EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Facial Recognition Enabled Smart Security Lock System Using Machine Learning Approach

M. Marimuthu[1,*], G. Mohanraj[2], J. Akilandeswari[3] and V. Sathiyapriya[4]

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
[2]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
[3]Department of Information Technology, Sona College of Technology, Salem, India
[4]Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem, India

Abstract

INTRODUCTION: In today's modern world of networking and intelligent devices, there is an imperative need to upgrade everyday things and make them intelligent; additionally, this is not the era to unquestioningly trust old and traditional security measures, particularly when it comes to smart door lock systems. Mostly, every smart door lock system has a security access code or fingerprint access outside the door that makes it vulnerable. The password in a classic security system can be readily hacked with advanced technology and, therefore, is no longer suitable for today's real-time environment.
OBJECTIVES: As a result, this paper intends to provide enhanced security for the user through facial recognition using a machine-learning approach with high accuracy and remote access via an Android application. Automated solutions leveraging machine learning have shown to be quite effective in security.
METHODS: Machine Learning (ML) algorithms are used to train different sets of images to identify and classify various sorts of faces. The specific algorithm that is to be used is Dlib and Support Vector Machine (SVM); Dlib is utilized for face recognition along with HOG (Histogram of Oriented Gradients), whereas SVM is used for image classification, which is used to authorize the personnel.
RESULTS: When compared to other cutting-edge methodologies, empirical results reveal that the proposed approach achieves 96% accuracy rate, with a recognition speed of 0.5 seconds per face in facia recognition which is more effective, reliable, and utilizes fewer resources.
CONCLUSION: Real-time face recognition enables quick and secure identification, supporting multi-factor authentication and monitoring. The proposed smart lock system uses the HOG+SVM approach, achieving higher accuracy and faster face detection.

Keywords: Face recognition, Dlib, SVM algorithm, OpenCV, Raspberry Pi

Received on 05 April 2024, accepted on 29 March 2025, published on 05 June 2025

doi: 10.4108/eetiot.5657

1. Introduction

Automation has become increasingly relevant in human life as a result of the advancement of digital technology and Android applications; people's lives are gradually changing with smart living. The need for authentication, privacy and security is growing and becoming a significant issue as people's needs grow smarter day by day [1]. Any object can be changed and modernized by eliminating its current flaws and adding additional functionality. Face detection is more complicated because specific characteristics, such as glasses and moustaches, are inherently unstable and have an impact on detection effectiveness [2]. Furthermore, various styles and angles of lighting can cause unusual facial brightness when detecting faces, which will affect the detection process [3].

*Corresponding author. Email: marimuthu.m@vit.ac.in

An in-depth examination of the OpenCV platform and its built-in libraries, such as Dlib, has been performed in order to generate code that correctly and efficiently performs facial recognition by leveraging modern and practical hardware. By using facial recognition for the home environment, this proposed system also helps as a home security system for person identification as well as door access control [4]. The human body is recognized as an intruder in a home environment captured by recorded footage from a web camera, and the captured video frames will be examined. As soon as the person presses the switch, the web camera captures a sequence of images. The benefit of this door access method is that the identification and recognition of the face is carried out using a facial detection technique by pressing a single and little push button switch [5].

Although the smart facial-recognition based security system provides fool-proof access system, it might face security breaches with printed pictures and recorded video of authorized users. To fight against these kinds of attacks the security has to be hardened through voice assisted face recognition system. This system directs user to respond as per the instruction given pre-recorder audio. Such type of approach prevents unauthorized users from misusing the locking system [6]. The best possible solution is to use a 3D and 3D-color Infrared Camera based face recognition system which has the capacity to scan both audio and video related images with multiple alarm functions.

The security is main problem, with respect to data, human life and asset security. Smart-locking based android application system were implemented with biometric and IoT devices can optimize the security features drastically. The system executes on-spot face recognition and detection using Bluetooth. Mostly, the main security concern in this system is about security flaws in android application and due to security concerns in the Bluetooth connection. A prototype has to be developed properly and tested, in case if configuration is not properly implemented it may affect system's working, efficiency, and reliability. The results show that it can be efficiently used to enhance human life and security and for commercial and residential purposes [7].

The maximum recognition of the face is achieved through facial image, identification or classification and feature reduction. People are becoming increasingly concerned about the protection of their property, knowledge, and themselves as the world progresses. Smart biometric door locks are the instrument that supports home protection, as only the person who has been pre-identified can access them. There's an open invitation to robberies and losses in the absence of such keys [8]. The Smart Door concept is expected to have a significant impact on the security industry, and it is eagerly anticipated because the time will come to integrate all aspects of everyday life. This model would be instrumental in the field of home security in a real-time environment. The significant contributions of this work are as follows:

- An automated Smart Home Security System has been developed based on Face Recognition and Machine Learning algorithms.
- Using the HOG+SVM approach, the authentication person images are validated.

The remaining section of the paper is organized as follows: Section 2 discusses the overall view of relevant work on the face detection framework model. The proposed smart lock system model is outlined in Section 3, and Section 4 demonstrates the implementation of the system. Section 5 discusses the results that are compared with face detection parameters. The conclusion and future research works are addressed in Section 6.

2. Related Works

In this work [9], a structure composed of three parts. The very first segment is a face detection process that is built on the Hair-like characteristics detection process and the recognition Local Binary Pattern (LBP) algorithm. The second segment is the security encryption scheme. The last segment is the GSM warning system. This platform consists of a combination of a face-recognition detection system, a password protection system and a GSM warning system. Using the Local Binary Pattern (LBP) algorithm, this method eliminates the duplication used in facial recognition systems. Conducted research on home surveillance systems with email-based cameras [10]. The study resulted in a system that could recognize a person based on their skin and face. Since the system still needs the homeowner's authorization through email, it is considered less reliable and productive. For face recognition, the machine incorporates a histogram. The use of a histogram as a feature is considered to be inaccurate.

Explore facial detection through biometric authentication, addressing several concerns, such as the complicated process and the long-term viability of the results [11]. This paper proposes methods for a quicker facial recognition process that provides accurate results. To solve these problems, multiple face detection and processing techniques are being used to process more than 60 images at once and achieve accurate results. With multiple face detection, the results show that this facial recognition technique is more than 90% accurate. Author researched fingerprint-based door-locking systems [12]. Since the user should position a finger on the sensor, fingerprint-based security systems are considered to be less effective. It's also thought to be a factor throughout the virus's spread. Fingerprint systems may also be duplicated, resulting in a low-security rating. Due to the wetness of our fingerprints, the machine can sometimes fail to read our fingerprints. As a result, biometrics has been replaced by a facial recognition security system.

