Offline Voting System Using Arduino and Machine Learning

Victoria Angelina Paul [1], Kavya NR[2], Indira L[3], Kavya S [4], Praveen N[5]

[1,2,3,4]*Student, Department of Computer Science and Engineering, Cambridge Institute of Technology, Bangalore, India*

[5]*Associate Professor, Department of Computer Science and Engineering, Cambridge Institute of Technology, Bangalore, India*

---***---

Abstract – This project is about voting using Arduino and machine learning algorithm. Securing the voted data, voter's privacy, and the voting process are the main challenges of this project. The project comprises of e-voting process authentication can be done using face recognition using LBPH algorithm, finger-print authentication which enables the electronic ballot reset for allowing voters to cast their votes. Also, the voted data and voters' details will be stored in the Arduino. This project presents a system to recognize the face by a variation of LBPH. We use a method of regression of local binary features to get the landmark of face images whose computational complexity is very low. We utilize these landmark points which can be trained to align the face, to extract the facial features. By calculating the Local Binary Patterns Histogram (LBPH) of these landmark points and its neighborhood pixels, we can extract effective facial feature to realize face recognition.

Key Words: voting, landmark, LBPH, face detection, finger print recognition, authentication.

1. INTRODUCTION

In the modern era, communications and the Internet keep growing, the need for more security measures is required. Due to this, computer technology users bring the increasing need for electronic services and security. Usage of the latest technology within the voting process improves the elections to natural. The technology implemented in this paper refers to e-voting systems where the election data is recorded, stored, and processed primarily as digital information, usually, information security was used mostly in military and government institutions. But now they need for this sort of security is growing in everyday usage. It is necessary to make sure that data, communications, or documents (electronic or physical) are enough secure and privacy enabled in the fields of computing, e-services and, knowledge security. In this paper, a 2-factor authentication system is proposed where a person can vote only if his details match with the database using finger print and face detection. Face detection and recognition is not new in our society we live in. The capacity of the human mind to recognize particular individuals is remarkable. Face recognition processes images and identifies one or more faces in an image by analyzing patterns, this process uses algorithms which extracts features and compare them to a database to find a match. LBP have been well utilized for facial image analysis before. In those existing work, the LBP histograms (LBPH) are extracted from local facial area, and descript the whole face by it. Local binary patters are a type of visual descriptor used for classification in computer vision. In this paper, we propose a new method to describe facial feature by LBPH. The feature point is marked to express face by face alignment through the regression of local binary features, these feature points are called as landmarks. We compute LBP operator of these landmarks and operators surrounded with them. By comparing the LBPH between the test image and train model, can we obtain the results of face recognition. It is based on the Facial recognition technique which falls under machine learning technology. The face is recognized from the datasets that are stored in the database.

2. LITERATURE SURVEY

[1] Secured E-voting System Using Two-factor Biometric Authentication was published in 2020 in the proceedings of the Fourth International Conference on Computing Methodologies and Communication by Sudeepthi Komatineni and Gowtham Lingala. The research work proposes a secured and robust electronic voting system based on popular machine learning based facial recognition algorithms and biometric authentication methodologies for the purpose of building a secure voting system with low cost. In particular, it focuses on the potential working of face detection and recognition and bio-metric authentication namely bio-metric scan, and the implementation procedure, which improves the security and decreases the duplicate vote and fraudulent to make the system as more efficient and user friendly for everyone to use the system easily.

[2] Using Blockchain Data Security Management for E-Voting Systems was published in 2020 8th International Conference on Cyber and IT Service Management (CITSM) by Erick Febriyanto, Triyono, Nina Rahayu, Kelvin Pangaribuan and Abas Sunarya. In this era of disruption, voting methods in elections have been carried out using the system designed. But in the process, there are still some obstacles, such as the calculation of election results can still be manipulated. In the 2019 election between candidates A and B, according to the fast-counting technology, media candidate A gets the highest votes, but in electronic media states candidate, B gets the highest votes in the election. This raises the possibility of manipulation of the votes in the election. This study addresses the issues involved in delivering valid results and also authenticates the validity of voting data in the elections. The method in developing this research uses blockchain technology that can verify data from voting with a decentralized system in the election process. Decentralization on the blockchain allows each server to connect and have the same role and form a peer-to-peer networks. Data tracking is easier, and when one server is in trouble, backups are easily performed by other servers, and the problematic server is temporarily removed from the blockchain networks. The application of blockchain technology in electronic voting can produce data that cannot be manipulated and will be maintained authenticity.

