ISSN: 2584-0495 Vol. 2, Issue 6, pp. 915-923

IJMIT International Journal of Microsystems and IoT

International Journal of Microsystems and IoT

Indian Society for VLSI Education

ISSN: (Online) Journal homepage: https://www.ijmit.org

Development of a Secure Access System

Manjot Kaur Bhatia, Gurpreet Kaur, Rajat Tanwar, Jayant Marwaha, Mrinal Narang

Cite as: Bhatia, M. K., Kaur, G., Tanwar, R., Marwaha, J., & Narang, M. (2024). Development of a Secure Access System. International Journal of Microsystems and IoT, 2(6), 915-923. https://doi.org/10.5281/zenodo.13149061

Published online: 24 June 2024

Submit your article to this journal:

Article views:

View related articles:

View Crossmark data:

DOI: https://doi.org/10.5281/zenodo.13149061

International Journal of Microsystems and IoT
Vol. 2, Issue 6, pp. 915-923 ; DOI: https://doi.org/10.5281/zenodo.13149061

Development of a Secure Access System

Manjot Kaur Bhatia, Gurpreet Kaur, Rajat Tanwar, Jayant Marwaha, Mrinal Narang

Department of Information Technology, Jagan Institute of Management Studies Delhi, India

ABSTRACT
Facial identification from real data, photo capture, sensor images, and database images are challenging tasks because of the wide variety of face looks, illumination effects, and intricate image backdrops. Face recognition is one of the most practical and modern applications of image processing and biometric systems. We describe face recognition methods and algorithms that have been created by several researchers in the fields of image processing and pattern recognition utilizing HAAR and OpenCV in this paper. This essay will also discuss the face recognition system's use of this technology and how it differs from alternative methods in terms of effectiveness. Therefore, a general review of face detection studies and systems that rely on various methodologies and algorithms is included in this research. We implemented a complete face recognition system by integrating the best option for each step. With training and without training, it achieves superior performance on every category of the test. The tools which are required for completing the system are a Camera, Microphone, RFID, and Pin Generator. This research study also analyses the performance of various approaches and algorithms in addition to the strengths and weaknesses of these literature studies and systems.

KEYWORDS:
Face Recognition,Image Processing, HAAR, OpenCV, Fingerprint

1. INTRODUCTION

Technology currently reduces the amount of work done by humans; hence it is essential for ensuring ownership of an individual's possessions. Instead of wasting time and money on security, it was made possible by the automation of electronic equipment. Bhatia, M.[2013, 2015, 2017] proposed secure user authentication system by hiding password in images. This project creates a system that thoroughly restrains human substances by relying on technology. This technology can help protect the privacy of any person or organization, such a bank vault or a money locker, among others.

Considering a breach of security, the system is a combination of biometric and prior tech to ensure security escalation of this system. The objective is delivering security progression over extremely concealed premises effortlessly at an affordable cost. Surveillance and facial recognition being operated by a camera for premium security purposes as it stores surveillance data on a memory chip for a definite period. [7] The camera is continuously searching for a human face, and an authorizer is able to see the situation through the camera in real time. To achieve this goal, wireless communication was established between the security system and the authorizer via VNC viewer. [9]

When a person places himself in front of the camera, the camera immediately scans his face with the image database stored in Raspberry Pi. The authorizer is able to see the name of that person at the top of his face in real time video.

If the face doesn't match with the database, the name will be replaced by an unknown person, and the system generates a sound which indicates the sound of an unknown person. After facial recognition, the system will give you a choice for two authentication methods it will ask for (Pin Password - RFID) or (Pin Password - Voice Recognition) if the user fails to enter the right password alarm will ring if the user enters the opposite password. If a user enters a password that is the reverse of the original password, the silent alarm will go to the police.

2. LITERATURE SURVEY

2.1 Bhattacharyya, Budhaditya, Akya Bhatnagar, and Arya Bhattacharya. "A NOVEL APPROACH TO AUTOMATED PARKING USING RFID BASED USER AUTHRIZATION." (2018).

This paper described that Law enforcement has effectively used fingerprint matching for more than a century. These days, a variety of uses for the technology are being made, including identity management and access control. In this context, research opportunities are presented together with a system for automatically identifying fingerprints and spotting significant issues. The description of an RTOS (Real-time operating system) implementation in the context of an embedded system in this report is written in a manner similar to that of a product design. Even though it is widely used, fingerprint recognition is a difficult pattern recognition problem.
Making accurate algorithms that can extract important characteristics and robustly match them is a difficult task. [20]

In this study, we provide a fresh approach to resolving current problems using a suitable embedded system architecture.

2.2 Chin, Howard. Face recognition based automated student attendance system. Diss. UTAR, 2018.

This paper proposed that the majority of institutions in underdeveloped nations still track students' attendance using paper sheets. The management of the students' attendance records urgently calls for the adoption of an alternative approach. RFID enables the university administration to use cutting-edge new technology while taking into account factors like dependability, time savings, and ease of control to improve the university's monitoring system. This article describes the design and development of a student attendance system in terms of hardware and software.

The system is integrated with a database management system to reach complete system capabilities, enabling real-time information manipulation. The RFID Platform is used to emulate RFID scanners. The RFID platform and the.NET Framework have been used to create an automatic attendance system that makes use of RFID.

