IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Face Detection Using Machine Learning And Morse Code Based Authentication

Anjushree K
Student
Mtech in CSE
Dr. Ambedkar Institute Of Technology
Bangalore, India

Dr. Siddaraju
Professor and Head
Dept of CSE
Dr. Ambedkar Institute Of Technology
Bangalore, India

Abstract: Machine learning techniques has evolved in our day today life and has turned out our life more easily efficient and secured in many aspects. Security is always the major concern. We need to secure our important belongings and information may it be the phone, house lock, UPI pin and fingerprints. But hackers always will always find a way to intrude and break the security wall. Hence it is safe to use more security steps for securing the system. More number of security checks the less the hackers or intruders can break the security wall. Here we are proposing a system containing two steps of security checks to get into the system. We may all be aware of face recognition in our phones. In recent generation phones face recognition acts as a major secured system to protect any device. Our system consists of two step authentication system which starts with face recognition and proceeds with Morse code based authentication. Morse code is a code which is a sequence of dots and dashes. PIN (Personal Identification Number) is usually given has input to any device to verify identification. Usually we tend to enter the PIN through keyboard. This can be stated has manual entry. But this method of entering the PIN is susceptible for cyberpunks to crack the PIN easily. Hence there was a necessity for a method which overcomes this hindrance. This paper mainly focuses on entering the PIN through eye blinking. Here we are able to enter the PIN using eye blinking technique. Both the authentications will run with the aid of smart camera in the device. Here we are using the cascade classifier for face recognition. We are implementing HOG features for eye blinking detection. Our model is user friendly, simple oriented and covers all the functional requirements specified.

***Index Terms* - Security, PIN (Personal Identification Number), Face recognition, Authentication, Morse code.**

I. INTRODUCTION

Data analyzing is a process of finding, investigating, cleaning and modelling the data. It is done for discovering useful information with the proper conclusions. It works with huge data to extract some useful information. Machine learning is a main application of AI (Artificial Intelligence). It enables the systems and monitors with the strength and ability of automatically grasping and learning. The systems in machine learning are very less explicitly programmed. It stresses on the overall development of computer generated programs. Main aim here is to train the model without any human intervention. So given a set of data the algorithm will have a capacity to recognize a pattern and gives the prediction. Security is a major concern in today's life. Present technology with respect to privacy should be constantly be updated for overcoming the intrusions. Digital security enacts a key role in securing our devices which stores important documents in various forms. We tend to use PIN (Personal Identification Number) for authentication before entering for securing the device or application. PIN based authentication is used since 90s for security margins. It's been widely used for maintaining the privacy. PIN when entered through keyboard can be easily traceable and can be decoded. It's not completely safe because we tend to enter the PIN manual using a keyboard. Hackers can easily trace the marks of PIN entered through keyboard. There was a huge need of a secured system to maintain the protection without been endangered by the intruders. Hence the biometric related authentication model has been quite popular these days which overcomes all the liabilities and drawbacks of traditional method. It's been attracted current generation globally and accepted worldwide. In this paper we are proposing a model where the PIN can be entered through eye blinking technique. Here we are trying to combine the biometric characteristics such as face and eye recognition and try to use the same for authentication. In the initial step of our model we try to implement the face recognition. The next stage of the model we have implemented PIN authentication in the form of Morse code through eye blinking technique. Here the PIN will be captured through eye blinking. The users can enter the PIN by blinking the eye. Hence it does not leave a trace mark of any prints. Through this approach a more secured way of entering the PIN is achieved which is not vulnerable to hackers. A crucial criteria for above strategy to work efficiently the user must be calm, composed, quick, distinguished and accurate. So the dataset provided during the training process of the model should be accurate. How does the machine learning techniques work. Let's take an example of a fingerprints on the phone. First we need to give a sample of prints as dataset. Once we give a sample of data the machine is able understand the fingerprints belongs to a so and so person and recognizes the print when it's given on a real time. This whole process can be considered as training the model with good amount of dataset. And then testing the model whether it's able to recognize the data. Same technique will be implicated here in order to active the outcome. Live dataset will provided to the model say 100 sample of face image will be captured for face recognition.

