2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) | 978-1-6654-1960-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICICV50876.2021.9388405

Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN

S .JEHOVAH JIREH ARPUTHAMONI M.E.
Electronics And Communication Engineering.
Scad College Of Engineering And Technology
Tirunelveli, India
jehovah83@gmail.com

Dr.A.GNANA SARAVANAN
Professor, Electrical and Electronics Engineering
Francis Xavier Enginering College, Tirunelveli,
India
vpscad@gmail.com

Abstract: : India being a democratic country, still conducts its elections by using voting machines, which involves high cost and manual labor. Web-based system enables voter to cast their votes from anywhere in the world. Online website has a prevented IP address generated by the government of India for election purpose. People should register the name and address in the website. Election commission will collect the fingerprint and face image from the voters. The database or server will store the images. When the images are obtained on the casting day, it will be compared with database and provides a secured voting on the Election Day. System utilizes faces and fingerprints to unlock the voting system, similar to the mobile phone are used. The current system requires the physical presence of voter, which is inconvenient to many voters. The process consumes less time as well. Using the detection of face and fingerprint images, the number of fake voters can be reduced. The eyes and eyebrows distance remains constant with growing age to make the system more secure. This research work utilizes ten print image to detect the correct name of voter.

Keywords: Online Website voting, Face Capturing, Face recognition using Haar cascade, pre-processing of fingerprints iamges, Fingerprints images matching using CNN

I. INTRODUCTION

Elections are the foundation of any democracy and the true spirit of democracy lies in people choosing their own government. But, the way elections are conducted right now in our country has defects and loopholes, which are being used for the advantage of the contestants and political parties. The current system has a lot of loopholes like the possibility of duplicate votes, rigging EVMs, faking the count, all of which tampers the true meaning of democracy. Electronic machines for conducting elections in most of the places, which is quite time-consuming, energy-consumption and should be done at an assigned place. The machine has to be transported and monitored with more man power and it is expensive. The system proposed here is a solution that addresses all the aforementioned concerns. Through the Smart voting system that uses facial and fingerprint recognition, people who do not live in the same place or the old or someone, who cannot wait in long queues for a long time will be benefitted. The voter can comfortably vote from anywhere and the possibility of duplication of the vote is also reduced through the same. This Online Voting System uses Image processing to detect voter's faces by using haar Cascade Algorithm. To exact mouth, face and eyes from full face and compared with face image in database. Fingerprint image are matched by calculate the Using CNN Deep learing. CNN reduced the computational time for processing the large size image. The Training of ANN is taken long time. CNN having two stages, future detection and Classifation of image. Face and fingerprint image features are exacted and compared with the database. When it matches .The voter will allow to vote. Voter can vote to any leader in election. After it disable the other leader slots. The votes are stored in the server and the counting is finished at end of election. Clint and server commission is important for the system. The IP address is given from the government website for the election. The Counting is very easy and time taken is very less compared to the existing system. after the key information fed to the system to distinguish the eligible voters from the fake one. Importantly, the system developed is entirely web-based which is very inexpensive compared to the present systems, very less manpower will be required if proper strong cyber-security is provided to the website. The existing systems and is also, an authentic model.

II. LITERATURE SURVEY

A. Iris Detection in Voting System

The image of eyes are captured and further the Iris is detected by using the image processing technique and compared with the stored images. once it matches, the system confirms the voter to be the eligible individual to vote by checking his/her Aadhar details. Once confirmed the voter will be allowed to cast the vote.[5] As the existing Aadhar database contains all the information about voter's Iris, fingerprints and other details like address, blood-group voter can be easily tracked and checked. This approach requires less manpower and highly secure,

B. Voting System using Fingerprint Recognition

.Fingerprint is Recognition using sensor and save in database .Once the biometric image is read and the information will be sent to the web application through the microcontroller's serial port. Input image is compared with the existing image in the database or server sends the message and displays it on the LCD confirming the voter's identity. If not Matching, it displays the same as not eligible through LCD.[2]

C. Smart Voting

Information of individuals above age 18 will be taken from the Aadhar database. In the first phase, the voters

will be given an Id and password through the registered e-mail Id before the voting process. [7]The second phase is validating the voter using fingerprints data and once confirmed voter will be allowed to cast the vote. After casting, as a part of the third phase, the voter id will be deleted leaving no second chance to vote again. Aadhar details that were used by the voter will be locked to track the voter for further access. The count will be updated parallel.