2.3 Kasar, M., Bhattacharyya, D. and Kim, T. (2016). Face Recognition Using Neural Network: A Review. International Journal of Security and Its Applications, 10(3), pp.81-100

This paper described that due to the broad range of face looks, illumination effects, and intricate image backgrounds, face recognition from real data, capturing photos, sensor images, and database images is a hard task. Face recognition is one of the most practical and modern applications of image processing and biometric systems. In this study, artificial neural networks (ANNs), which have been used in the fields of image processing and pattern identification, are used to cover the facial recognition techniques published by various researchers. In addition, this paper will explain how ANN will be used for the face recognition system and why it is superior to other approaches.

There are numerous ANN-suggested methods that offer an overview of face recognition using ANN. This study presents a review of the literature on ANN-based facial recognition systems. In this paper, several face recognition system architectures, approaches, algorithms, methodologies, databases for training or testing image sets, and performance metrics are examined. Every researcher has their own way of identifying faces in databases or videos, and while many studies have attempted to address the issues with the earlier suggested method, there are still some benefits and drawbacks to the methods we have mentioned.

2.4 Mikael Nilsson, Jorgen Nordberg, and Ingvar Claesson “Face detection using local SMQT features and split up SNOW classifier in IEEE International conference on Acoustics, Speech, and signal processing (ICASSP),2007, vol 2, pp. 589-592

This study serves two purposes. First, it proposes local Successive Mean Quantization Transform features for object recognition that operates in the absence of light and sensors. Secondly, a split Sparse Network of Winnows is provided. The classifier and attributes are integrated to fulfil the task of frontal face detection. For the MIT+CMU and Bio ID databases, the results of detection are displayed. The best-published result for this face detector comes from the Receiver Operation Characteristics curve for the Bio ID database. The outcomes of the CMU+MIT database can be compared to modern face detectors. A face detection system was developed by fusing the local SMQT characteristics with the split-up classifier. The face detector obtains the best reported ROC curve for the Bio ID database and a ROC curve that is comparable to published, cutting-edge face detectors for the CMU+MIT database.

2.5 Bifari, E.N.; Elrefaei, L.A. “Automated Fingerprint Identification System Based on Weighted Feature Points Matching Algorithm”, 978-1-4799-3080-7114/$31.00 ©2014 IEEE

This paper shows that the majority of fingerprint identification systems use matching algorithms based on various minute fingerprint features. Typically, details are taken from the fingerprint picture that has been thinned. The thinning image might produce a lot of false minutiae as a result of the image noise and various pre-processing techniques, which could hurt the system's performance. In order to create the Automated Fingerprint Identification System in this study, some pre-existing algorithms from other studies were merged. On the basis of a feature with two points, minutiae and ridge point, a new matching algorithm was suggested. Additionally, a suitable weight was applied to each extracted feature in accordance with the recommended weights table. A database demonstrated its effectiveness and showed that it outperforms the traditional minutiae-based matching algorithm in terms of outcomes.

The procedures to develop AFIS via MATLAB were described in this study along with some suggested changes to the filter algorithm and a new matching algorithm. Five FVC databases were used in the systems testing. Two points—minute and ridge points—were combined as a fingerprint characteristic, changing the minutiae-based matching process. Then, a weight table was provided to provide a similarity value based on the quality of each feature for each feature. The experimental test demonstrates that the outcomes are dependable and efficient. In order to achieve better results, we advise integrating the suggested approach with other techniques such as local minutiae matching in future studies.

2.6 Rowley, H.A., Baluja, S., Kanade, T. Neural Network-based Face Detection. IEEE Trans. Pattern Anal. Machine Intel, Vol. 20, No.1 Rowle

This paper presents that a fundamental issue in computer vision is object detection. Simply being aware of an object's presence or absence is helpful for applications like image indexing. Face recognition and other technologies that often deal with people depend on facial detection in particular. The object detection problem can be solved using a variety of techniques, including matching sets of two-dimensional images of the object and matching two- and three-dimensional geometric models to photographs.

This dissertation will show how artificial neural networks can be utilised to successfully implement the later view-based technique, which permits the detection of upright, slanted, and non-frontal faces in crowded images. In this study, the majority of the detector's training was done with real-world sample photographs, both with and without faces. For this strategy, a big training data collection is required.

3. PROPOSED MODEL

This model describes how our model performs different types of work in a single system. The name of this model is “Development of Secure Access Systematization”. In this product, we can use it in many ways according to the requirement of the client. As we can see in Fig. 1 the proposed model of our system.
A system for managing the different requirements effectively. It helps to overcome the situation now facing of using a manual system like a signature, RFID, Finger Print based systems but they fail to proof the system.

This product solves many problems which we faced during the execution. This product removes the lack of security because we provide the RFID which is very secure. Titan Security Product also removes the time-consuming system. It provides efficient storage for better data searching.