II. LITERATURE SURVEY

Contains various conceptual works to understand the basic practices. Literature survey is a process of discovery, digging and finding of various related sources inter related to a theme. Referring to literature survey will allows us to enhance our present knowledge and also acts as a foundation for new ideas using the same concept. Researcher Mehrube Mehrubeoglu [1] describes about PIN(Personal Identification Number) entered physically can be vulnerable to password cracking through shoulder surfing. Entering the PIN in an public place makes the PIN exposed to many eves dropping consequences and affects the privacy. Here the main highlight is to enter the PIN through gazed based authentication with the aid of a smart camera which enables a real time eye detection and eye tracking mechanism. PIN authentication should be done with hands off based PIN entry to overcome these tracking. Gaze based authetication means tracking the eye over time and entering the PIN using a real time camera. Since there is no contact while entering the PIN, this acts as a high level of security and helps us to reduce the vulnerabilities caused during the PIN entry. Researcher Sota Shimizu [2] describes how eyes actions are captured with respect to two criterias i.e. tennis experts and beginner will be compared to detect the motion skills. This paper mainly motivates on the eye movement between the two catogories of players. A eye tracking device is taken as reference to analyze the data. We can evident that there is a difference between the experts and also the beginners in the results. We can observe that the beginners will follow the tennis ball once the opposite player shots it. This is a reflex action. With the aid of eye tracking devices a gaze point can be recreated. Researcher Aniwat Juhong [3] explains how a smart eye tracking system can help people suffereing with disabilities and old people. Here the main concept is how to control appliances using eye movement. It also focuses on how to control the wheelchair through eye movement. Here they have implemented image processing through C++. Image will be captured and will be sent to Raspberry Pi comprising of a microcontroller for image processing. They have used OpenCV to determine the eye ball and its co-ordinates. Eye ball movement is refereed for the cursor movement for controlling the system. Eye blinking is used as a command to enter. Just like how we press enter on keyboard. The wheelchair module is controlled using wheelchair joystics. System is implemented to communicate with the other devices by sending messages. Researcher Naga Soundari [4] discusses about accessibility. Here main aim is to cut down the distance between disabled individuals. There is a list of challenges for physically disabled persons to overcome. A method of eye tracking is proposed for carrying out simple tasks. Eye based interfaces have been created to carry out the interactions and the various processes to reduce the traditional methods of interaction such as mouse and keyboard. A robot is found which can be controlled and can run based on eye blinks. A Human Computer Interface is designed for communication between human action and the workstation. They have tried to reimburse the disabled people by providing an interface that uses facial features to interact with the system. Researcher Rupali Gawande [5] tries to explain how the interfaces is evolved to being an important aspect of our daily life. One such field is face recognition which has increased number of fans in order to deal with the security aspect. Real time face recognition is a tedious task which includes implementing and extracting only essential features required for detection. Recognition and extraction are essential steps from a live dataset. Once the face is recognized next important step is to implement the eye movement based interactions. They have used Human computer interface to achieve the same. Researcher JeHun Gu [6] presents Morse Code based representation using EMG signals. Morse code is a powerful communication method. It decodes a sequence of numbers or alphabets with the sequence of dots and dashes. Through this method we can decode a password or code word or a secret word. It has a simple structure which consists of only dots and dashes. The inputs can be given in many ways of human gesture such as finger movement, tongue gestures and through eye blinking movements. Here Electromyography (EMG) signals have been used to engender the hand movements. Here the Morse code has been implemented by either folding or stretching of the hand which constitutes the dots and dashes. They able to decode all the 26 alphabets successfully with increased accuracy. Researcher Ainampudi Kumari Sirivarshitha has proposed a scheme for face detection utilizing OpenCV technology and various libraries provided in python. There is tremendous amount of growth in video and image dataset and want to understand the curve behind the dataset. Any software which uses face attributes in order to detect and classify is called as a biometric. Essential features will be captured with respect to an individual person and will be stored in the database in order to recognize. A machine learning technique compares the image stored with image taken and classifies it accordingly. Facial recognition software can have a huge number of application with respect to employee detection in any firm, student detection in educational institution, passenger detection in travel agency and many more. Here main libraries such as OpenCV is used. Researcher Romit Ganjoo has presented Anti spoofing of door lock using the facial recognition system with eye blinking technique. This paper mainly emphases on the facial recognition which helps to identify an unauthorized access and breakage into the system. Here the basic technique used in Histogram of Gradients (HOG) in order to verify the face. This technique uses support vector machine algorithm to recognize the facial instance. With the help of raspberry pi the entire work is implemented. The coding is done in Python using the build in libraries such as OpenCV. The first model i.e. the HOG model is used to collect the essential facial features from the individual. Here local gradients and edgy directions will help to determine the shape and appearance of the individual. The second model i.e. the support vector machine model to determine the classification process. It helps us to identify the hyper plane to classify the points with more accuracy and perfection. Here along with facial recognition the eye blinking technique is also implemented so a third party person cannot intrude.