Another research was done on face recognition using the principal component analysis method (PCA) [13], which resulted in a system that can identify faces with different poses and orientations. The research intends to use a simulation with a face database. Face recognition methods should be chosen based on performance, time constraints, processing speed, and availability. PCA is a technique for reducing data dimensionality by choosing the most relevant features that collect the most details about the dataset. Face recognition using PCA is chosen based on these criteria

because it is the simplest and easiest solution to implement, with a very short computation time. Face detection and recognition systems based on SVM algorithms are developed and implemented in this research. The concept is being considered for use in a smart home security system.

Conducted face recognition research using the Dlib and Opencv libraries. For the IoT platform, OpenCV is a better option for developing face recognition applications [14]. It is more effective and has enhanced face recognition functionality. It means that developing recognition applications for the IoT Platform is easier with OpenCV. When looking for other algorithms, such as the Haar cascade, the HoG algorithm was investigated; it takes longer to run but provides more accurate results. If there will be a lot of pictures in the future for many people, this approach should be considered. Face recognition, which is implemented in real-time, assists in the recognition of human faces and can be used to identify and authenticate people. Support vector machine classifiers, which are capable of accurately classifying various types of faces, are used to implement face detection. Face recognition accuracy can be enhanced by the number of images used during training [15].

Research on facial recognition for identifying authorized and unauthorized users. In this case, the device's performance and accuracy are primarily determined by the core processor, and the face recognition process is more accurate [16]. The Raspberry Pi used in the system lacks sufficient memory and processing speed to measure the image file, which is a system limitation. Another paper describes how to use an Android application to provide authentication over the internet [17]. There are a number of commercial smart door lock security systems available in the market. Its purpose is to design an Android security lock system that would be both virtual and practical to use. When compared to previous systems, Wi-Fi technology-capable solutions have proven to be operated remotely and provide home protection. As a result, the system can be monitored in and around the house.

On the front end of the setup, a smart door, they were using a live HD camera mounted to a monitor screen connected to the camera to identify who was standing in front of the computer, and then the entire system would be able to provide speech outcomes by processing text on the Raspberry Pi Embedded system used and displaying the responses as feedback on the monitor [18]. Microsoft Face API achieves facial recognition; however, the desktop software Microsoft Visual Studio (IDE) reduces processing time by detecting the face in a photograph and submitting the result to Microsoft Face API, which is handled by Microsoft Azure cloud support.

Home automation based on Android, in comparison to other smart door lock systems Nagendra Reddy et al. [19], allows the device to be more versatile and offers an appealing user interface [20]. When completed with Raspberry Pi automation, the machine can be operated from anywhere in the world. They explain how they designed and developed a remote door lock control system using a Raspberry Pi and an Android application in this paper. The Adaboost algorithm detects faces. In contrast to traditional approaches, improved AdaBoost with the colour of skin detection algorithm achieves more reliable efficiency and faster speeds. To decide whether or not an image is a face, AdaBoost learning is used to select a small number of weak classifiers and combine them into a robust classifier. Then, by comparing the critical components of the actual face to those of recognized individuals in a pre-constructed facial database, a specific face can be identified using the principal component analysis (PCA) algorithm.

The author proposed [21] a facial detection and recognition system using Image manipulation and Machine Learning (ML) techniques [22]. Based on the face image that has been detected, the system will make decisions based on the pattern of images learned through the facial recognition process. Through this inference decision will be taken to open the door or not. Home security-based application to send frequent notifications to the house owners if any unknown person tries to unlock the door. A home security system for face-recognizing and identifying the person's authenticity to enter into the home [23]. A deep learning model has been implemented to learn patterns, and it makes the system more robust in detecting intruders more accurately [24]. CNN is the implemented model which shows excellent progress in facial recognition and facial detection systems. It shows that accuracy has crossed more than 90% with an increase in the number of images to get processed. In the future, data from IOT device such as Raspberry Pi will be used to collect some real-time data sets, which might increase system accuracy much more and provides more safety features.

An IoT-based smart protection framework that uses computer vision techniques for facial recognition and detection [25]. Lots of sensors have been used to track intruders and notify the house owners if anything happens with respect to security breaches. The proposed system is further enhanced by using image processing techniques. If the image of the person is not recognized for 20 seconds, then this information will notify the house owner. If anybody tries to break into the house, then the alarm will activate, and an alert message will be sent to the police department.

A Deep-learning model for facial recognition and evaluation. Almost all smart devices are connected to a network [26]; these connected devices will produce massive volumes of data. In order to gain knowledge from such data, Machine Learning (ML), Deep Learning (DL) and Edge computing (EC) techniques have been used. CNN is the deep learning model which replaces the traditional facial recognition models. The face recognition system gives greater accuracy with this deep learning model. To test its accuracy, it has been implemented in the smart classroom for taking students' attendance. It shows more than 95% accuracy in detecting the student's face in various orientations. Suggested an extensible web crawler service based on a cloud computing environment to identify, extract, and recognize photos for facial detection and recognition [27]. Web page images are utilized to evaluate information for a search strategy in this detection process. Principal component analysis is used to improve the proposed system's character recognition and dimensionality reduction. In addition, the K-Nearest Neighbor's method is used to select pictures from a web page that are strongly linked.

Proposed a biometric recognition retrieval system based on multi-sample facial photos and multi-instance fingerprints for recognizing and verifying a user's validity [28]. An adaptive deep learning network with vector quantization was utilized to obtain texture patterns with variance. The system used a vector quantization based on K-mean to address memory and overfitting concerns. With these classifications and feature-extracting approaches, the expectancy maximization methodology is adopted to predict incomplete information. It will also make it easier for users to retrieve the information while still protecting them from spoofing attempts. Differing amounts of face image data based on both thermal and video photographs will be employed in the future for face biometric identification. To overcome the weaknesses of the adaptable deep learning vector quantization classifier [29], suggested a combination adaptive deep learning vector quantization classifier. The use of a multi-sample face image with different sequences and attributes further reinforces this idea. Various criteria are used to determine the correctness of the proposed and current models. In addition, the trend retrieval strategy is employed to forecast incomplete information using an expectancy maximization technique. This would safeguard from spoofing attacks in the future by identifying false facial photographs.

Investigate how the gender balance in the training data impacts the accuracy of face recognition [30]. Female face information is underrepresented in both the training and test datasets, resulting in lower accuracy in detecting and recognizing female faces. To investigate this issue, three separate datasets with variable female and male face picture proportions were chosen to train a conventional CNN deep learning model. Three distinct loss functions are used to assess the correctness of the model. Examine how gender classification methods function varies in various genders. Toward this purpose, researchers look into the influence of structural variations in learning algorithms and training set unbalance as a possible cause of discrimination that causes efficiency disparities between gender and race. UTKFace and FairFace, two of the most recent large-scale publicly released facial feature sets, are used in the experiments [31].