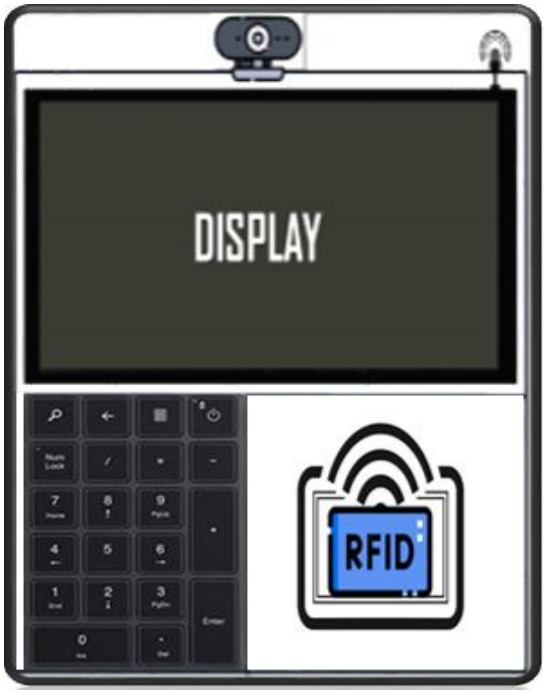


Fig.1 Proposed Model for Facial Recognition System

3.1 Working of device

Some steps would be followed strictly for working the device successfully:

3.1.1 First person has to show his face to the camera for ***Facial Authentication****. If the face will be authenticated then he/she will move on to the next level of authentication else a security alarm will siren.*

3.1.2 Camera will click photos of authenticated users and non-authorized users with the date and time spontaneously at the time of facial recognition and will send them to an application/web portal which can be further reviewed by the admin.

3.1.3 Then the person will have the choice to authenticate two security layers from the rest of the three different security layers ***(RFID, PIN, Voice Recognition).***

3.1.4 If somebody fails to authenticate any of two layers from the rest of the 3 security layers, then the buzzer will siren.

3.1.5 If a person uses a pin password as one of the authentication methods from the rest of 3 and enters the password reverse of the correct password a silent alarm will inform the police about the threat.

3.1.6 After facial recognition, voice recognition would take place where sample audio would be recorded of the person.

3.1.7 The sample audio would be processed to match the phrase spoken by the person and along with that to match the pitch of the person.

3.1.8 Once the process is passed by the system the door would be opened.

3.1.9 Once the person has entered the premises a log file would be updated where the IN time of the person would be logged.

3.2 System Components

The HAAR-Cascade Detection in OpenCV provides the trainer as well as the detector.
We can train the classifier for any object like cars, planes, and buildings by using OpenCV.

There are two primary states of the cascade image classifier:

3.2.1 The first one is training and
3.2.2 The other is detection.

OpenCV provides two applications to train cascade classifiers OpenCV HAAR training and OpenCV train cascade. These two applications store the classifier in different file formats.

For training, we need a set of samples. There are two types of samples.
3.2.3 Negative sample: It is related to non-object images.
3.2.4 Positive sample: It is a related image with detects objects.

A set of negative samples must be prepared manually, whereas the collection of positive samples is created using the OpenCV create samples utility.

3.3 LBPH Algorithm

Local Binary Patterns Histogram algorithm is used for Face Recognition. It is one of the top performing texture descriptors and is based on the local binary operator. Facial recognition systems are getting more and more important. They are used in access control, surveillance, and smartphone unlocking, among other applications. Using LBPH, features from a test image input are extracted and compared to the database of faces as we see in Fig 2.

Steps of the algorithm

3.3.1 *Selecting the Parameters: The LBPH accepts the four parameters: Radius, Neighbours, Grid X & Y.*

3.3.2 *Training the Algorithm.*

3.3.3 *Using the LBP operation.*

3.3.4 *Extracting the Histograms from the image.*

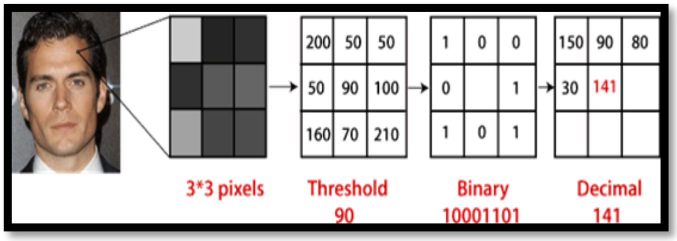


Fig.2 LBPH Algorithm Working

3.4 Microphone Use for Voice Recognition

They are mentioned implementation uses The Free ST American English Corpus dataset (SLR45), which is a free American English corpus by Surfing technology, containing utterances from 10 speakers (5 females and 5 males)

Once we download the data set, we split it into two different parts –

3.4.1 *Training set: Some parts for training the individual gender models.*

3.4.2 *Testing set: Some parts for testing the accuracy of gender recognition.*

Voice Features Extraction- The Mel-Frequency Cestrum Coefficients (MFCC) are used here since they deliver the best results in speaker verification. MFCCs are commonly derived as follows –

3.4.3 *Take the Fourier transform of (a windowed excerpt of) a signal.*

3.4.4 *Map the powers of the spectrum obtained above onto the Mel scale, using triangular overlapping windows.*

3.4.5 *Take the logs of the powers at each of the Mel frequencies.*

3.4.6 *Take the discrete cosine transform of the list of Mel log powers, as if it were a signal.*

3.4.7 *The MFCCs are the amplitudes of the resulting spectrum.*

To extract MFCC features I usually use the Python-Speech-Features library, it is simple to use and well-documented.