III. PROBLEM STATEMENT

A real time application and aid that enables a person to use a secure system to protect their device. Here we can enter the code without any physical touch with the keyboard. Using eye blinking technique the Morse code can be entered to the device. This project has two verification steps. One is face recognition the next is code verification using Morse code. Here in our proposed project we are including two step of security checks to get into the system. We may all be aware of face recognition in our phones. In recent generation phones face recognition acts as a chief secured system to protect any device. Along with face recognition we can also set a code which can play as a security code. We need to secure our important belongings and information may it be the phone, house lock, UPI pin, fingerprints etc. But hackers always will find a way to intrude and break the security wall. So it’s always safe to use more security steps in order to secure the system. More number of security checks the less the hackers or intruders will have possibility to break it. PIN is called as Personal Identification number is implemented to secure the phone ever since 90s. These PIN numbers might be easily traceable and can decoded. Hence there is necessity for a more secured technique than manually entering the PIN on the device. We have introduced PIN authentication without using hands i.e. manual entry.

IV. METHODOLOGY

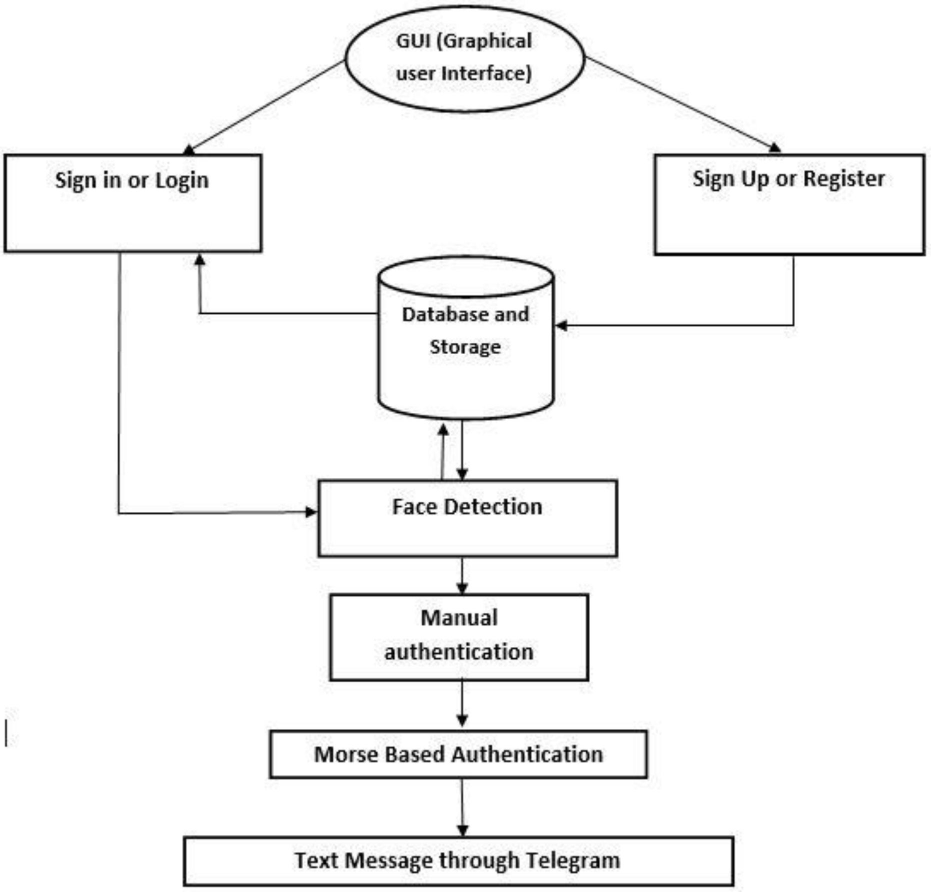


Figure 1. Architecture

4.1. Face recognition modules

Face recognition is a systematic approach which acquires data from an individual and extracts essential features. Now it will compare the essential feature set with the captured data and gives the results out from the comparison. Face recognition model as 5 important modules which are listed below:

A. Acquisition module: A real time camera embedded within the system is essential to collect raw data of the individual. In our system we are going to collect 100 real time pictures which is essential to train the model. Acquisition module acts as a machine interface and therefore is crucial to determine the net performance. The data collected will be an image and only necessary features will be taken from the set of images.

B. Pre-processing module: The data set acquired from the individuals is not an accurate data or cleaned data is utilized for further processing. Hence it is required to pre-process the data to useful form and extract required features from it for the further processing.

C. Convert the images to grayscale: Converting the image to grayscales means to remove the colour from the image. In a coloured image each pixel can be denoted as three important colours i.e. RGB-Red, Green, and Blue. In grayscale image there is only one channel which represents the brightness or intensity of the pixel. Hence the mechanism of converting the coloured image to grayscale image is taking the average of RGB colours at each particular pixel and setting a channel to the average value. In grayscale image contains only a single intensity value. It usually ranges from 0 to 255. Here we are converting the coloured image to grayscale because colour information is not necessary hence for simpler data set we do this process.