A deep learning-based classification method is used to evaluate training and test data. Investigate whether ocular-based authentication and gender classification are perfectly fair for males and females. The VISOB 2:0 data is used to investigate if ocular biometrics techniques based on ResNet-50, MobileNet-V2, and lightCNN-29 models are equal. According to the findings, male facial gender classification is considerably superior to female face gender classification based on the ocular biometrics procedure [32]. This research will be expanded in the future to include ocular biometrics acquired from visible and infrared spectral face photographs of people of all genders, ages, and races.

A novel transportation mode detection (TMD) model that combines a spatial attention-based transudative long short-term memory (TLSTM) network with an off-policy proximal policy optimization (PPO) algorithm for improved feature selection [33]. This approach overcomes the limitations of traditional LSTM models and manual feature extraction, enhancing the detection of subtle temporal shifts and complex patterns in time-series data. The model achieves high F-measure scores—92.323% for the Sussex Huawei locomotion (SHL) dataset, 91.151% for the HTC dataset, and 91.352% for the United States-TMD (US-TMD) dataset. Additionally, the integration of the artificial bee colony (ABC) algorithm for hyperparameter optimization improves model efficiency.

This study [34] introduced a lightweight intermediate fusion network using manifold learning for dimensionality reduction. It demonstrated that incorporating manifold learning significantly reduced errors by 41.69% compared to Principal Component Analysis (PCA) in intermediate-level fusion networks. The research evaluated six manifold learning methods, with the MDS method achieving 96% accuracy in stress detection. The study also highlighted the benefits of data balancing through down-sampling, which improved performance by reducing computation time and ensuring unbiased results. Additionally, adding an extra 1D-CNN layer boosted accuracy by 7.41%, precision by 6.18%, recall by 9.23%, and the F1-score by 9.42%. These results emphasize the importance of manifold learning, data balancing, and architectural improvements in enhancing stress detection systems.

[35] emphasizes the critical importance of security and privacy in electronic health record (EHR) sharing systems. It proposes a solution that uses blockchain's decentralized structure to remove reliance on third parties, along with searchable encryption to enable secure data searches by network miners. It addresses concerns about the privacy risks of storing sensitive health data in cloud systems controlled by a single entity. The proposed protocol combines blockchain technology with cryptographic methods like ring signatures and searchable encryption to protect privacy and enhance access control, eliminating the need for a trusted third party.

It addresses the challenges of Automated Facial Expression Recognition (FER), particularly with compound expressions that involve multiple emotions. Current FER datasets use hard-labels, assigning a single emotion to each expression [36]. To improve recognition accuracy and reduce intra- and inter-class challenges, the paper proposes using soft-labels, where facial expressions are labeled with multiple emotions at varying confidence levels. The authors introduce AffectNet+, a new dataset that includes soft-labels, three complexity subsets, and additional metadata (e.g., age, gender, ethnicity). AffectNet+ aims to support more realistic emotion recognition, enable multi-labeling, reduce bias, and improve decision boundaries. The dataset will be publicly available for future research, especially in areas like soft-label prediction, noise reduction, and generalization [37].

The following Table 1. summarizes the relevant works that are currently available in the literature.

Table 1. Summarization of Related Works

S.No	Author & Year	Face Recognition Techniques Used	Observation
1	Soe Sandar et.al. 2019	Face recognition system (LBP+GSM)	Using the Local Binary Pattern (LBP) algorithm eliminates the iteration used in facial recognition. It also has a GSM alert system and password protection.
2	Pooshkar Rajiv et.al. 2016	Home Security Systems with Email-Based Cameras	Less effective Email Authorization and poor system accuracy due to histogram features.
3	T.Mantoro et.al., 2018	Multi-Faces Recognition (Haar Cascades + Eigenface methods) Process	Facial Recognition is addressed by biometric authentication, but it has limited accuracy because of its lengthy process.
4	A.AdityaShankar et.al. 2015	Fingerprint Security Systems (Biometrics+Authentication)	Fingerprint-based security systems are considered to be less successful and can also be duplicated in such a way that they are rated as having low security. So, the fingerprint is replaced by a security system of face recognition.
5	Liton Chandra Paul et.al. 2012	(Principal Component Analysis Method + Eigenvalue Approach) Face Recognition	Reducing the recognition of face during authentication.
6	K. M. Rajesh et.al. 2016	Face recognition and emotion detection system using (SVM)	Face recognition is implemented using support vector machine classifiers that can correctly classify a variety of faces. In order to store and process huge amounts of facial orientation data sets, facial image storage is required.
7	Karan Maheshwari et.al. 2017	Facial Recognition Using Microsoft Face API	In addition to making the device more friendly and effective for consumers, a Chabot should be deployed. High security-based protocols can be introduced to address security risks. Offline data storage is needed to solve the problem of power shortage.
8	H. Bharathi et.al. 2017	Home Automation By Using Raspberry Pi And Android Application	Raspberry Pi used in the device does not have the memory space or processing speed to measure the image file, which is a drawback of this method. It is essential to protect our home from all threats. A cloud-based service is needed for this.
9	Karan Maheshwari et. al. 2017	Smart Locking System (Raspberry Pi + Microsoft Face API)	Microsoft Face API achieves facial recognition, but the Microsoft Visual Studio IDE desktop program decreases processing time by identifying the face from the image and submitting this result to the Microsoft Face API.
10	M. Nandhini et. al. 2020	Smart Security System (IOT) based (Raspberry Pi + OpenCV)	DeepFace Model has been trained with SVM to learn probabilities of facial image matching. It processes a large number of image frames in a second compared to other existing models. This approach improves intruders' facial detection rate.
11	A. Krishnan et al. 2020	VGGFACE Gender Classification Algorithms Across Gender-Race Groups	In terms of influencing structural changes in algorithms and training sets, the VGGFACE approach becomes less successful. Such imbalance could be a source of bias, resulting in performance gaps among men and women.
12	V. Albiero et al. 2020	Multi-Faces Recognition (Conventional CNN model)	Female face information is underrepresented in both the training and test datasets, resulting in lower accuracy in detecting and recognizing female faces.
13	M. E. El Araby and M. Y. Shams, 2021	Face retrieval system (elastic web crawler over cloud computing + KNN Classifier)	Web page images are utilized to evaluate information for a search strategy in this detection process. Principal component analysis is used to improve the proposed system's character recognition and dimensionality reduction.
14	Proposed smart lock system model	HOG+SVM approach	Faces are easily identified because of HOG+SVM, and the face has taken less time to detect. Facial characteristics are extracted from HOG+DLib so that the authenticated person's image can be checked immediately and authentication performed locally and remotely. Images are obtained automatically using the object detection method (CasecadeClassifier).