Gaussian Mixture Models:

To train Gaussian mixture models based on some collected features, you can use scikit-learn-library specifically the scikit-gm as we see the Gaussian Mixture Model in the Fig 3

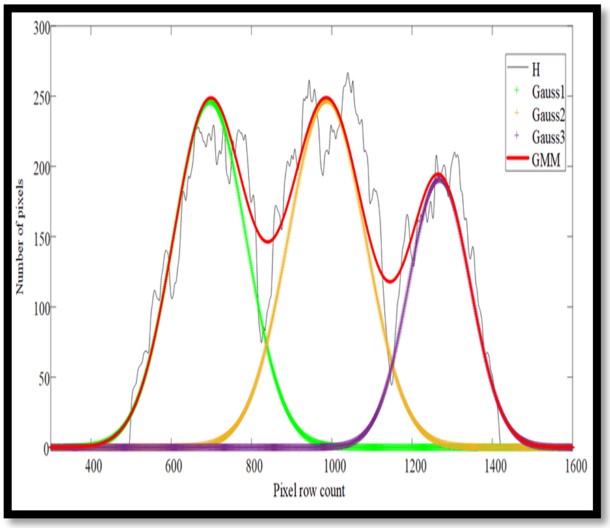


Fig.3 Gaussian Mixture Model

3.5 Speech to text Phrases Matching

Steps of Working:

3.5.1 *Our voice and phrases will be trained through CMU Sphinx.*

3.5.2 *With CMU Sphinx voice sample will be transcribed.*

3.5.3 *With the result that the phrase would be saved in data for the initial stage.*

3.5.4 *When the system would be set up completely and user data would be entered. The input/voice sample provided by the user would be transcribed and compared to throughout the data to match the phrase.*

CMU Sphinx

3.5.5 *State of art speech recognition algorithms for efficient speech recognition. CMU Sphinx tools are designed specifically for low-resource platforms.*

3.5.6 *Support for several languages like US English, UK English, French, Mandarin, German, Dutch, Russian and the ability to build a model for others.*

3.6 RFID System

The reader/writer device emits electromagnetic waves at a certain frequency through the antenna when the magnetic card is in the broadcast area of the reader. It receives the energy and retransmits its own code. From there, it knows exactly which devices are in the control area.

Most RFID systems often have multiple read devices connected to a central computer.

RFID Components:

A simple RFID system is made up of two main components: device reader/writer and tag as we see in Fig 4.

Device Reader/Writer: It is a wireless communication device that can detect tags that have the same operating frequency within a certain range.

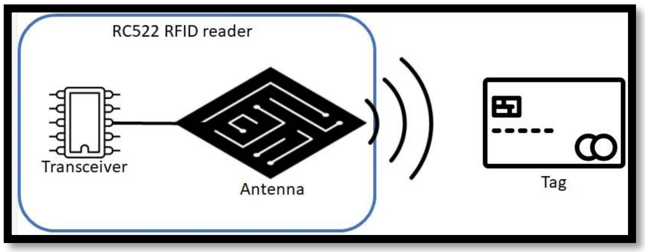


Fig 4: Raspberry Pi in place of computer.

The RF module here is used along with a pair of encoder/decoder. The encoder is used for encoding the bits to be transmitted parallel which are decoded by the decoder on their reception at the receiver. The encoder/ decoder pair used in the proposed model is HT12E – HT12D. The ‘12’ in the name means 8-address lines and 4-data lines. The encoder has four input lines. These lines serve the purpose of providing the input which has to be encoded. The input given to data pin is in parallel form which is being transmitted into serial form from the data output pin. The resistance to be applied between oscillator pins can be found out from the frequency vs voltage graphs for decoder and encoder given in Fig 5 and Fig 6, respectively. [14] As we also add System Control flow chart which is given in Figure 7.

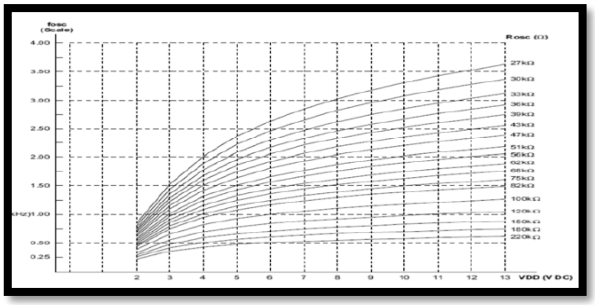


Fig 5: Frequency of oscillation vs Vcc graph for decoder.

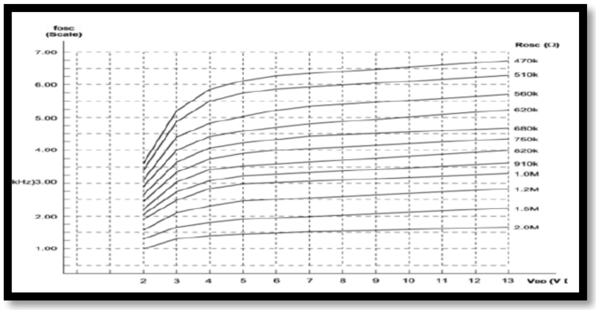


Fig 6: Frequency of oscillation vs Vcc graph for encoder.

Vcc = 9V, frequency of oscillation (encoder) = 3.7 KHz, frequency of oscillation (decoder) = 185 KHz. From Figure 5 and Figure 6 resistance across oscillator pins (encoder) = 820 KΩ, resistance across oscillator pins (decoder) = 47 KΩ.