[3] Machine Learning with Blockchain for Secure E-voting System was published in 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH) by

Muhammad Asaad Cheema, Nouman Ashraf, Asad Aftab, Hassaan Khaliq Qureshi, Muhammad Kazim and Ahmad Taher Azar. In order to resolve these concerns, we propose a stable e-voting system based on the principles of blockchain and machine learning algorithms. We use blockchain to ensure the integrity and security of votes, machine learning model to detect intrusion in voting data centres and e-voting systems. In the proposed model, we use the concepts of personal and public blockchain models. The personal blockchain is used for the purposes of voter registration and voting system. The public blockchain is used to maintain the integrity of the personal data of the voters by storing the root hash derived from the Merkle hash tree and revealing the results of the voting stations as soon as the voting process is completed by the voter. The proposed blockchain-based e-voting system offers transparency, treasury, confidence and prevents intrusion into the information exchange network system.

3. PROPOSED METHODOLOGY

First before a person is about to vote his details will be checked using a voter card or it may be anything. The person should register before voting. While the person is about to vote, person face will be recognized with the present data base if the face id is present in the data base it checks and next it goes with another factor of authentication i.e., fingerprint after the face id is checked fingerprint also will be checked once the fingerprint is also correct with the respective face id then the voting access for the person will be granted and the person can vote for any of the candidates. If any of these authentications is mismatched then the voting procedure will not at all happen. Hence security and also malpractice will not happen with this type of authentication system.

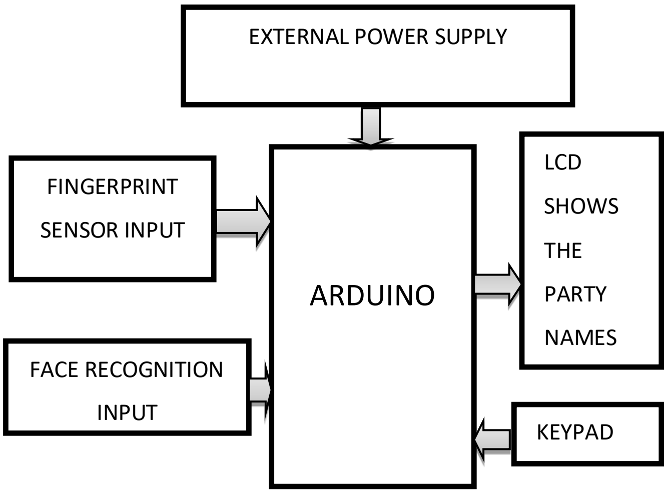


Figure 1: working of Arduino

Power supply plays a vital role in each and each device maintaining the facility to the components is that the main part within the embedded system. Here basically a primary factor authentication is formed i.e., face recognition using ML techniques in python. Then the matched face id input is given to the microcontroller using serial communication. After feeding the input to controller in LCD it displays that place finger then the person should place finger within the fingerprint sensor then the fingerprint checks with the stored data base of the fingerprint if both are matching then the person will have access for voting using keypad. In LCD it displays that no of candidates, in step with the chosen candidate by the one who is voting; vote is going to be casted and at the ultimate stage no of votes to the candidates are often checked.

4. IMPLEMENTATION

1] Face recognition- Face recognition is substantially the task of recognizing the individual based on their facial image for processing in accordance with the illumination variation, resolution, occlusion, etc. Face recognition is different from face detection.

A. Face Detection: It has the intention of detecting faces in the images which can later be used in face recognition algorithms. The face detection is an object-class detection in which the main objective is to spot and identify the objects in a particular given class. Any facial changes in the database images will eventually invalidate the matching process.

B. Face Recognition: The process is to convert the formerly extracted, cropped, and resized images to grayscale. After that face recognition algorithm is predominantly responsible for finding the specific or unique feature which best match the image. Face recognition can be carried out using two methods. • Verification compares the input image with the image that is already stored and saved in the database for the purpose of providing authentication to the users. • Identification compares the given input image with all the images stored in the dataset previously in order to find the user that matches that particular face. There are numerous face recognition algorithms that help in obtaining the image information. Each method works in its own way to match the input images with the images in the dataset. The various algorithms are: Eigenfaces (1991), Local Binary Patterns Histograms (1996), Fisher faces (1997), Scale Invariant Feature Transform (1999). The paper relies on Local Binary Patterns Histograms (LBPH) which is one of the face recognition algorithms. Local Binary Pattern is a easy and efficient algorithm which entitles the pixels of an image by thresholding each neighbor pixel and regard the obtained result as a binary number. It was first enforced in 1994 and it is used to represent each facial image with a simple data vector when it is compounded with the histograms of oriented gradients (HOG). Further the algorithm can be explained in step-by-step process as follows:

Parameters: There are four parameters used in Local Binary Patterns Histograms (LBPH). They are: -