From the above Table 1, it is understood that home security is becoming one of the important things that both the society and the smart home systems need to remember. The major disadvantage of traditional home security systems currently in use is a security with a password at the doorstep that uses radio waves transmitted between doors and windows to control panels but also can be easily broken using modern technologies such as intercepting data and deciphering commands. Such signals may also be jammed to prevent them from setting off an alarm by transmitting radio noise to the control panel, which prevents the signal from moving through the sensors.

In the current scenario of the modern world, everything is fitted with advanced technology and the internet to make human work more straightforward and more effective. However, the current system lacks it; the main security issues that our system addresses are:

- A high-level safety system requires a lot of maintenance and expense.
- Because of its complexity, many homeowners are unaware of their security system and how it functions.
- Lack of remote access to the security system.
- Training is time-consuming and is not robust.

To overcome the above security issues, a smart lock system based on the HOG+SVM approach was presented. The proposed model is implemented and explained in detail in the following sections.

3. Solution Approach

In the emerging technology environment, security has become an imperative problem statement. Theft of information, lack of protection, and privacy breaches, among other things, are the essential components that must be secured. This system provides security features for facial recognition, as well as a keypad for entering the passcode to unlock the door. To begin with, if the system predominantly relies on a facial recognition module, there is a chance that the face cannot be detected at times, stopping the door from being unlocked. Second, if the system uses a keypad to enter the passcode to unlock the door, there's a chance the key might be observed or detected by others without the user's permission. As a result, two-step verification is generated, with facial recognition as the first step and a passcode as the second. The new advanced system, however, has the same issues. Hence, a proposed model is being developed those addresses all of the existing problems.

The proposed smart lock system uses a Raspberry Pi3-connected web camera for face recognition and a solenoid lock attached to it for door opening and closing. The system is designed to get more accuracy and productivity on the basis of Machine Learning. Initially, the authorized person's image is captured at different angles and stored in the database. Feature extraction is done through the DLib algorithm, which detects facial landmarks as a subset of shape prediction problems. The images are now converted to vector form which then is given into the Support Vector Machine (SVM) classification algorithm. The training of images through SVM and feature extraction through Dlib is stored as a pickle file for authentication. Figure 1. depicts the entire framework model for the smart lock system. The implementation of the proposed framework model can be explained in the following section.

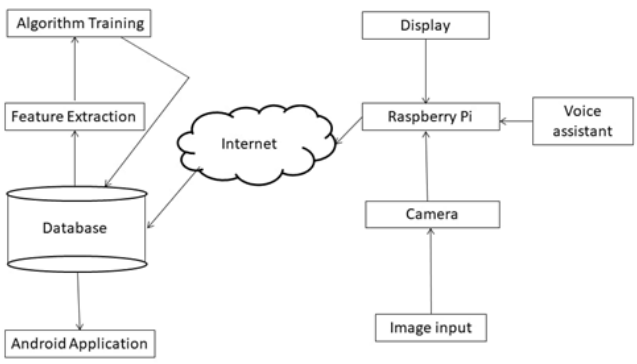

Figure 1. Framework model for the smart lock system

4. System Implementation

4.1 Data Collection

The dataset of each person is collected through the camera connected to Raspberry Pi3 and stored in the database. The image of the person is detected from the video frame, and HoG or Histogram of Oriented Gradients Classifiers detects the face. The image of the person is captured using a webcam, and Cascade Classifier is used to detect 2000 face samples automatically. The detected face is cropped and stored in the database which is shown in Table 2. In Figure 2., data collection is depicted below, and the face samples as shown in Figure 3. These descriptors can be implemented by dividing the image into small connected areas called cells and compiling a histogram of gradient directions or edge orientations for the pixels inside each cell. The sum of these histograms measures the descriptor. For better accuracy, local histograms can be contrast-normalized by measuring the intensity value over a wider region of the image, known as a block, and then using that value to normalize all cells within that block. As a consequence of the normalization, there is more invariance for changes in lighting or shadowing.

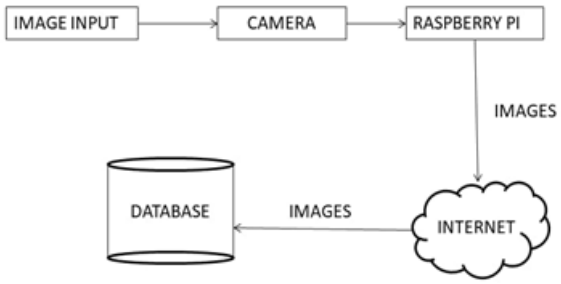

Figure 2. Dataset Collections and Storage in Database

Figure 3. Face Samples for an individual person

Table 2. Features of Dataset

Type	Size	Diversity
Face Recognition Dataset – Kaggle	2000	Only Face and Full-Size images

4.2. Feature Extraction

The images in the database are converted to vector form by extracting the essential features by the facial landmarks through DLib. Figure 4. shows the flow of feature extraction and conversion of images into vectors. The vectorized images are labelled and stored in the database. The issue of shape prediction includes the recognition of facial landmarks as a subset. Given an image as input, a shape predictor attempts to find essential points of interest along the shape (usually an ROI that specifies the object of interest). Facial landmarks aim to predict important facial structures on the face using shape-prediction methods.

Figure 4. Feature extraction from Image dataset

As a result, detecting facial landmarks is a two-step process:
Step #1: Determine the location of the face in the image.
Step #2: On the ROI face, detect the main facial structures.

Face recognition (Step 1) can be achieved in a number of ways. They can take advantage of OpenCV's built-in hair cascades. For facial detection, they can use a pre-trained HOG + SVM Classifier object detection system or might also use Deep Learning (DL) algorithms to pinpoint the image's location. It makes absolutely no difference which algorithm is being used to classify the face in the picture in this scenario. Instead, might obtain the bounding box of the face, i.e., the (x, y) coordinates of the facial image via some process. Step # 2: Identify critical facial structures throughout the face region that can then be applied. There seem to be a number of facial landmark detectors available, but they all aim to locate and recognize the following facial regions:

- Right eye
- Left eye
- Right eyebrow
- Left eyebrow
- Nose
- Mouth
- Jaw

Figure 5. Facial Landmarks detected through Dlib

The first step in this approach is to use a training dataset of facial landmarks on the image. The different (x, y)-coordinates of the regions surrounding each facial structure are manually labelled on such images. A collection of regression trees is trained using these training results to predict facial landmark positions directly from the pixel intensities themselves (i.e. no "feature extraction" is taking place). The outcome is a facial landmark detector that can be used to detect facial landmarks in real-time and with high-quality predictions refer to Figure 5. through Dlib.