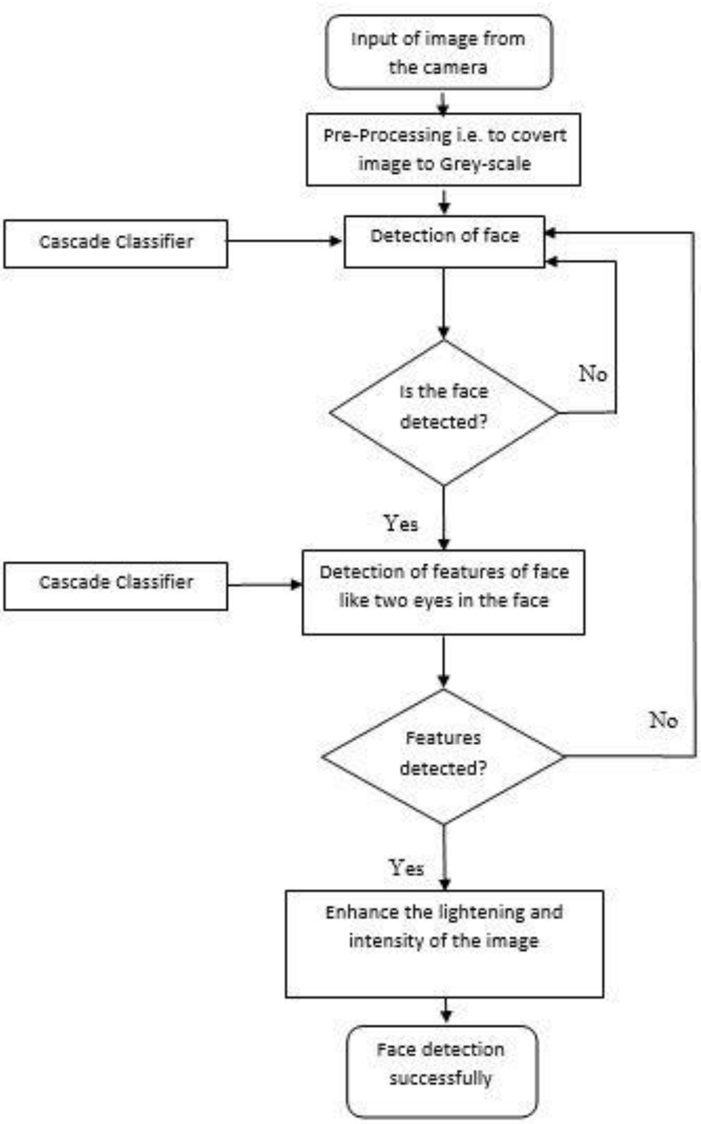
D. Feature Selection module: The data that is been processed is all set for feature selection. Feature selection is a method of extracting required features from the face area for detection of the face. For example: for detection of face position and distance of eyes, nose, and mouth features will be extracted. This feature data set will be accumulated in the data base. This data will be used for training purpose and it is commonly called as template.

E. Classification module: Once the system is trained it is prepared to be tested in real time. We will collect the testing data extract the required feature. Now this feature set will be equated with the stored feature dataset. This process is called as classification. The classification module consists of a decision making instance to compare. Here we are going to apply Haar cascade and LBPH classifier to for the classification process. We need essential libraries. We can import these libraries easily in python since most of them are in built.

F. Database module: Database module is the significant module for storing the information and data. For training purpose the required features mined out from the data set needs to be deposited in a repository for classification or identification purpose. The stored data set that's usually used for comparison to determine the performance and to carry out the classification process. For any given application the user data information for basic features like login, username and password collects the data and will be stored in the database module. The database module is set to mandatorily manage the data and to modify, create, delete and to rename the data from the database. The stored images are often referred as training images. The images caught during the authentication process is called as input or test images. Here we are employing the DB browser for managing the data.

V. IMPLEMENTATION

5.1 Face detection process



Input of image from the camera
Pre-Processing i.e. to covert image to Grey-scale
Cascade Classifier
Detection of face
Is the face detected?
No
Yes
Cascade Classifier
Detection of features of face like two eyes in the face
Features detected?
No
Yes
Enhance the lightening and intensity of the image
Face detection successfully