• Radius • Neighbors • Grid X • Grid Y

A. Radius: It is used to build a circular local binary pattern which represents the radius around the central pixel. It is usually assigned to 1. B. Neighbors: It is the count of sample points that is used to generate the circular local binary pattern. It is generally set to 8. C. Grid X: It is the count of cells in the horizontal direction. The more the cells, the higher the dimensionality of the subsequent feature vector. It is generally assigned to 8. D. Grid Y: It is the count of cells in the vertical direction. The more the cells, the higher the dimensionality of the subsequent feature vector. It is generally assigned to 8. • Training the algorithm: The most important part in the algorithm is to indoctrinate the algorithm. For that we need to make use of the dataset that holds the facial images of the individual that is needed to be recognized. It is also notable that each image should be given with an ID number or name with which it is easy to acknowledge the input image and give the desired output. • Applying the LBP operation: The foremost step in this method is to generate an intervening image that describes the primary image in a better way, by highlighting the important facial features. To perform that the algorithm uses a particular concept called as sliding window that is based on two parameters which is radius and neighbors. Local Binary Pattern is an easy and efficient algorithm which entitles the pixels of an image by thresholding each neighbor pixel and regard the obtained result as a binary number. • Extracting the histograms: After the before step and using the image that is being generated already, we can utilize the Grid X and Grid Y parameters to categorize the image into multiple grids. • Performing the face recognition: This is the final step in which the algorithm is previously skilled. Each histogram that is being created is used to represent each image from the training dataset. So to find the image that matches the input image we just need to resemble two histograms and return the image with the approximate histogram. The Local Binary Pattern Histogram is considered to be one of the easiest and efficient face recognition algorithms which can symbolize local features in the images. The process is to convert the formerly extracted, cropped, and resized images to grayscale. After that face recognition algorithm is predominantly responsible for finding the specific or unique feature which best match the image. The paper relies on Local Binary Patterns Histograms (LBPH) which is one of the face recognition algorithms. Local Binary Pattern is a easy and efficient algorithm which entitles the pixels of an image by thresholding each neighbor pixel and regard the obtained result as a binary number.

2] THUMB RECOGNITION

Fingerprint recognition is the most unique biometric authentication known so far, as the ridge arrangement on every finger of every individual is unique and it will not alter although the dimensions of fingers. There is never a scenario where any two fingerprints among billions available are found similar so far. Thus a 2-factor verification using fingerprint recognition will make the system more efficient and foolproof. Out of all the algorithms available minutiae algorithm is widely used for fingerprint recognition and is described as follows:

a) BINARIZING THE FINGERPRINT IMAGE

The usual fingerprints taken from an individual are called the grey scale images with intensity ranging from 0 to 255, which makes it vivid that they aren't clear enough to mark minutiae. Hence, they are converted into binary images. A threshold value is fixed and the pixel values that fall above it are set to 1 and below it to 0 respectively which implies that the Binarized Images are more intense.

b) RIDGE THINNING

Though the Binarized image is intense it isn't thin enough to extract minutiae effectively, so it is thinned to reduce the thickness of all ridges to single pixel width using block filter. Ridge thinning doesn't alter the location of minutiae, it just places white pixels at the boundaries of the ridges of a binary image preserving the outermost pixels.

c) MINUTIAE EXTRACTION & MARKING

The ridged image is further divided into 3x3 matrices and crossing number technique described below is applied to mark the minutiae as: a) Bifurcation: In a 3x3 matrix if the central pixel and 3of its neighbors have a value of 1 then the central pixel is a branch of bifurcation.

b) Termination: If central pixel and just one of its neighbors have a value of 1 then the central pixel is a ridge ending or termination.

c) Trifurcation: If both the uppermost pixel and the rightmost pixel have a value of 1 false minutiae points are removed and left-over minutiae points are marked.

5. RESULTS

The voting system using Face Recognition and Finger Print detection consists of the following modules:

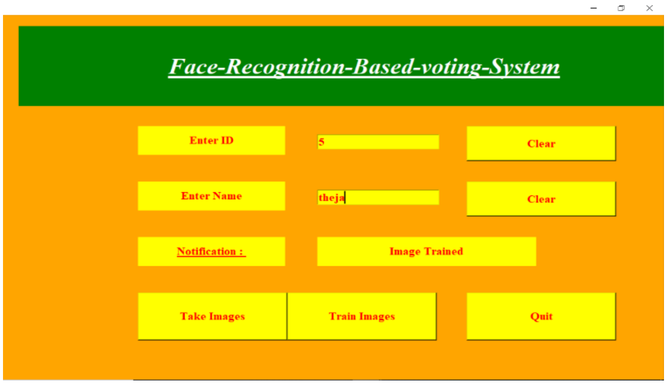
1] Voter's login

2] Face recognition portal

3] Finger print recognition.