4.3 Model Training Using SVM

The vectorized images are given as input to the SVM (Support Vector Machine) algorithm (Figure 6. shows the flow of model training). The model is trained with SVM due to the following advantages:

- Highly effective even if the dimensionality is more
- Efficient even if the number of dimensions is greater than the number of sample spaces
- Robust algorithm, which is also memory efficient

Among the most helpful classification problem techniques is Support Vector Machines (SVM). One primary example is face recognition. When the function vectors representing the samples have missing entries, however, SVM cannot be used. The well-known Support Vector Machines (SVM) classification algorithm was successfully used in this scenario, and it can be applied to the actual presence space or subspace extracted after a feature extraction procedure. SVM classifiers have an advantage over conventional neural networks in that they can perform better in generalization.
The algorithm gives the best approximation of an unknown person's identity from the qualified model of identified or permitted individuals. The algorithm is given an image of individuals in authentication, and the algorithm asserts whether the person is allowed or not. It also provides a measure of trust about the claim's validity.

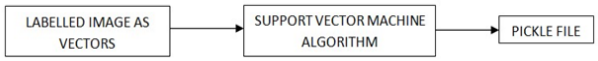

Figure 6. Model Training using SVM Algorithm

4.4 Authentication of Visitors

When a person enters the premises, the camera captures the image, which then is converted to a vector and given to the algorithm trained and stored as a pickle file in the database. The algorithm predicts whether the person is a known person or an unknown person. Suppose the individual is predicted to be a known person (i.e., the person who is already enrolled in the system). In that case, the next step of verification is carried out by the use of passcode security or binary lock pattern. If the person is unknown (i.e., the person who is not enrolled in the system), the image of the person is recorded and placed in the database.

The stored image is sent to the owner/admin of the premises through an Android application, from which the owner/admin can authenticate or de-authenticate the unknown person from entering the premises. In case of detecting an unknown individual, automated questionnaires are asked of the person through smart devices like Alexa or Google Assistant connected to the Raspberry Pi3. The reply is sent back to the admin via the Android application. The admin can decide whether or not to allow the person with the help of an unknown person's image and the person's reply to the questionnaires. In case of any suspicion, the system is automated to call the nearby police station through the GSM module. Figure 7. depicts the flow of the authentications of visitors at the doorstep.

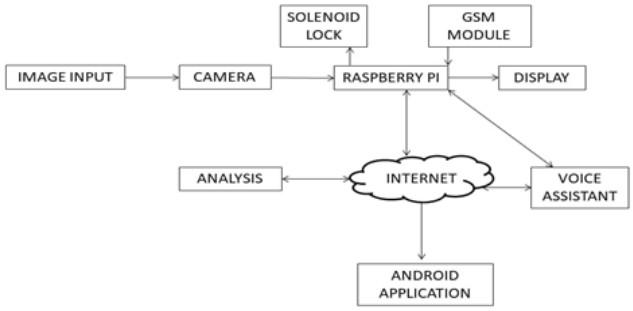

Figure 7. Authentications of Visitors

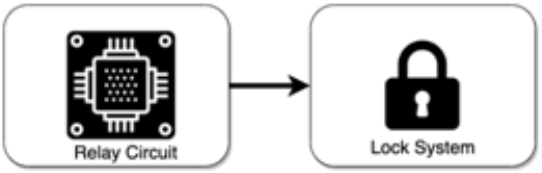

Figure 8. Application of Door lock Circuitry

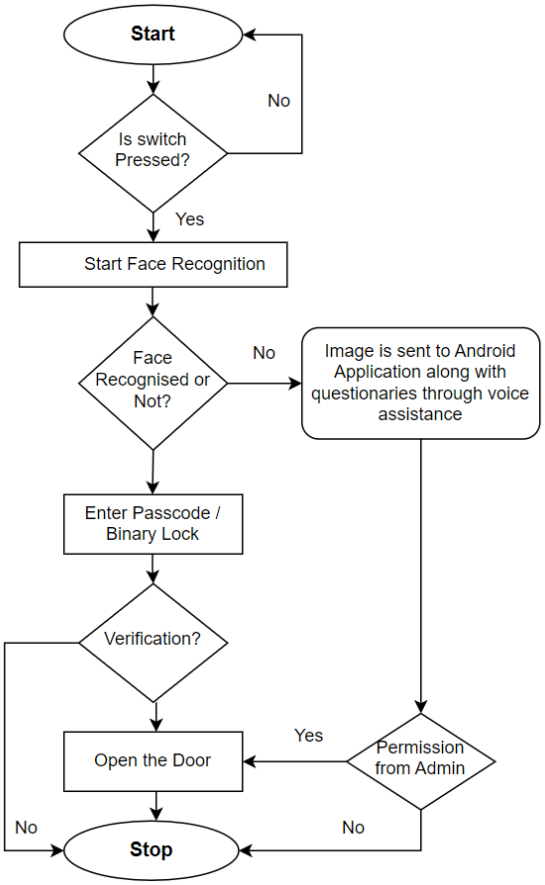

Figure. 9 Working Procedure of the smart lock system

4.5 Application of Door Lock Circuitry

Based on the test results shown in Figure 8. an application-specific system consisting of a Locking Mechanism (Door Lock) Circuitry is linked to the Locking Mechanism Authentication Module and continues to perform Face Recognition-based Open or Close Door Lock operations.

4.6 Working of the Smart Door Lock

Figure 9. depicts the procedural view person detection process and authentication of a person into the premises by the application module. The application starts when the person at the door presses the switch, which then calls the code to be implemented. The pi camera captures the image through face detection by HoG. The image is converted to a vector and given to the SVM algorithm, which is a classification algorithm that finds whether the image detected (converted into a feature map) is authenticated or not. If the image is a match, then passcode verification or binary lock pattern verification takes place. If the verification is true, the door lock circuitry is given a signal to open the door the door remains closed. If the image is not a match, then the person's image is sent to the Android application through the cloud for verification by the admin to give access to the person entering the premises. After unlocking the door, the FTP sends an alert to authorized personnel. The log of persons entering the premises is stored in the database along with the image of the person that can be viewed as and when needed through the Android application.