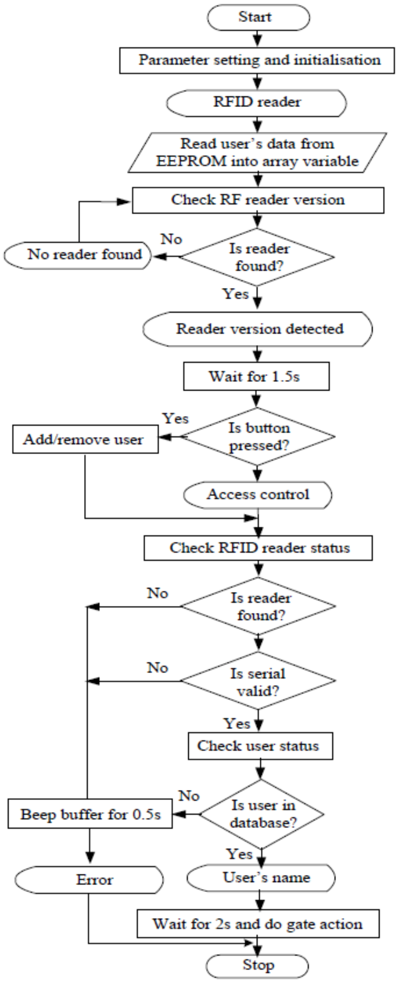


Fig 7: Control system is the RFID-based security system.

3.7 PIN Generator

If a user enters a password that is the reverse of the original password, the silent alarm will go to the police. We are using the RSA algorithm to encrypt passwords and save them on the local machine and users can add PINs according to their choice.

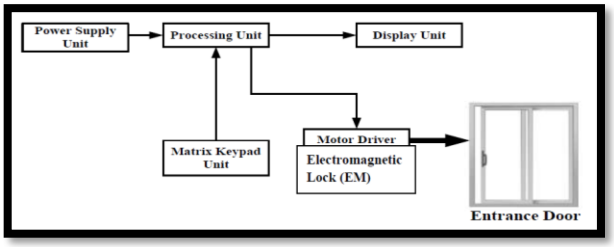
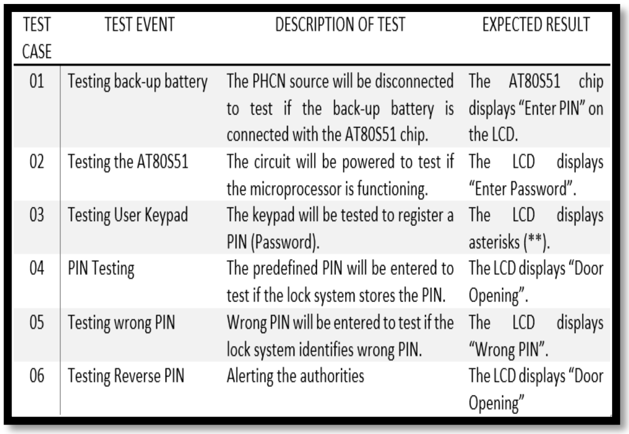


Fig 8: Block Diagram of Entrance Door for PIN

In figure 8, it shows the block diagram of the secured entrance door lock system. In the hardware design and implementation, five functional units are involved. The functional units include: the power supply unit, the processing unit, the display unit, the Electromagnetic Lock (EM) unit and the matrix keypad unit.

This will be documented, implementation of the capabilities, strength and Effectiveness of the secured door lock system with doors used. The expected outcome/result of the research is shown in Table 1. [13]

Table. 1 Test Case for the PIN



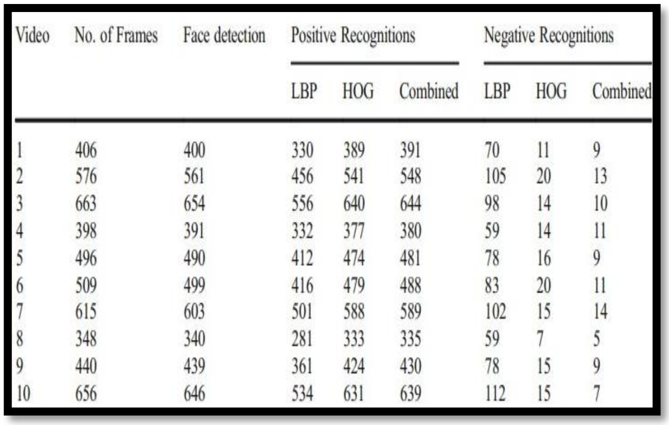
TEST CASE	TEST EVENT	DESCRIPTION OF TEST	EXPECTED RESULT
01	Testing back-up battery	The PHCN source will be disconnected to test if the back-up battery is connected with the AT80S51 chip.	The AT80S51 chip displays "Enter PIN" on the LCD.
02	Testing the AT80S51	The circuit will be powered to test if the microprocessor is functioning.	The LCD displays "Enter Password".
03	Testing User Keypad	The keypad will be tested to register a PIN (Password).	The LCD displays asterisks (**).
04	PIN Testing	The predefined PIN will be entered to test if the lock system stores the PIN.	The LCD displays "Door Opening".
05	Testing wrong PIN	Wrong PIN will be entered to test if the lock system identifies wrong PIN.	The LCD displays "Wrong PIN".
06	Testing Reverse PIN	Alerting the authorities	The LCD displays "Door Opening"

4. COMPARATIVE STUDIES

The comparative study presented in this section examines theoretical issues and simulations carried out with the LBP, HOG, and both combined algorithms, a database with many classes and few images per class. Due to certain characteristics of the approaches, it is crucial to employ both types of classifiers. [8], [10] The Histogram of Oriented Gradients (HOG) and the Local Binary Pattern Histogram Algorithm (LBPH) were used to extract two distinct sets of features from each facial image (HOG).