D. Blockchain Based Secure Voting System using Iot.

The voting process is record in client and it is stored in the Server (5). Registered the name and address of voter in the Website and Lot is given to voter at the time of voting process. Fingerprint image is taken by using sensor and fingerprint image is compared with database images. When it match with input voter will allow to vote. Block chain means blocks of voting recorded for each voter and stored in the server.

E. Multimodal Biometrics based on CNN

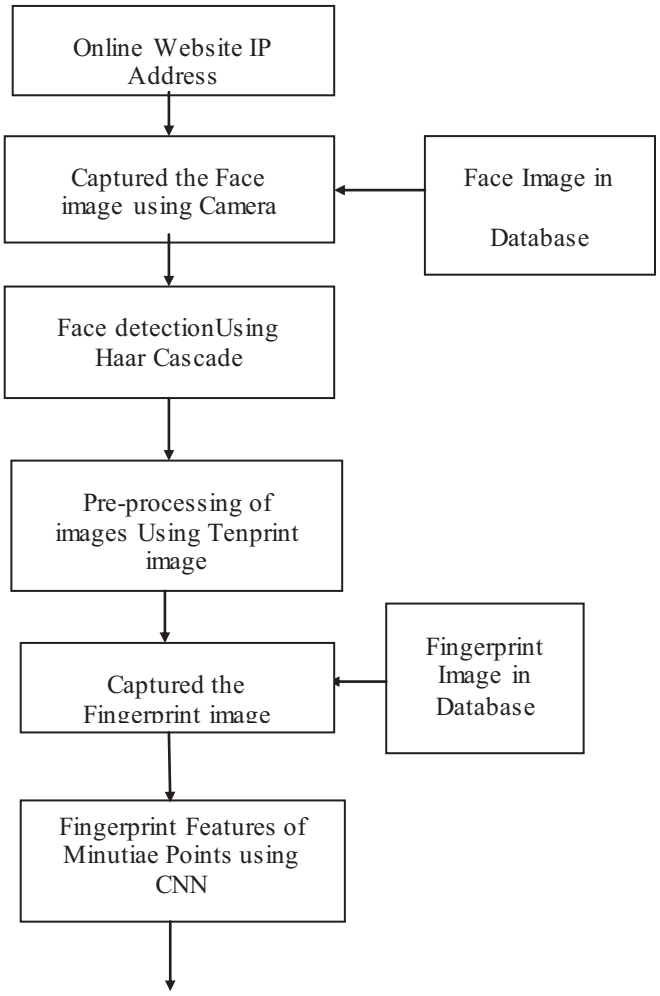
The Multimodal Biometrics recent method having the secure of face, iris and palmprint images. The features extraction of images done using Convolutional Neural Networks. The multimodal Biometrics is old method using CNN. The input image is compared with images in database using CNN .The matching of fingerprint images are also done by CNN. Two layer fusions is used in the recent CNN (8).

III. PROPOSED SYSTEM

The designed and proposed smart voting system uses face and Fingerprint recognition by using the image processing and CNN, which is more secured than the existing one. The main security level is where the system recognizes the face and fingerprint of the voter from the current database of face images and Fingerprint images given by the election commission. If the image captured matches the respective image of the voter in the database, then a voter can cast their vote in the election. Haar Cascade Algorithm is used to extract the facial features and to recognize the facial part of the image. Visual Studio and software HTML were used to create the online platform and to implement the algorithm. Minutiae based Matching method is for matching fingerprint images and image given by election commission. If the image captured is matched and voter is allow to vote.

