CrossRef]

[19] Patil P, Shinde S. Comparative analysis of facial recognition models using video for real-time attendance monitoring system. In: 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA); 2020 Nov; p. 850–855. IEEE. [CrossRef]

[20] Ramalingam M, Vinothkumar S, Varadhaganapathy S, Subha S. Multi-user authentication using biometric sensor using parallel processing algorithm for attendance monitoring. In: 2021 6th International Conference on Inventive Computation Technologies (ICICT); 2021 Jan; p. 84–89. IEEE. [CrossRef]

[21] Er BA, Şişman A, Ardali Y. Applicability of radial-based artificial neural networks (RBNN) on coliform calculation: a case study. Sigma J Eng Nat Sci 2022;40:724–731.

[22] Frischholz RW, Dieckmann U. BioID: a multimodal biometric identification system. Comput 2000;33:64–68. [CrossRef]

[23] Utomo SB, Hendradjaya B. Multifactor authentication on mobile secure attendance system. In: 2018 International Conference on ICT for Smart Society (ICISS); 2018 Oct; p. 1–5. IEEE. [CrossRef]

[24] Maheswari VU, Aluvalu R, Mudrakola S. An integrated number plate recognition system through images using threshold-based methods and KNN. In: 2022 International Conference on Decision Aid Sciences and Applications (DASA); 2022 Mar; p. 493–497. IEEE. [CrossRef]

[25] Gawande U, Golhar Y. Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques. Int J Biometrics 2018;10:142–175. [CrossRef]

[26] Khan MY, Ram SA. GPS-enabled employee registration and attendance tracking system. In: 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT); 2015 Dec; p. 62–65. IEEE. [CrossRef]

[27] Charity A, Okokpujie K, Etinosa NO. A bimodal biometric student attendance system. In: 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON); 2017 Nov; p. 464–471. IEEE. [CrossRef]

[28] Yadav A, Sharma A, Yadav SS. Attendance management system based on face recognition using Haar-cascade. In: 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE); 2022 Apr; p. 1972–1976. IEEE. [CrossRef]

[29] Wagh P, Thakare R, Chaudhari J, Patil S. Attendance system based on face recognition using eigenface and PCA algorithms. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT); 2015 Oct; p. 303–308. IEEE. [CrossRef]

[30] Bhat A, Rustagi S, Purwaha SR, Singhal S. Deep-learning based group-photo attendance system using one-shot learning. In: 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC); 2020 Jul; p. 546–551. IEEE. [CrossRef]

[31] Agarwal L, Mukim M, Sharma H, Bhandari A, Mishra A. Face recognition-based smart and robust attendance monitoring using deep CNN. In: 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom); 2021 Mar; p. 699–704. IEEE.

[32] Moura AF, Pereira SS, Moreira MW, Rodrigues JJ. Video monitoring system using facial recognition: a FaceNet-based approach. In: GLOBECOM 2020-2020 IEEE Global Communications Conference; 2020 Dec; p. 1–6. IEEE. [CrossRef]

[33] Sawhney S, Kacker K, Jain S, Singh SN, Garg R. Real-time smart attendance system using face recognition techniques. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence); 2019 Jan; p. 522–525. IEEE. [CrossRef]

[34] Singh S. A neural network-based attendance monitoring and database management system using fingerprint recognition and matching. In: 2019 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT); 2019 Jul; p. 1–7. IEEE. [CrossRef]

[35] Sivakumar P, Rathnam BR, Divakar S, Teja MA, Prasad RR. A secure and compact multimodal biometric authentication scheme using deep hashing. In: 2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT); 2021 Nov; p. 27–31. IEEE. [CrossRef]

[36] Garg V, Singhal A, Tiwari P. A study on transformation in technology-based biometrics attendance system: human resource management practice. In: 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence); 2018 Jan; p. 809–813. IEEE. [CrossRef]

[37] Dhanalakshmi N, Kumar SG, Sai YP. Aadhaar-based biometric attendance system using wireless fingerprint terminals. In: 2017 IEEE 7th International Advance Computing Conference (IACC); 2017 Jan; p. 651–655. IEEE. [CrossRef]

[38] Bouzouina Y, Hamami L. Multimodal biometric: iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM. In: 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART); 2017 Aug; p. 1–7. IEEE. [CrossRef]

[39] Al-Waisy AS, Qahwaji R, Ipson S, Al-Fahdawi S, Nagem TA. A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal Appl 2018;21:783–802. [CrossRef]

[40] Aronowitz H, Li M, Toledo-Ronen O, Harary S, Geva A, Ben-David S, et al. Multi-modal biometrics for mobile authentication. In: IEEE International Joint Conference on Biometrics; 2014 Sep; p. 1–8. IEEE. [CrossRef]

[41] Purohit H, Ajmera PK. Optimal feature level fusion for secured human authentication in multimodal biometric system. Mach Vis Appl 2021;32:1–12. [CrossRef]

[42] Tripathi S, Murgi J, Soni KRS, Singh R. A literature survey on multimodal biometric systems. J Comput Technol 2021;10:1–5.