4.7 Algorithm for the smart lock system

The entire implementation of the proposed system is given as a single step-by-step pseudocode given below. The system implementation starts with the dataset collection (i.e., capturing images of the authenticated persons) and storing them in the database. The SVM algorithm does model training on the dataset.

Algorithm
BEGIN
Capture Image Dataset of the Authenticate Persons
Store the images in the Database
Extract Facial Features from images using HoG and DLib
Split Dataset into train and test
Train the model with SVM algorithm
    TESTING BEGINS
    Read Image through the camera using cv2
    Load the model created
    Let the model predict the person detected
    if (Model predicts Known Person)
        Enter Passcode
        if (Correct Passcode)
        Door opens and the person can enter
        else
        User unauthorized Door remains closed
        goto STEP 1
    else (Model predicts Unknown Person)
    Save person's image in the Database
    User Unauthorized and the Door Remains Closed
    END
END

5. Result and Discussion

This section discusses the outcomes of the proposed smart lock system. When a person enters the premises and presses the button, the system starts face recognition to determine whether the person is known or unknown. The system prompts you to enter the passcode since the person is predicted to be a known person. After entering the passcode, it is compared to the database passcode. The user's passcode entry is validated, and they are authorized access to the premises.

Figure 10. Passcode Entry

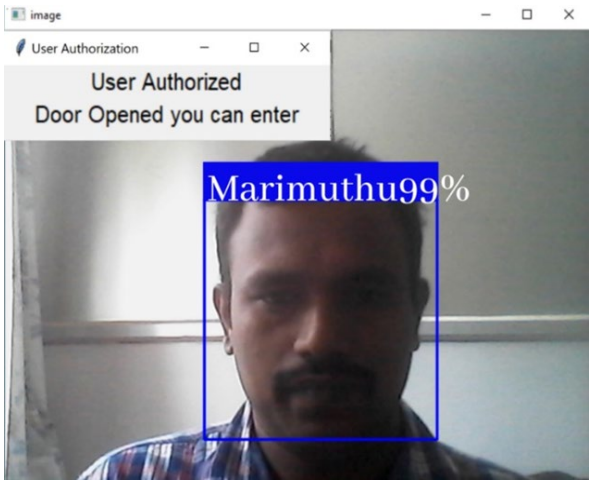

Figure 11. User Authorized

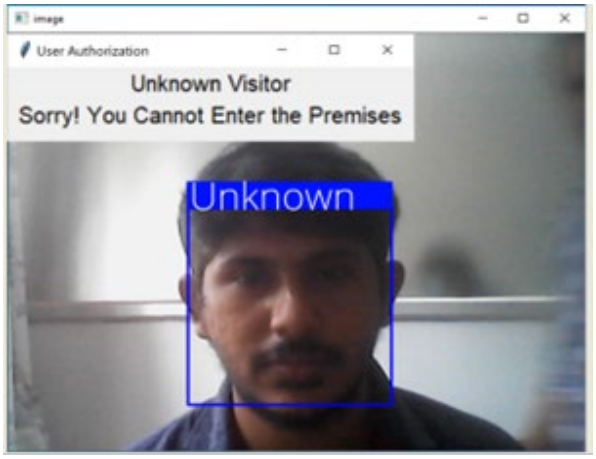

Figure 12. Unknown User

The door is opened by a solenoid lock that is linked to the smart lock system. When an unknown user enters the premises, the system detects it, and the user is not allowed to enter the premises, so the door remains closed for the entry of the person. The Android application sends the picture of the unknown person to the admin. The following Figure 10. passcode entry, Figure 11. user authorized and Figure 12. unknown user depicts the proposed smart lock system results, which is described above.

The results obtained show that the HOG+SVM approach is more robust and precise than that of the LBP and Haar Cascades approach, while the accuracy is higher for CNN compared to SVM but is negligible in the case of face recognition systems. SVM stands at its best based on time complexity so the proposed system takes only less time compared to other algorithms as SVM is robust. The time complexity of HOG+SVM and CNN is shown in Figure 13, depicting that HOG+SVM is more robust than CNN. Having a robust algorithm for training and testing makes it more feasible for applicative purposes; thus, it is straightforward to add a new member for authentication, even though an Android application with the automation code to capture faces at different postures. Capturing images of a person at different postures has the advantage of recognizing the person at different poses or angles during authentication at the doorstep.

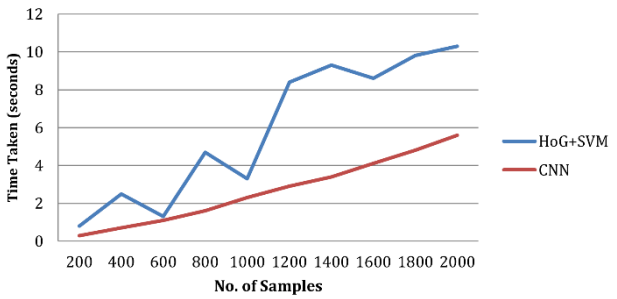

Figure 13. HOG+SVM vs CNN Based on Time for Training

Two thousand samples of images for a single class are used to train the algorithm, and for testing the algorithm, images captured from the webcam are used. The facial features are extracted using Dlib, and the experimental results show that different persons can be identified. The Accuracy Under the Curve for the proposed system is shown in Figure 14. The Accuracy obtained is 96%, which leads to overfitting of the data. So, making further changes in the hyperparameter tuning of the SVM algorithm gives better results.

From the experimental analysis of SVM and CNN, it is found that SVM has good accuracy compared to CNN in the case of detection, whereas CNN has the best accuracy than SVM in the case of classification, which is represented in Figure 15. Table 3 presents the comparison of the proposed methodology with the other existing models with respect to the accuracy and number of samples. It is clear that our proposed methodology has higher accuracy when compared to other models. But the accuracy rates do not vary abruptly, so SVM is used in the proposed system as it is more robust compared to CNN; also SVM requires only low computational facilities, on the other hand, CNN requires more computational power.

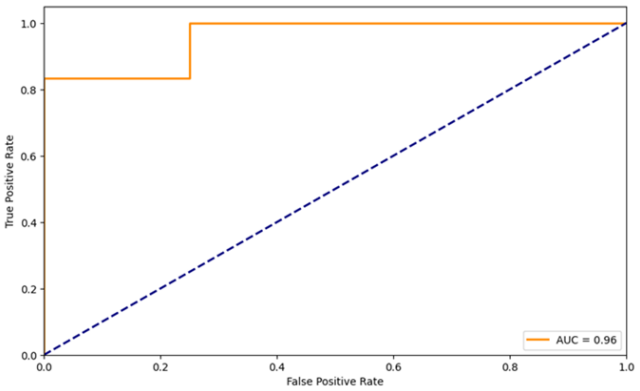

Figure 14. Accuracy Under Curve (AUC) for the proposed System

Many experiments are conducted in order to evaluate the performance of the proposed method of face detection and recognition, and the results are summarized as follows. The face detection algorithm based on template matching is tested at various distances from the person to the camera. When the range is less than or equivalent to 240 centimeters, the face position in an image can still be identified.