IV. METHODOLOGY

This proposed concept is an entirely web-based system so the basic features related are web-based technologies such as database creation, image processing properties which determine the software requirement of the system. This is authorized government sites. The voters will be able to cast their votes by use of this website. Eligible voters will be allow after by facial and Fingerprint recognition. The voter will open the website on the day of elections. The server stored fingerprints and face images fron the Election Commission authorizes. The voters can open the website with IP address provide. open the website and click on the vote button, the voter's face and fingprints will be captured with the help of whatever device they are using the website from like a laptop, PC or their mobile camera. The captured image will then be received by the server. The server goes through all the images in the database and tries to find a match in the registered ones. If a matching face and fingerprints is found, the voter is registered and recognized by the election commission and hence is allowed to vote. Face detection is done by Using Haar Cascade algorithm.If a match is not found, the page will say voter is not recognized and would not be allowed to vote.the fingerprint image is saved in the server ,when the fingerprint images are same. The ten fingerprint image are taken and position of tenfinger, count are calcaulated. After comparing the two images we can find out the correct voter fingerprint. Fingerprint image matching is done by comparing input and with image stored in database using CNN. The images matched will be displayed along with their ID numbers and the voting page where voter can vote to any political party they prefer from the list of voter options displayed. They click on their preferred party, the choice cannot be changed and the rest of the options will be disabled as well. The server accepts the votes cast by the authenticated voters and stores them. The count of how many votes each political party's candidates will be stored as well. This way even the counting of votes is very easy and the mission or the candidates or the voters do not have to wait for days to know the results.



Voting

Fig.1 Methodology of the System

V. FACE DETECTION USING HAAR CASCADE

Face detection, object detection algorithm used to identify objects in an image or video. The algorithm is trained to detect a face by Haar features-sequence of square-shaped functions. Then it uses classifiers to detect the face (1) and not a face (0). This face detection happens in four stages. The first being, detection of Haar features, using integral images, third stage is Adaboost and fourth is the cascade of classifiers.

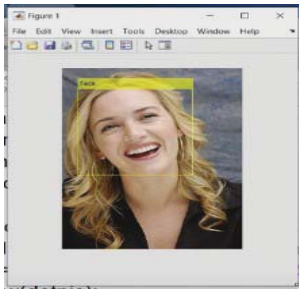


Fig.2 Face Detection

A. Detecting Haar features

Before Haar features, image pixel intensities were used for face detection which is a lot of effort and work,sed Haar wavelets which detect faces taking smaller subsections of a face at once into consideration compute sum of their pixel intensities and then difference between these sums. For black and white image pixels, we have normalized greyscale.

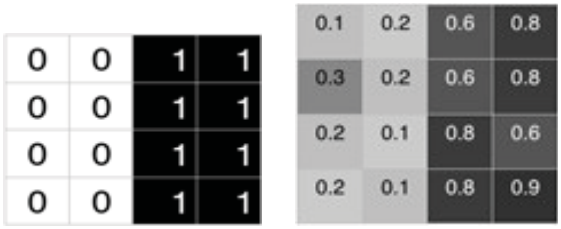


Fig.3: Pixel intensities of detected Haar-features (a) ideal case (b) real case.

Detecting Haar feature in the image

$$\Delta = \frac{1}{n}\sum_{dark}^{n} I(x) \frac{1}{n}\sum_{white}^{n} I(x)$$ Eq. (1)Ideal case: Δ = (1/8)*(8) — (1/8)*0 = 1

Real case: Δ = (1/8)*(5.9) — (1/8)*(1.3)=0.575

Haar features are very effective in detecting rectangle features, thereby making it a very functional face detection technique. The figure 3(b) below can be an eye. The darker region being the eye and the lighter region corresponding to the cheek part of the face. As eyes are the darkest parts of the face compared to the rest of the face usually in the grey scale images or otherwise, they are detected first. Another example is figure 3(a) could be the bridge of nose is usually elevated and is darker than the cheek part of the face. This is how Haar features at detecting lines and edges detect the face or subsections of the face first.

(a)

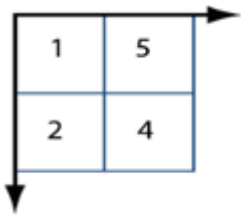
(b)

(c)

Fig. 4: Some common Haar features (a) Nose (b) Eyes (c) Mouth

B. Integral images

A huge amount of features are returned by the above computation. To decide, what features should be taken into consideration, integral images are used. It is a specialized algorithm designed to generate the sum of values in a rectangular subset of a grid.The summations of pixel intensities within a window. when a certain window is chosen, this algorithm computes cumulative sum of the pixel intensities row-wise and column-wise, which reduces the number of operations that have to detect is a window is useful or not. The part of the face we need to detect. If we consider the below given boxes as a subset of a face where the numbers are pixel intensities, we have to do 1+5+2+4 for the left side table, which is 12. Whereas, on the right, we have a table with cumulative sums, row-wise and column-wise, here all you have to do is 12+0-0-0, which is equal to 12. We have considered a simple computation here, but with increasing sizes of subsets, the computation using integral images are much faster, less time-consuming and effective.