[43] Jagadiswary D, Saraswady D. Biometric authentication using fused multimodal biometric. Procedia Comput Sci 2016;85:109–116. [CrossRef]

[44] Arya S, Agrawal A, Indore I. Face recognition with partial face recognition and convolutional neural network. Int J Adv Res Comput Eng Technol 2018;7:91–94.

[45] Waingankar A, Upadhyay A, Shah R, Pooniwala N, Kasambe P. Face recognition-based attendance management system using machine learning. Int Res J Eng Technol 2018;5:1979–1985.

[46] Sharma S, Shanmugasundaram K, Ramasamy SK. FAREC-CNN-based efficient face recognition technique using Dlib. In: 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT); 2016 May; p. 192–195. IEEE. [CrossRef]

[47] Tyagi S, Chawla B, Jain R, Srivastava S. Multimodal biometric system using deep learning based on face and finger vein fusion. J Intell Fuzzy Syst. 2022;42:943–955. [CrossRef]

[48] Akrouf S, Belayadi Y, Mostefai M, Chahir Y. A multi-modal recognition system using face and speech. Int J Comput Sci Issues 2011;8:1694–1814.

[49] Vishi K, Yayilgan SY. Multimodal biometric authentication using fingerprint and iris recognition in identity management. In: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2013 Oct; p. 334–341. IEEE. [CrossRef]

[50] Jing XY, Li S, Li WQ, Yao YF, Lan C, Lu JS, et al. Palmprint and face multi-modal biometric recognition based on SDA-GSVD and its kernelization. Sensors. 2015;15:5551–5571. [CrossRef]

[51] Leghari M, Memon S, Dhomeja LD, Jalbani AH, Chandio AA. Deep feature fusion of fingerprint and online signature for multimodal biometrics. Comput 2021;10:21. [CrossRef]

[52] Lowe DG. Distinctive image features from scale-invariant keypoints. Int J Comput Vis 2004;60:91–110. [CrossRef]

[53] Introduction to SIFT (Scale-Invariant Feature Transform) [Internet]. Medium; Available at: https://medium.com/data-breach/introduction-to-sift-scale-invariant-feature-transform-65d7f3a72d40 Accessed Feb 19, 2024.

[54] Geeganage J, Rathnayake K, Fernando V, Kumarasinghe P, De Silva SD, Wuttisittikulkij L, et al. Precise integrated contactless attendance tracking, recording and analyzing system. In: 2022 19th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON); 2022 May; p. 1–4. IEEE. [CrossRef]

[55] Nakagawa T, Nakanishi I, Itoh Y, Fukui Y. Multimodal biometrics authentication using online signature and voice pitch. In: 2006 International Symposium on Intelligent Signal Processing and Communications; 2005 Dec; p. 399–402. IEEE. [CrossRef]

[56] Kiran TA, Reddy NDK, Ninan AI, Krishnan P, Aravindhar DJ, Geetha A. PCA-based facial recognition for attendance system. In: 2020 International Conference on Smart Electronics and Communication (ICOSEC); 2020 Sep; p. 248–252. IEEE. [CrossRef]

[57] Wang J, Li Y, Ao X, Wang C, Zhou J. Multi-modal biometric authentication fusing iris and palmprint based on GMM. In: 2009 IEEE/SP 15th Workshop on Statistical Signal Processing; 2009 Aug; p. 349–352. IEEE. [CrossRef]

[58] Kumar A, Verma L, Singh T. Introduction to multimodal biometrics using OpenCV. In: 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE); 2022 Apr; p. 1505–1509. IEEE. [CrossRef]

[59] Devi R, Sujatha P. A study on biometric and multimodal biometric system modules, applications, techniques and challenges. In: 2017 Conference on Emerging Devices and Smart Systems (ICEDSS); 2017 Mar; p. 267–271. IEEE. [CrossRef]

[60] Zhang H, Huang Z, Li Y. An overview of multimodal biometrics based on face and ear. In: 2009 IEEE International Conference on Automation and Logistics; 2009 Aug; p. 1705–1709. IEEE. [CrossRef]

[61] Middendorff C, Bowyer KW, Yan P. Multi-modal biometrics involving the human ear. In: 2007 IEEE Conference on Computer Vision and Pattern Recognition; 2007 Jun; p. 1–2. IEEE. [CrossRef]

[62] Kamelia L, Hamidi EAD, Darmalaksana W, Nugraha A. Real-time online attendance system based on fingerprint and GPS in the smartphone. In: 2018 4th International Conference on Wireless and Telematics (ICWT); 2018 Jul; p. 1–4. IEEE. [CrossRef]

[63] Cihan M, Uzbaş B, Ceylan M. Fusion and CNN-based classification of liver focal lesions using magnetic resonance imaging phases. Sigma J Eng Nat Sci 2023;41:135–145. [CrossRef]