Figure 2. Flow diagram of Haar Cascade Algorithm

Haar cascade classifier is known as a chief machine learning algorithm which is implemented to classify the negative and a positive image. This algorithm was found by scientist Paul and Michael in the year 2001. Haar feature based classifier is utilized for classifying of object detection. Haar like features are nothing but simple rectangular filters which are used to abstract required data and material from the given image. Haar features are black and white rectangular boxes of different size and positions. This features are necessary to know the intensity or brightness of neighboring adjacent regions. To train the model and to create Haar cascades for anterior face detection the model will be trained using a large dataset containing the images. These images can be both progressive and non-positive images. A positive image involves of a face whereas a negative image consists of a non-face image. The Haar cascade algorithm will make use of the Haar features and threshold to differentiate between positive and negative image. The speed of computation will be increased of Haar features for faster process. Hence we are including an integral image for this process. Integral image is a representation of its original image. In the integral image each pixel is the addition of all pixels either to the top or left of it. This will help us to boost the algorithm and enables it to compute the intensity or brightness in any given region with a constant time. Cascade classifier is a major part which is used to reject the images which contains the non-face images. Basically during the face detection process each image will be passed through the cascade classifier to identify and reject the non-face images. Once we get a bundle of potential facial regions we can apply non-maximum suppression methods to remove the duplicate facial detection and to keep only the potential facial detection. Face detection is a process of finding, extracting the face from a given input photo, video or webcam. Following are the prominent features extracted with regards to a face namely:

- Edge Feature
- Linear feature
- Central feature

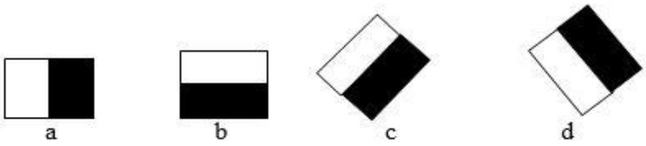


Figure 3. Edge Feature

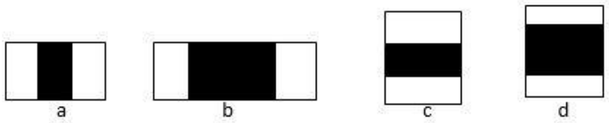


Figure 4. Liner Feature

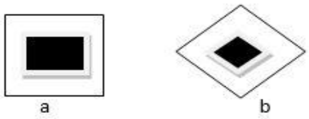


Figure 5. Central feature

These features will be carefully found and specifically detected in the captured image. If we found these features enough to detect the face then the particular face is discovered. Each feature is calculated by subtraction of the total number of pixels white in color from the total number of pixels black in color. Boosting skill is used to select the feature set for a particular object in the image for neat detection. We will obtain a group of classifiers as output which will be combined in a cascade structure to give the desired output to check the face is detected or not as shown below:

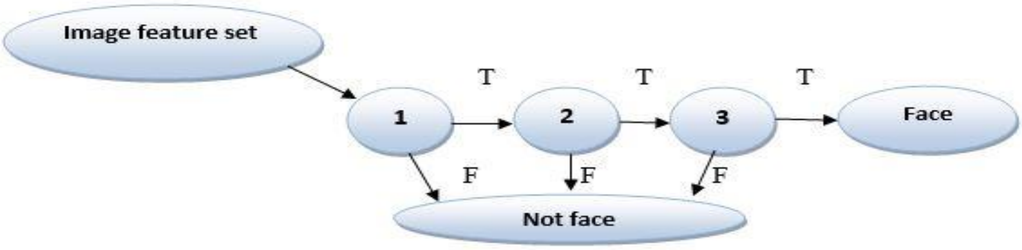


Figure 6. Cascade classifier

5.2 Face recognition process

Local Binary Pattern Histogram is a popular, simple and very effective algorithm utilized for face recognition purpose. The methodology uses a step by step procedures to analyze and identify the faces. The main method is marking pixels in an image comparing to a specific threshold value and equating it with the neighboring pixels. The result will be computed to a binary number. It was found in the year 1994 and since then has been a popular algorithm used for classification technique. It is a blend of Local Binary Pattern (LBP) with (HOG) Histogram of Oriented Gradients. They are combined together to form LBPH which improves the performance, detection rate on some dataset combination. By using the LBP combined together with histograms we are able to denote face images for huge volume of data sets. The steps of the algorithm can be depicted as following:

a) Parameters. The algorithm uses mainly 4 parameters name:

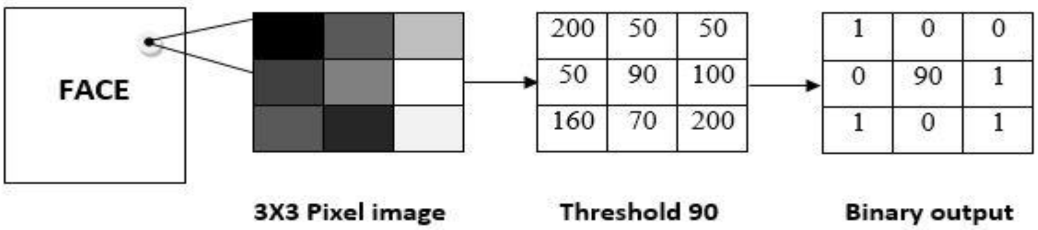
- Radius: The radius is mainly used to create the circular shape of local binary patterns. The radius represents the radius around the central pixel in an image. It’s generally set to 1.
- Neighbours: The neighbours are the amount of sample points employed to build the circular local binary pattern. Higher the sample points we include higher will be the computational cost. It’s usually set to 8.
- Grid X: It indicates the set of cells horizontally. The more number of cells the finer will the grid with higher dimension and is usually set to 8.
- Grid Y: It indicates the number of cells vertically. The additional number of cells vertically finer will be the grid with higher dimensions and it’s also usually set to 8.