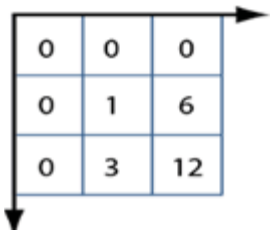


Fig.5: The generated subset of a grid. (a) input image (b) integral image

C. Adaboost

Besides being numerous, features might also be irrelevant. Feature that is part of the face. Adaboost both selects the best features and the weak ones and trains the classifiers that use them. 'Strong' classifier is constructed and weak' classifiers by the algorithm. Here a strong classifier means one which has less error rate, one which will definitely be a part of the face and a 'weak' classifier are have less than 50% error rate so we know that it mostly will be a feature that belongs in the face region. Therefore, we use Adaboost to combine these weak classifiers into on strong classifier that will lead to the detection of a face.

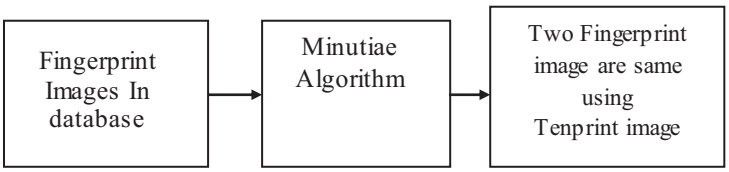
D. Cascade of classifiers

In an image, there are face-regions and non-face regions. The features that are detected from subsections into different stages of classifiers. We don't consider the remaining features in it. The second stage of features will be applied and the process is continued only if it passes the first stage. Required face region is the window that passes every stage. Cascade is used so as to save time, energy and effort windowthrougha all the stages. The window will only it has a detected the face feature. The cascade of classifiers does not belong in the face region,The stages combine to form one big window which results in the face that is being detected.

VII. PRE-PROCESSING USING TENPRINT IMAGE

When the two fingerprint images are same we can use Tenprint image method. Tenfingerprint images are taken and features'are recorded for each fingerprint image in the database. In this section we will discuss these attributes in turn, leaving the discussion of minutiae attributes to its own subsequent section. When the fingerprint of two person are same and records value are equal. The tenprintimage mate minutiae records along with all image records in this database have been assigned a physical finger position. two voter fingerprints are same, minutiae features are recorded. These features include points in a finger's friction called a ridge ending. The ideal minutiae on the tenprintimage mate were initially detected by an automatic AFIS system. Combing of ten fingerprint image and features are recorded by minutiae points ,compared the two features of fingerprint images detected and which is belong to correct voter.

Block Diagram of Tenprint image



Tenprint image Algorithm:-

Step 1: Input-
We are taken the input image
Step 2: Binarization of Image :
Gray image is converted to binary image
Step 3:Thinning of image:
To eliminate the redundant pixels and training algorrithm
Step 4: When two fingerprint images are same in the database. We apply tenprint images.
Step 5: Ten fingerprint images are taken, position of fingers, record and count are determined
Step 6: Latent image is compared with the Tenprint image in the database

VIII. *FINGERPRINTS RECOGNITION USING MINUTIAE CNN deep learning*

Fingerprints of voter can taken by sensor and stored in the sever database. Input fingerprint is compared by the fingerprint given by the election commission. Fingerprint recognition can be a verification of Fingerprint. Thevote of a person verification using his fingerprint. MinutieaPoints and Matching of Fingerprint. Machine learning is differ From Deep Learning. Machine is taken long time to training ,But Deep Learning is finite duration and less than machine Learning

Fingerprint images Matching with minutiae CNN:-

1. The fingerprint is scaned using sensor and stored in the database. Another input is given to CNN, it compares two fingerprints and given the Features of images.