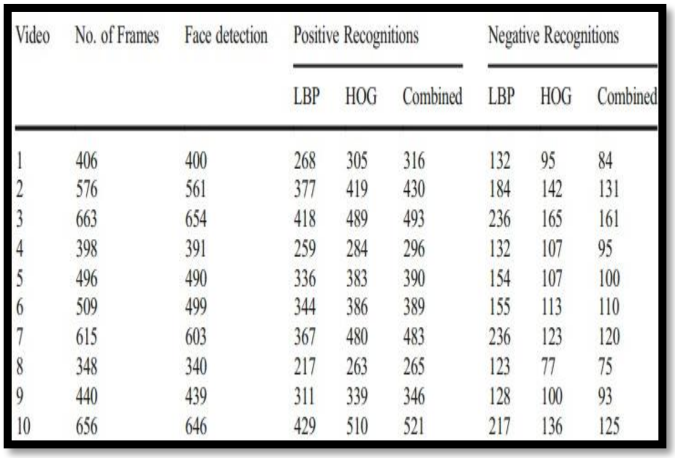
The classification recognition rate is performed on the Video Database with various classifiers, and the results are reported in Tables 2 and 3. The comparative test is carried out with the two local facial components using the k-Nearest Neighbours Algorithm (KNN) and the Support Vector Machine Algorithm (SVM). LBP is an excellent local characteristic for facial recognition. However, as anticipated, HOG also outperforms LBH; for this reason, when we combined the two algorithms, the output supported positive recognition in the KNN classifier, but in negative recognition, it demonstrated LBH is superior to other algorithms, demonstrating our system performs better and produces good results.[19]

Table 2: Recognition Rate on Video Database with KNN classifier.



Video	No. of Frames	Face detection	Positive Recognitions			Negative Recognitions		
			LBP	HOG	Combined	LBP	HOG	Combined
1	406	400	330	389	391	70	11	9
2	576	561	456	541	548	105	20	13
3	663	654	556	640	644	98	14	10
4	398	391	332	377	380	59	14	11
5	496	490	412	474	481	78	16	9
6	509	499	416	479	488	83	20	11
7	615	603	501	588	589	102	15	14
8	348	340	281	333	335	59	7	5
9	440	439	361	424	430	78	15	9
10	656	646	534	631	639	112	15	7

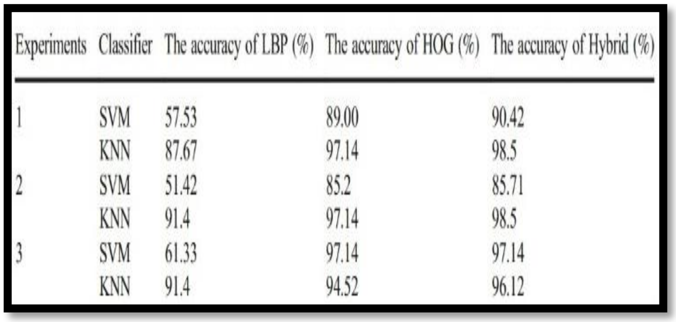
Table 3: Recognition Rate on Video Database with SVM classifier.



Video	No. of Frames	Face detection	Positive Recognitions			Negative Recognitions		
			LBP	HOG	Combined	LBP	HOG	Combined
1	406	400	268	305	316	132	95	84
2	576	561	377	419	430	184	142	131
3	663	654	418	489	493	236	165	161
4	398	391	259	284	296	132	107	95
5	496	490	336	383	390	154	107	100
6	509	499	344	386	389	155	113	110
7	615	603	367	480	483	236	123	120
8	348	340	217	263	265	123	77	75
9	440	439	311	339	346	128	100	93
10	656	646	429	510	521	217	136	125

According to the results, we can conclude that LBPH Algorithm is a more effective technique for facial recognition. Also, Table 4 shows the Accuracy rate of the KNN & SVM classifier, and the three together regions of experiments show that LBH and Hybrid both conclude better results.

Table 4: Accuracy Rate of KNN & SVM classifier.



Experiments	Classifier	The accuracy of LBP (%)	The accuracy of HOG (%)	The accuracy of Hybrid (%)
1	SVM	57.53	89.00	90.42
	KNN	87.67	97.14	98.5
2	SVM	51.42	85.2	85.71
	KNN	91.4	97.14	98.5
3	SVM	61.33	97.14	97.14
	KNN	91.4	94.52	96.12

There are just some of those technologies that everyone knows and has accepted for the system to get better and more accurate results, but bottom line is that currently, Hybrid is not user intuitive. While there are a lot of recipes, they are all borderline useless because they all need to be thoroughly customized to the point of creating a custom model [11], [12].

5. EXPECTED RESULTS

Write the text from your article in different sections. Write the text from your article in different sections. Write the text from your article in different sections. Write the text from your article in different sections. Write the text from your article in different sections.

In the expected results, we define how our system actually works and how accurately it gave the output to the user. We also have a working system so we also attached some screenshots for more clarity like how Facial Recognition, Voice Recognition works and how it responds.