b) Training: Training the algorithm is the next step. For achieving this we need to have a dataset of images to recognise. Hence a bunch of real time dataset of images will captured for training the model. Here we are setting an ID (Identification Number) for each person. The algorithm will use the id as reference to recognize the person’s image. Say we are going to capture 100 sample images of a person for training the model. All these images of the individual will contain the same id since all of them belong to a unique single person.

c) LBP process: here the initial process is creating an intermediate image. An intermediate image is produced by using the original dataset. It is created for describing and explaining actual image of a person by highlighting the main facial characteristics. Hence to do this process the algorithm mainly uses a concept of sliding window. To create the same it makes uses of the parameters considered in the step 1 i.e. the radius and neighbours.

d) Extraction of Histograms: In step 3 we obtained a LBPH image. By using this image we will generate an image using the parameters Grid X and Y to generate a pattern of histogram.

e) Face recognition: Now at this stage the algorithm is at present trained. The histograms created in the previous steps will represent the images from the training data. Hence if a fresh image is given the above steps will be processed to create the histogram which represent the original image. Here main process is to find the image which equals to the input image. Compare the respective histograms generated and output the histogram that equals very closely with the input image. There are several ways to compare the histograms. One might be to calculate the distance among the two histograms. Some common methods are Euclidian distance, chi-square distance, absolute value distance etc. The output of the algorithm will be the ID of the picture having the nearest histogram. The output of the algorithm is the distance among the two histograms which is usually referred as confidence. Lower the confidence better is the prediction. For measuring the performance of the algorithm we can use the confidence with the threshold value whether the algorithm is bale to correctly recognize the image. We can conclude that if confidence id lower than that of threshold value than the image recognized id successful.



200	50	50
50	90	100
160	70	200

1	0	0
0	90	1
1	0	1

Figure 7. LBHP Algorithm

5.3 Morse code implementation

0	— — — — —
1	●— — —
2	●●— — —
3	●●●— —
4	●●●●—
5	●●●●●
6	—●●●●
7	— —●●●
8	— — —●●
9	— — — —●

Figure 8. Morse code Table

Morse code is a unique method of encoding alphabets and numbers together as a text using a sequence of dots and dashes. Its invention was around the year 1800's by scientist named Samuel Morse. It was mainly discovered for the purpose of safe and encrypted communication from one end to another. Morse code was one of the widely used telegraphy method for communication. In Morse code each and every character will be encoded in the form a dots and dashes. The standard way of encrypting the alphabets and numbers. Here the length of a dot is nothing but a basic unit of time. Length of dash is equal to three units of time.

VI. RESULTS AND DISCUSSION

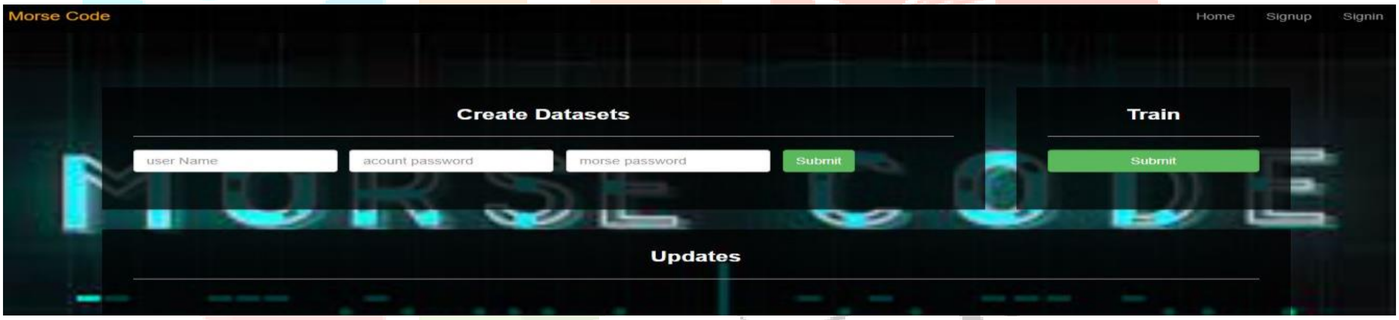
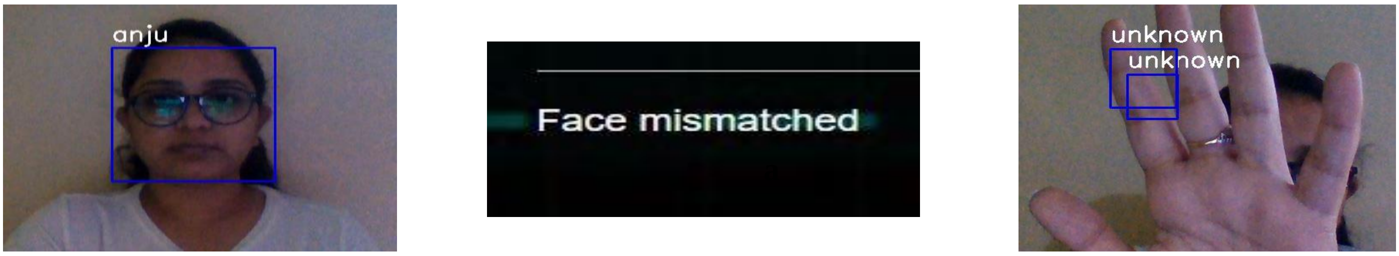