2. CNN determine minutiae points in Dv=(S1,S2)

3. Fingerprints match also done in CNN by comparing of Fingerprints minutiae points of Dv.

Basics of CNN:-

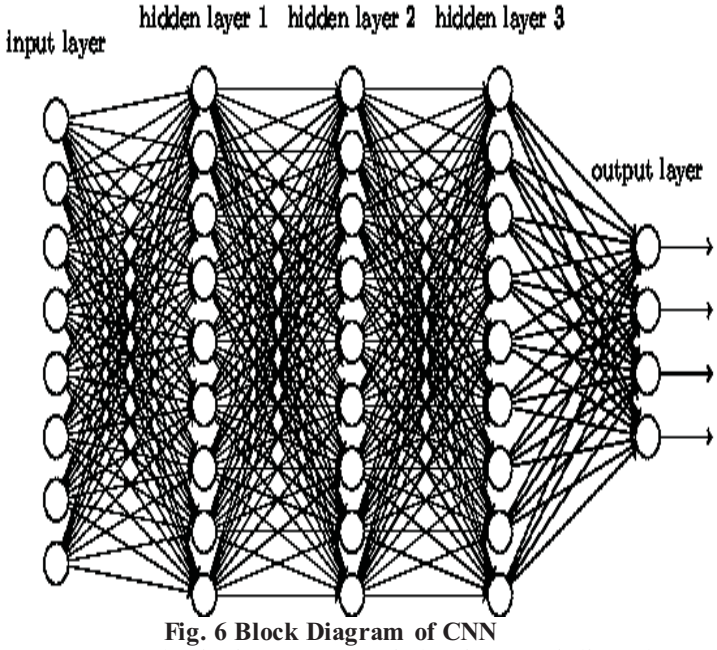


Fig. 6 Block Diagram of CNN

- CNN contain the layer of convolution layer and filters, it combined with ANN

- Convolution neural Network decreased the computional speed of large image is reduced.
- Input image size is 128*128, at output of filters 5*5 image size
- ANN is also trained algorithm with weights and it taken several minutes
- CNN is trained and it taken small duration than ANN.
- CNN is given the results of feature exaction of fingerprint image.
- Image segmentation, edge detection, fingerprint matching And Features image can exacted Using CNN.
- Convolutional of 5*5 pixels are filtered through filter with 3*3 pixels and form as 4*4 pixels

IX. VOTING

The voting page where he or she can vote to any political party they prefer from the list of options displayed. Once they click on their preferred party, the choice cannot be changed and the rest of the options will be disabled as well. The authentication are face detection and fingerprint matching secured voting system.The server accepts the votes cast by the authenticated voters and stores them. The count of how many votes each political party's candidates will be stored as well. This way even the counting of votes is very easy and the mission or the candidates or the voters do not have to wait for days to know the results.

X. RESULTS

An online website is created using HTML and all the software codes are implemented using Visual Studio. The designed system is superior to the existing systems and is highly secure. The CNNalgorithm used makes the system unique and efficient. It makes sure that the voter is validated before the voting process. By using the Smart Voting System the count of fake votes automatically reduce and may cease to occur and also makes the whole voting and counting of the votes easier, energy-efficient, accessible and more secure. Secure network can reduced Wrong votes. Required man power can be reduced by online voting system.