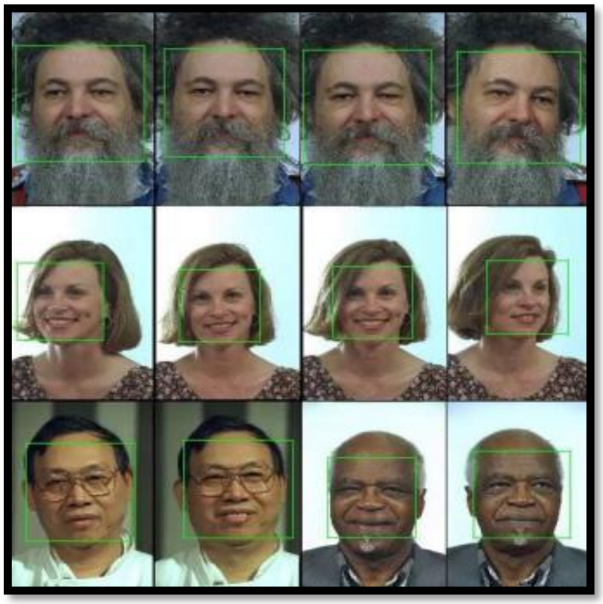


Fig 5: Sample results taken from data set testing using LBP algorithm.

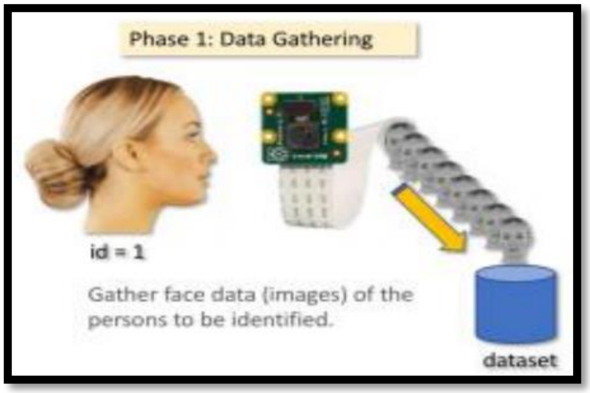


Fig 6: Data Gathering

In Fig 5, we shows how the sample results taken from data set testing using LBPH algorithm.

In Fig 6, here we show clearly how the user data gather and also how we train the data of the user and store that data in the database (MySQL). It also shows the System where we add user details and also train the data of the user.

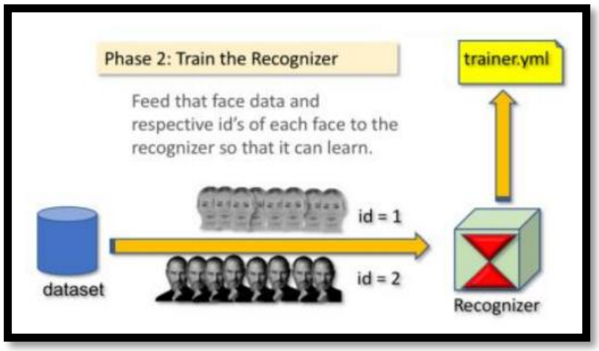

Phase 2: Train the Recognizer
Feed that face data and respective id's of each face to the recognizer so that it can learn.
trainer.yml
id = 1
id = 2
dataset
Recognizer

Fig 7: Train the Recognizer

In the above section which represents Fig 7, shows how system recognize the train data for feed that face data and respective id's of each face to the recognizer so that it can learn.

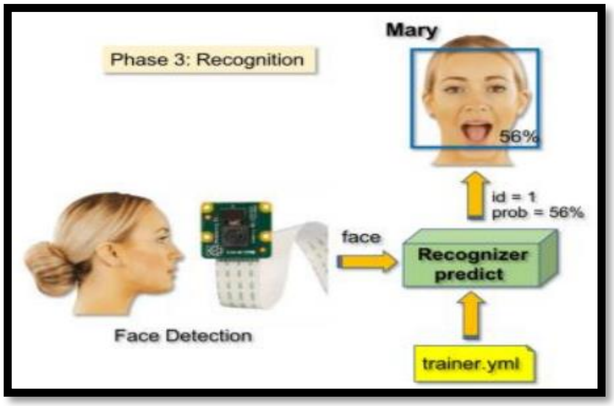


Fig 8: Final Recognition

In Fig 8 here we also see the actual output of the system how it recognizes the face of the user using Camera and later on we also add different components in the system for more security like RFID, PIN, Voice Recognition.

To ensure the safety of lives and properties, a modern technology that can overcome the challenges of the traditional approaches is required. [15] [17] This describes the design and control strategy of a two-factor authentication security system based on the technology with efficient control facilities and an enhanced user interface that can secure the entrance to a house.

6. CONCLUSION

This paper includes a summary review of our proposed model and how it actually works in real-life and also solves many problems related to face recognition systems based on HAAR, and OpenCV. Here we discussed different architectures, approaches, and methods for training or testing images, and performance measures of face recognition systems were used in each study. Every researcher has their own method for identifying faces in databases or on video in order to address the issues with prior proposed approaches, but these methods are still not without their benefits and drawbacks. We now have RFID, PIN, Facial Recognition, Voice Recognition, and three-factor authentication (multiple). The method helped to ease a variety of worries, including the potential for cheating in various movement and facial expression components. The encryption method also improves security by preventing unauthorized tampering with the material that has been recorded.

REFERENCES

1. Hardika, C. and Chitaliya, N. (2017). Smart Attendance Management and Analysis with Signature Verification. International Journal of Advance Research, Ideas and Innovations in Technology, 3(3), 89-90. https://www.ijariit.com/manuscripts/v3i3/V3I3-1150.pdf.