1.Voter's login

This is the voters login page. The voter login using their ID and name.



Face-Recognition-Based-voting-System

Enter ID 5

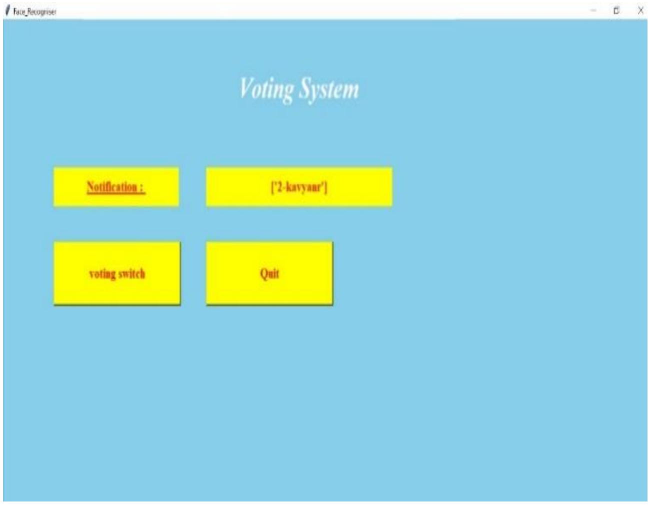
Enter Name theja

Notification : Image Trained

Figure 1- Voter's login page

2. Face recognition portal

This page recognizes the voter's image and trains the image using LBPH algorithm.



Face_Recogniser

Voting System

Notification : ['2-kavyanr']

Figure 2: Face recognition page

3. Finger print recognition

The fingerprint is given to the Arduino with the help of the finger print sensor. Then the voter's image and finger print is stored in the Arduino. The first procedure of portrait acquisition can be done by using the camera to capture the faces of the individual. In this process the system will first detect the presence of face in the capturing image, if there are no face detected, the system will prompt the user to capture their face again until it meets certain number of portraits which will be 50 required portraits in this project for each student. Then, the images will undergo several pre-processing procedures to obtain a grayscale image and cropped faces of equal sizes.

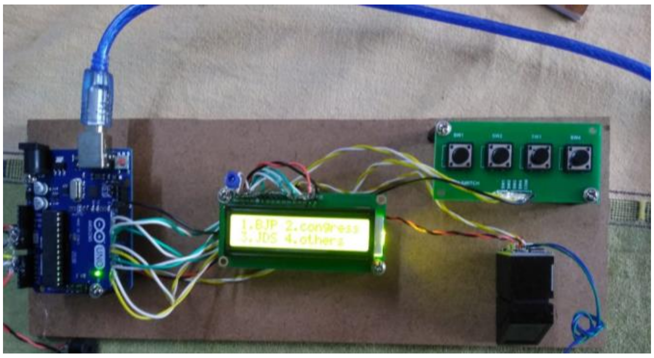


Figure 3: Finger print recognition set up

6. CONCLUSIONS

A number of these advantages are lesser cost, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. It's very difficult to style ideal e-voting system which might allow security and privacy on the high level with no compromise This project presents a system to recognize the face by a variation of LBPH. We use a method of regression of local binary features to get the landmark of face images whose computational complexity is very low. We utilize these landmark points which can be trained to align the face, to extract the facial features. By calculating the Local Binary Patterns Histogram (LBPH) of these landmark points and its neighborhood pixels, we can extract effective facial feature to realize face recognition. Future enhancements focused to style a system which may be easy to use and can provide security and privacy of votes on acceptable level by concentrating the authentication and processing section.

REFERENCES

[1] Sudeepthi Komatineni, Gowtham Lingala, "Secured E-voting System Using Two-factor Biometric Authentication". Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020) IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2.

[2] Erick Febriyanto; Triyono; Nina Rahayu; Kelvin Pangaribuan; AbasSunarya, "Using Blockchain Data Security Management for E-Voting Systems". 2020 8th International Conference on Cyber and IT Service Management (CITSM).

[3] Dana IndraSensuse; Pandu Bintang Pratama; Riswanto, "Conceptual Model of E-Voting in Indonesia". 2020 International Conference on Information Management and Technology (ICIMTech).

[4] Muhammad Asaad Cheema, Nouman Ashraf, AsadAftab, Hassaan Khaliq Qureshi, Muhammad Kazim, Ahmad Taher Azar, "Machine Learning with Blockchain for Secure E-voting System". 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH).

[5] Giovanni N. de los Santos; Jessie Richie N. de los Santos; Lorna G. de los Santos, "e-voting kiosk: A specification School-based Registration and Voting System". 2020 IEEE 12th International Conference on Humanoid, Nanotechnology, Information.