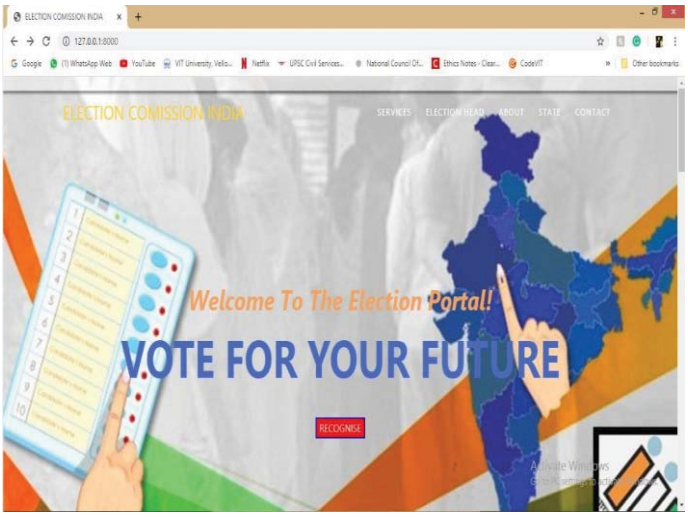


Fig.7. website for voting where face recognition using live camera

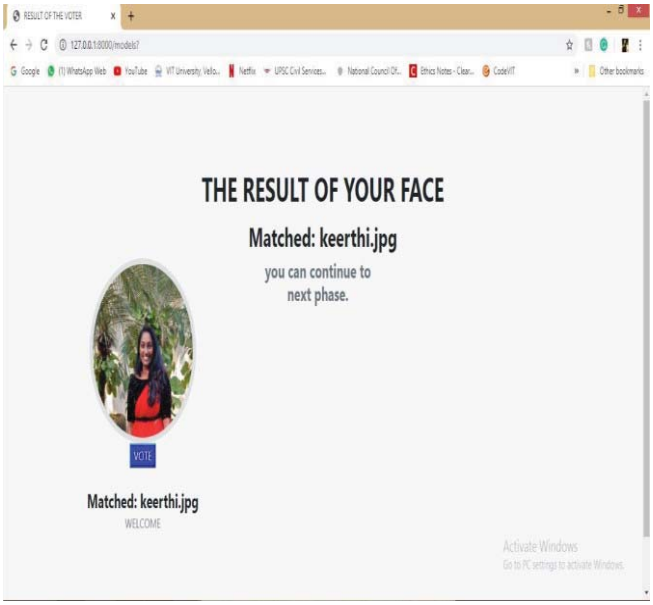


Fig. 8 Result of face detection in realtime

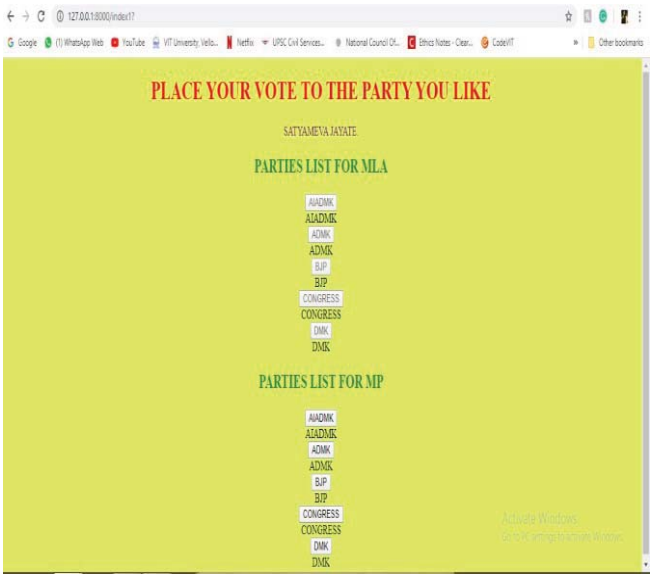


Fig.9. the page where voting for preferred political party takes place

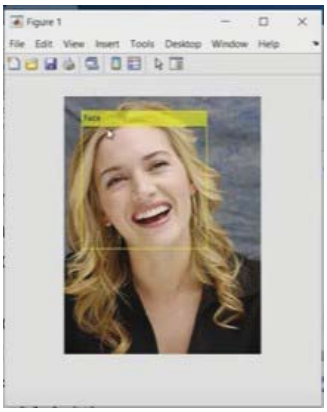


Fig10. Face detection results

Fig 11. Mouth detection

Preprocessing results

Fig. 12 input of Fingerprint image

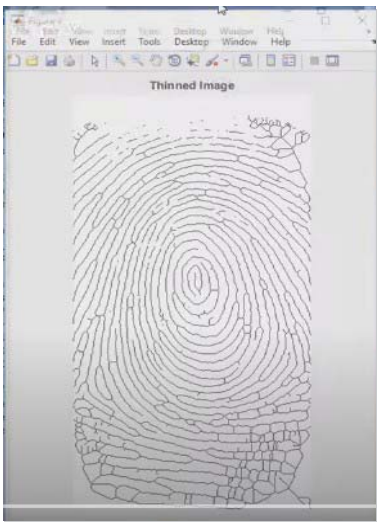


Fig.13 Thinned images

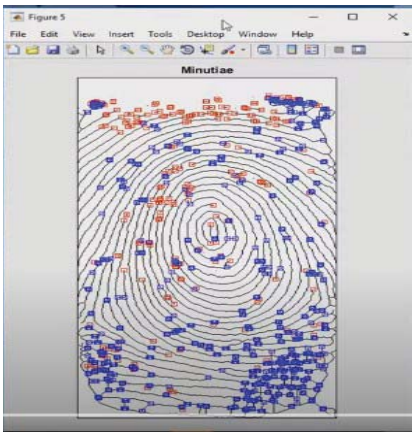


Fig14. ***Minutiae Results***

X. PROSPECTIVE IMPROVEMENTS

We could add more layers of security by adding verification of unique identification numbers like Aadhar card,Plam and eyes verification could be voter ID number. Finger print verification can also be included besides face recognition if Aadhar database is connected as it has iris and fingerprints connected to Aadhar number. This entire system would be more efficient and accessible as an IOS or an android application.OTP generation can also be a part of the verification system if the voting app is made. Then the face recognition can happen with the phone camera itself. OTP generation can also be a part of the verification system. Algorithm can changed and performance also so varied. Time of compute can varied by training of algorithm

XI. CONCLUSION

This Journal discusses which is more secure and efficient than the existing system. Time taking, vote is less than the old system, bogus voting. Unique features like the distance between the eyes and eyebrows never change regardless of aging. Fingerprint features cannot be changed, but they can same for two members. But we can detect the database image which voter fingerprint is that using Tenprint images of minutiae records .The designed system is also less time-consuming, inexpensive and a hassle-free way of conducting the election process, making smart voting a better way to vote.

XII. REFERENCES