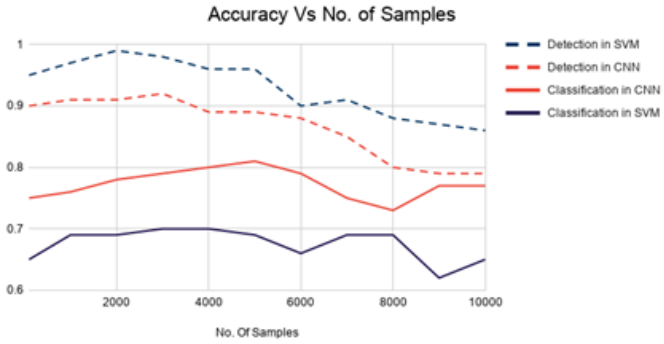

Figure.15 Graph representing accuracy rates of Detection and Classification using SVM and CNN

Table 3. Accuracy comparison with exiting models

Authors	Techniques / Models	Accuracy
Pooshkar Rajiv et.al. 2016	Home Security Systems with Email-Based Cameras	0.95
T.Mantoro et.al., 2018	Multi-Faces Recognition (Haar Cascades + Eigenface methods) Process	0.91
K. M. Rajesh et.al. 2016	Face recognition and emotion detection system using (SVM)	0.94
A. Krishnan et al. 2020	VGGFACE Gender Classification Algorithms Across Gender-Race Groups	0.91
V. Albiero et al. 2020	Multi-Faces Recognition (Conventional CNN model)	0.92
M. E. El Araby and M. Y. Shams, 2021	Face retrieval system (elastic web crawler over cloud computing + KNN Classifier)	0.95
M. Nandhini et. al. 2020	Smart Security System (IOT) based (Raspberry Pi + OpenCV)	0.92
Proposed smart lock system model	HOG+SVM approach	0.96

The presented face detection approach is also evaluated by taking into consideration the person's various accessories. The performance of the algorithm to detect the face position is affected by the use of glasses or a hat. In other instances, the person beard causes face detection may fail. The colour of a person's shirt will cause the face detection system to mistake the face position. When a person wears a shirt which is precisely the same colour as their skin, the algorithm has a lot of difficulty detecting a face. The experimental result has shown that our proposed work smart lock system performed well compared to other approaches. Also, the accuracy and performance are evaluated by accurate data using the HOG+SVM algorithm, and the implementation is done using Spyder (Python 3.7). The entire dataset and implementation of the proposed algorithm has been uploaded in GitHub repository [38] for further reference.

This work offers seamless, hands-free authentication, making access quicker and more efficient, especially in environments like smart homes, offices, and healthcare settings. It can automatically personalize experiences based on recognized users, such as adjusting home settings when a person enters. Facial recognition increases security by making it harder to spoof access compared to traditional methods like passwords or keys. It also allows for real-time monitoring and can be integrated into systems requiring multi-factor authentication for added protection. The technology can be applied across various sectors, including enterprise access control, healthcare (for patient identification), and government facilities (for securing sensitive areas), improving workflow efficiency and security.

6. Conclusion and Future Works

Face recognition in real-time assists in the recognition of human faces, which can be used for person identification and authentication. Support vector machine classifiers are being used to implement it, and they are capable of accurately classifying different types of faces. By increasing the number of images during the training, face recognition accuracy can be improved. As a result of the reduced detection time, the system has a shorter run-time while maintaining high accuracy. Moreover, the successful implementation of the system on the Android platform enhances its accessibility and usability. To make the system more smart, interactive systems and voice assistance can be implemented, which does not require human intervention even in the case of an unknown person at the premises. Suspicious activity detection can be done, and the police department can be called automatically with the assistance of a GSM module attached to the system. The proposed smart lock system model use HOG+SVM approach and attains the accuracy rate of 96%. The accuracy of the detection degrades with the distance increase, a reflection of the lights and colour, and facial feature changes. Further, face detection can be improved using advanced feature extraction techniques to achieve accurate results.

In future, this work will be extended to explore advanced feature extraction techniques to improve face detection accuracy. Also, Investigates the integration of cutting-edge algorithms and methodologies to achieve more precise results in challenging scenarios.

References

[1] Arshi, O., and Chaudhary, A., "Fortifying the Internet of Things: A Comprehensive Security Review," EAI Endorsed Transactions on Internet of Things, 9(4), e1-e1, October 2023.

[2] Jiawei, Z. H. A. O., Mengyao, K. A. N. G., and Zheng, H. A. N, "Robustness of Classification Algorithm in the Face of Label Noise," EAI Endorsed Transactions on Internet of Things, 9(1), June 2023.

[3] Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, and Manoj A Murthy, “Smart Door Locking System using IoT,” International Research Journal of Engineering and Technology (IRJET), Volume: 07, Issue: 05, May 2020.

[4] M Shanthini, G Vidya, and R Arun, “IoT Enhanced Smart Door Locking System,” 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), October 2020.

[5] A. R. Syafeeza, M. K. Mohd Fitri Alif, Y. Nursyifaa Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, “IoT based facial recognition door access control home security system using raspberry pi,” International Journal of Power Electronics and Drive System (IJPEDS) Vol. 11, No. 1, March 2020, pp. 417-424.

[6] D. Cindori, I. Tomičić and P. Grd, "Security Hardening of Facial Recognition Systems," 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2021, pp. 1015-1019, doi: 10.23919/MIPRO52101.2021.9596961.

[7] Caballero-Gil, C., Álvarez, R., Hernández-Goya, C. et al. Research on smart-locks cybersecurity and vulnerabilities. Wireless Netw 30, 5905–5917 (2024). https://doi.org/10.1007/s11276-023-03376-8

[8] M.R.Sanghavi, Srujal Sancheti, Bhakti Patel, Sanjana Shinde, and Neha Lunkad, “Smart Door Unlock System Using Face Recognition And Voice Commands,” International Research Journal of Engineering and Technology (IRJET), Volume: 07, Issue: 06, June 2020.

[9] Soe Sandar and Saw Aung Nyein Oo, “Development of a Secured Door Lock System Based on Face Recognition using Raspberry Pi and GSM Module,” International Journal of Trend in Scientific Research and Development (IJTSRD), Volume 3 Issue 5, August 2019.