2. Yadav, D. K., Singh, S., Pujari, S. and Mishra, P.(2015). Fingerprint Based Attendance System Using Microcontroller and Labview. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 4, 5111-5121, doi: https://doi.org/10.15662/ijareeie.2015.0406029.

3. Al-Naima, F. M. and Saleh, M. A.(2015). A Proposed RFID Based Student Attendance System. International Journal of Computing and Network Technology, 3(2), 49-55, https://link.gale.com/apps/doc/A606881367/AONE?u=anon~d39369d&sid=googleScholar&xid=3fc2edc7.
4. Walton, C. (1973). Electronic Identification & Recognition System. U.S. Patent No. 3,752,960: https://patents.google.com/patent/US4388524.
5. Lee, Y. J. et al. (2007). Biometric Key Binding: Fuzzy Vault Based on Iris Images. Lecture Notes in Computer Science, International Conference on Biometrics, Berlin, Heidelberg: Springer. 4642, 800-808. doi: https://doi.org/10.1007/978-3-540-74549-5_84.
6. Kasar, M. M., D. Bhattacharyya, and T. H. Kim (2016). Face Recognition Using Neural Network: A Review. International Journal of Security and Its Applications, 10(3), 81-100. doi: https://dl.acm.org/doi/10.5555/2391659.2391750.
7. Chin, H. (2018). Face Recognition Based Automated Student Attendance System. Dissertation, UTAR. http://eprints.utar.edu.my/2832/1/EE-2018-1303261-1.pdf.
8. Nilsson, M., Nordberg, J. and Claesson, I. (2007). Face Detection Using Local SMQT Features and Split up Snow Classifier. IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07, Honolulu, HI, USA, II-589-II-592. doi: https://doi.org/10.1109/ICASSP.2007.366304.
9. Bifari E. N. and Elrefaei, L. A. (2014). Automated Fingerprint Identification System Based on Weighted Feature Points Matching Algorithm. International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India. 2212-2217. doi: https://doi.org/10.1109/ICACCI.2014.6968559.
10. Agrawal S. and Khatri, P. (2015). Facial Expression Detection Techniques: Based on Viola and Jones Algorithm and Principal Component Analysis. Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, India, 108-112. doi: https://doi.org/10.1109/ACCT.2015.32.
11. Rowley, H. A., Baluja, S. and Kanade, T. (1998). Neural Network-Based Face Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(1), 23-38. doi: https://doi.org/10.1109/34.655647.
12. Reynolds, D. A., Quatieri, T. F. and Dunn, R. B. (2000). Speaker Verification Using Adapted Gaussian Mixture Models. Digital Signal Processing, 10(3), 19-41, doi: https://doi.org/10.1006/dspr.1999.0361.
13. Umar, A. O. (2019). A Secured Entrance Door Lock System Using Password Based. African Scholars Journal of Pure and Applied Science, 15(9),110-126,https://www.africanscholarpublications.com/wp-content/uploads/2020/06/AJPAS_Vol5_No9-7.pdf.
14. Verma, S., Garg, N., Sharma, S. and Kashyap, I. (2018). A Novel Approach to RFID Based Automated Parking Charges Collection System. International Journal of Computer Applications, NCNCCACT 2017, 7-13,https://research.ijcaonline.org/ncnccact2017/number1/ncnccact2017008.pdf.
15. Okundamiya M. S. and Emakpor, S.(2017). Design and Control Strategy of a Security Door System Using Radio Frequency Signal. IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), 406-412. https://www.researchgate.net/publication/323228541

AUTHORS

Manjot Kaur Bhatia received the PhD degree in information security from the University of Delhi, Delhi, India. She is currently working as a Professor of Computer Science with the Jagan Institute of Management Studies, Delhi. She has more than 20 years of teaching and research experience in the areas of information security, databases, Linux, and operating systems. Her research interests include cloud computing, steganography, data hiding, information security, and software testing.
E-mail: manjot.bhatia@jimsindia.org

Gurpreet Kaur completed her bachelor's degree in computer applications from the Jagan Institute of Management Studies, located in Delhi in 2021. Currently, she is pursuing her master's degree in computer applications from the same institution. Driven by her passion for technology, she has developed a keen interest in various domains within the field of computer science. Her areas of expertise and interest lie in Python programming and front-end development.
E-mail: 156.gurpreet@gmail.com

Rajat Tanwar completed his bachelor's degree in computer applications from the Institute of Information Technology & Management in Delhi in 2021. Currently, he is studying in Master of Computer Applications at Jagan Institute of Management Studies, Delhi. He has a strong passion for technology and finds various aspects of computer science fascinating. He is skilled in Python programming, front-end development, and blockchain technology.
E-mail:rajattanwar63@gmail.com

Jayant Marwaha completed his bachelor's degree in computer applications at Chander Prabhu Jain College of Higher Studies & School of Law in Delhi in 2021. Currently, he is pursuing his master's degree in computer applications from Jagan Institute of Management Studies affiliated to GGSIPU. His profound passion for technology has ignited a keen interest in various domains within the realm of computer science, with a particular focus on Python programming and machine learning.
E-mail: jayant_mca21@jimsindia.org

Mrinal Narang completed his bachelor's degree in computer applications from the Institute of Information Technology & Management in Delhi in 2021. Currently, he is studying in Master of Computer Applications at Jagan Institute of Management Studies, Delhi. He has a strong passion for technology and finds various aspects of computer science fascinating. He is skilled in Python programming, b Linux and Cloud platform.
E-mail: mrinalnarang51@gmail.com