[1] Chandra Keerthi Pothina, Atla Indu Reddy"**Smart Voting System using Facial Detection"**IEEE Journal, April 2020.

[2] Anurag Chowdhury, Simon Kirchgasser, Andreas Uhl, Arun Ross "**CNN Automatically Learn the Significance Of Minutiae Points for Fingerprint Matching?"**IEEE Conference, Mar 2020.

[3] Samarth Agarwal, Afreen Haider, "**Biometrics Based Secured Remote Electronic Voting System".** IEEE Conference, Sep 2020.

[4] Suresh Kumar, Tamil Selvan G M, "**Block chain Based Secure Voting System Using Lot"**, IEEE Journal, JAN 2020.

[5] Hanzhuo Tan, Ajay Kumar, **"Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching"** IEEE Conference 2020.

[6] Chengsheng, Yuan, Zhihua, Xia, "**Fingerprint Liveness Detection using an improved CNN with image Scale Equalization"** IEEE Journal 2019.

[7] Hui Xui, Miao Qi, "**Multimodal Biometrics Based on Convolutional Neural Networks by Two-Layer Fusion**" IEEE Conferences 2019.

[8] Abdelleratif EI Idrissi, Youssef El Merabet, "**Plamprint Recognition using state-of the art Local texture descriptors**." IEEE Conferences 2020.

[9] Uttam U. deshpande, V.S. Malemath, "**A Convolution Neural Network-Based Latent Fingerprint Matching Using the Combination of Nearest Neighbor Arrangement Indexing"** IEEE Conference, JAN 2020.

[10] Giulia orru, Roberto Casual, "**LivDet in Action Fingerprint Liveness Detection Competition**" IEEE Conference 2020.

[11] Chengsheng Yuan, Zhihua Xia, "**Fingerprint Liveness Detection using an improved CNN With Image Scale Equalization"** IEEE Conference, JAN 2019.

[12] Al Takahashi, Yoshinori Koda**, "Fingerprint Features Extraction by combining Texture Minutiae, and Frequency Spectrum using Multi -Task CNN"**, IEEE Conference, Oct 2020.

[13] Ayushi Tamrakar, Neetesh Gupta, **"Low Resolution Fingerprint Image Verification using CNN Filter and LSTM Classifier"** IEEE Confernce, Jan 2020.

[14] Ishank Geol, N.B.Puhan**, "Deep Convolution Neural Network for Double-Identity Fingerprint Detection",** IEEE Conference 2020.

[15] Maliha Khan, Rani Astya, **"Face Detection And Recognition Using Opencv"** IEEE Conference 2020.