Figure 9. Registration page

Figure 9 shows a new user has to provide basic details like user name, account password and Morse password and click on submit button. This will stored in the database. Once saved we need to click on train button to train the model. The model will take 100 input images of the individual and learns the particular image belongs to the user for face recognition process.



Face mismatched

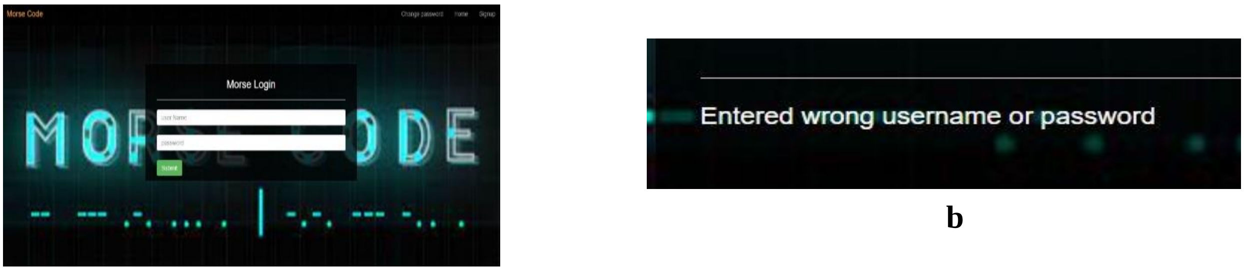
b

a

c

Figure 10. Face Recognition

Once we click on sign-in page first step of authentication will process. Takes live input and recognizes the face as shown below. In case of mismatch leads to figure b and c. In case of successful match leads to figure a.



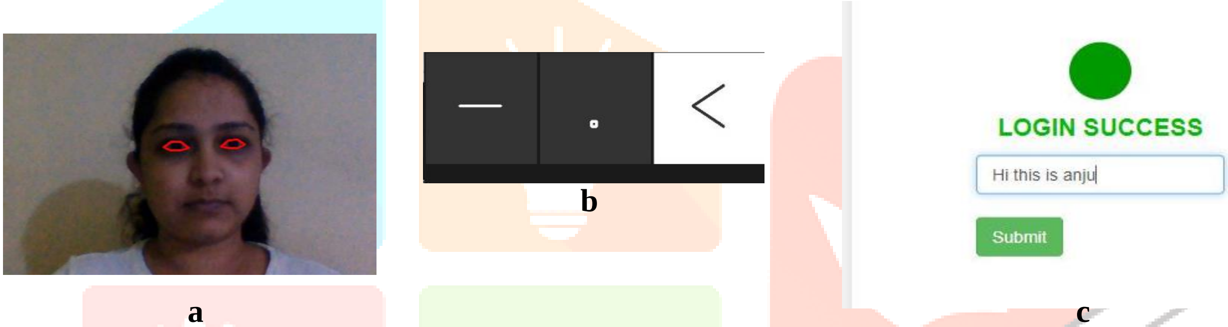
Entered wrong username or password

b

a

Figure 11. Manual authentication

Once face authentication step is successful manual authentication of username and password will be verified. In case of successful login will lead to Morse code authentication. If the entered password or username is wrong leads to figure b