[10] Pooshkar Rajiv, Rohit Raj, and Mahesh Chandra, “Email based remote access and surveillance system for smart home infrastructure," Engineering and Material Sciences, February 2016.

[11] T. Mantoro, M. Ayu, Suhendi, “Multi-Faces Recognition Process Using Haar Cascades and Eigenface Methods,” 6th International Conference on Multimedia Computing and Systems (ICMCS), 2018.

[12] A.AdityaShankar, P.R.K.Sastry, A. L.Vishnu Ram, A.Vamsidhar, “Fingerprint Based Door Locking System”, International Journal Of Engineering And Computer Science, ISSN:2319-7242 , Volume 4 Issue 3 March 2015, Page No. 10810-10814.

[13] Liton Chandra Paul, Abdulla Al Sumam, "Face Recognition Using Principal Component Analysis Method," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 9, November 2012.

[14] N. Boyko, O. Basystiuk and N. Shakhovska, "Performance Evaluation and Comparison of Software for Face Recognition, Based on Dlib and Opencv Library," 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Lviv, 2018, pp. 478-482.

[15] K. M. Rajesh and M. Naveenkumar, "A robust method for face recognition and face emotion detection system using support vector machines," 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), Mysuru, 2016, pp. 1-5.

[16] K. P. Bhattarai, B. P. Gautam and K. Sato, "Authentic Gate Entry System (AuthGES) by Using LBPH for Smart Home Security," 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 2018, pp. 191-196.

[17] Karan Maheshwari and, Nalini N, “Facial Recognition Enabled Smart Door Using Microsoft Face API,” International Journal of Engineering Trends and Applications (IJETA) – Volume 4 Issue 3, May-Jun 2017.

[18] H. Bharathi, U. Srivani, M. D. Azharudhin, M. Srikanth and M. Sukumarline, "Home automation by using raspberry Pi and android application," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2017, pp. 687-689.

[19] P. S. Nagendra Reddy, K. T. Kumar Reddy, P. A. Kumar Reddy, G. N. Kodanda Ramaiah and S. N. Kishor, "An IoT based home automation using android application," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 285-290.

[20] Lihua Zhao and Richard Tsai, “Locking and unlocking a mobile device using facial recognition,” United States Patent, March 2015.

[21] Niketha Mohan Jamakhandi, Harshith M, Jagriti, and Priyanka Bharti, “Smart Door Lock using Face Recognition,” International Journal of Computer Sciences and Engineering, Vol.-7, Special Issue-14, May 2019.

[22] Marimuthu, M., Akilandeswari, J., & Chelliah, P. R. (2022). Identification of trustworthy cloud services: solution approaches and research directions to build an automated cloud broker. Computing, 104(1), 43-72. https://doi.org/10.1007/s00607-021-01015-8

[23] Nourman S. Irjanto, and Nico Surantha, “Home Security System with Face Recognition based on Convolutional Neural Network,” International Journal of Advanced Computer Science and Applications, Vol. 11, No. 11, 2020.

[24] Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D., (2023). Safeguard Confidential Web Information from Malicious Browser Extension Using Encryption and Isolation Techniques. Journal of Intelligent & Fuzzy Systems, pp. 1 – 16. DOI: 10.3233/JIFS-233122

[25] M. Nandhini, M.Mohamed Rabik, Kiran Kumar, Ashish Brahma, “Iot Based Smart Home Security System with Face Recognition and Weapon Detection Using Computer Vision,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-10 Issue-1, November 2020.

[26] Muhammad Zeeshan Khan, Saad Harous, Saleet Ul Hassan, Muhammad Usman Ghani Khan, Razi Iqbal, and Shahid Mumtaz, “Deep Unified Model For Face Recognition Based on Convolution Neural Network and Edge Computing,” Special Section On Data Mining For Internet Of Things, Volume 7, 2019

[27] ElAraby, M. E., and M. Y. Shams. "Face retrieval system based on elastic web crawler over cloud computing." Multimedia Tools and Applications 80, no. 8, 2021, pp. 11723-11738.

[28] Shams, M.Y., Sarhan, S.H. and Tolba, A.S, “Adaptive Deep Learning Vector Quantisation for Multimodal Authentication”. J. Inf. Hiding Multim. Signal Process, 8(3), 2017, pp.702-722.

[29] Sarhan, Shahenda, Aida A. Nasr, and Mahmoud Y. Shams, "Multipose Face Recognition-Based Combined Adaptive Deep Learning Vector Quantization", Computational Intelligence and Neuroscience 2020 (2020).

[30] V. Albiero, K. Zhang, and K. W. Bowyer, "How does gender balance in training data affect face recognition accuracy?" 2021.

[31] A. Krishnan, A. Almadan, A. Rattani, Understand-ing fairness of gender classification algorithms across gender-race groups, in: IEEE International Conference on Machine Learning and Applications (ICMLA), 2020, pp. 1028-1035.

[32] Krishnan A, Almadan A, Rattani A (2021) Probing Fairness of Mobile Ocular Biometrics Methods Across Gender on VISOB

2.0 Dataset. In: International Conference on Pattern Recognition (ICPR), pp. 229-243.
[33] Mahsa Merikhipour, Shayan Khanmohammadidoustani, and, Mohammadamin Abbasi, “Transportation mode detection through spatial attention-based transductive long short-term memory and off-policy feature selection.,” Expert Systems with Applications, 267(1), April 2025.
[34] M. Nasri, M. Kosa, L. Chukoskie, M. Moghaddam and C. Harteveld, "Exploring Eye Tracking to Detect Cognitive Load in Complex Virtual Reality Training," 2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), Bellevue, WA, USA, 2024, pp. 51-54.
[35] M. Bodaghi, M. Hosseini and R. Gottumukkala, "A Multimodal Intermediate Fusion Network with Manifold Learning for Stress Detection," 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI), Mt Pleasant, MI, USA, 2024, pp. 1-8.
[36] Seyedmohammad Nouraniboosjin, Melika Yousefi, Sadaf Meisami, Melina Yousefi, and Sajad Meisami, “Empowering healthcare: a blockchain-based secure and decentralized data sharing scheme with searchable encryption.,” International Journal on Cybernetics & Informatics, 13(4), August 2024.
[37] Ali Pourramezan Fard, Mohammad Mehdi Hosseini, Timothy D. Sweeny, and, Mohammad H. Mahoor, “AffectNet+: A database for enhancing facial expression recognition with soft-labels.,” Computer Vision and Pattern Recognition, arXiv:2410.22506, Oct 2024.
[38] https://github.com/MarimuthuSCTSA/Face-Detection-Dataset-and-Implementation-code.