LOGIN SUCCESS

Hi this is anju

Submit

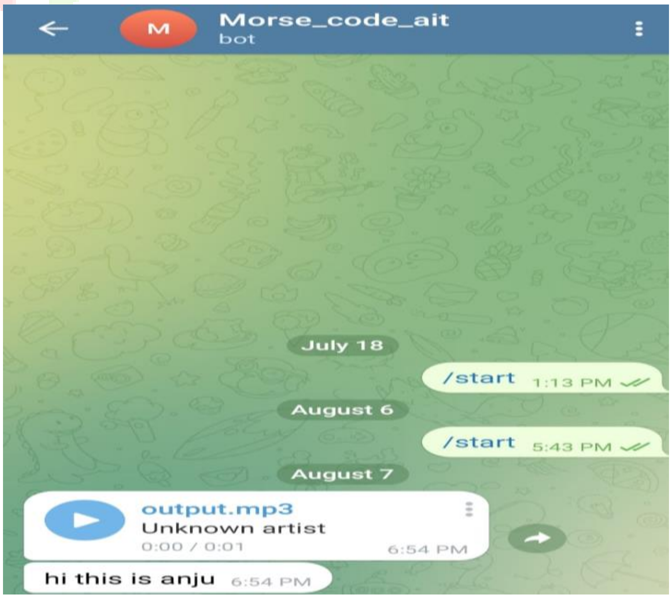
b

a

c

Figure 12. Morse code authentication

After manual authentication been successful next step is the Morse code authentication. The user has to enter the Morse password through eye blinks with the help off virtual keyboard provided in figure b. The entered password is correct will lead to figure 13 for sending an authenticated message through telegram group.



Morse_code_ait
bot

July 18

/start 1:13 PM

August 6

/start 5:43 PM

August 7

output.mp3
Unknown artist
0:00 / 0:01 6:54 PM

hi this is anju 6:54 PM

Figure 13. Telegram message

VII. CONCLUSION

The facial login with Morse code based authentication represents a unique and innovative method of login process. We are able to combine the power of computerized vision approach with the simplicity of Morse code method as a secure authentication process for successful login. Throughout the entire project we have explored and implemented various modules towards the success of facial login with Morse code system. The pre-processing module ensures whether the input face images are properly aligned and normalized for accurate feature extraction. The feature extraction module has successfully captured the essential features for face detection and recognition. The algorithms implemented such as Haar Cascade is used for face detection and Local Binary Pattern Histogram used for face recognition and Morse code used for eye blink authentication are productively carried out. The facial login through Morse code shows a great promise towards the user security and privacy of data. Our system can be implemented easily and effectively for various applications needing worthy security. As our system deals with biometric based authentication efficiently prevents unauthorized access providing a safe login. Overall our project represents a step towards more secure user authentication process. With various advancement in technology and guaranteed commitment of user's security and privacy this system has full potential to offer a seamless and simple secured user experience.

REFERENCES

[1] R. Revathy and R. Bama, 2015, "Advanced Safe PIN-Entry Against Human Shoulder-Surfing," IOSR Journal of Computer Engineering (IOSR-JCE), vol 17, issue 4, ver. II, pp. 9-15.

[2] D. Asonov and R. Agrawal, 2004, "Keyboard Acoustic Emanations", IEEE Symposium on Security and Privacy. Oakland, California, pp. 3-11.

[3] Y. Berger, A. Wool and A. Yeredor, 2006 "Dictionary attacks using keyboard acoustic emanations", Computer and Communications Security (CCS). Alexandria, Virginia, USA, pp. 245 -254.

[4] L. Zhuang, F. Zhou and J. D. Tygar, 2005, "Keyboard acoustic emanations revisited", Computer and Communications Security (CCS). Alexandria, Virgina, USA: ACM Press. pp. 373-382.

[5] M. G. Kuhn, 2004, "Electromagnetic Eavesdropping Risks of FlatPanel Displays" International Workshop on Privacy Enhancing Technologies, LNCS. Springer-Verlag: Berlin / Heidelberg. pp. 88107.

[6] M. Brooks, C.R. Aragon and O.V. Komogortsev, 2013 "Perceptions of interfaces for eye movement biometrics", 2013 International Conference on Biometrics (ICB), pp.1-8.

[7] D. Rozado, 2013, "Using Gaze Based Passwords as an authentication Mechanism for Password Input", 17th European

[8] M.Martin, T. Marija and A.Sime , 2013, "Eye tracking recognitionbased graphical authentication", 7th International Conference on Application of Information and Communication Technologies (AICT), pp. 1 -5.

[9] M. Khamis, F. Alt, M. Hassib, E.V. Zezschwitz, R. Hasholzner, A. Bulling, 2016, "GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices", CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. . . . 2156 -2164.

[10] Z. Li, M. Li, P. Mohapatra, J. Han, S. Chen, 2017, "iType: Using Eye Gaze to Enhance Typing Privacy", IEEE Infocom on Computer Communications, pp. 1-9.