IJARnD
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume3, Issue3)
Available online at: www.ijarnd.com

Electronic Voting Machine with Facial Recognition and Fingerprint Sensors

Jaison Isaac Prince P[1], Kishoritha K. R[2], Ganesh B[3], Gokulprashanth P[4], Dr. G. Udhayakumar[5]

[1,2,3,4]*Student, Valliammai Engineering College, Kattankulathur, Tamil Nadu*
[5]*Associate Professor, Valliammai Engineering College, Kattankulathur, Tamil Nadu*

ABSTRACT

In this project, an attempt has been made to the development of an authenticated electronic voting system using fingerprint and facial images. The two-fold authentication system improves the security of the voting process and reduces the chances of a corrupt election process. The facial recognition process utilizes the Local Binary Pattern Histogram and Support Vector Machine process to scan, store and recognize faces efficiently. The fingerprint recognition involves the capturing of multiple 2D images and High Sensitive Pixel Amplifier to improve the quality of those images to scan the fingerprint to provide the primary form of authentication. Visual Basic is used to develop a very easy to use User Interface that enables an easy voting process. A private server is used to store both the user data and the election results separately. This reduces the chances of external manipulation of the election results.

Keywords: *Fingerprint, Local Binary Pattern Histogram, Support Vector Machine, High Sensitive Pixel Amplifier, Histogram of Oriented Gradients.*

1. INTRODUCTION

The simple and cold truth is that everyone hates the problems and security flaws that are glaring at everyone's face. They are so apparent to ignore, as many witnesses these flaws straight on. Some of these flaws can be easily corrected and that is the main objective of this project, to rectify the flaws that can be rectified [3]. To list some of these so-called flaws, are a polling of proxy votes, polling of illegal votes, polling of votes under a stolen identity, external manipulation of the voting process pre and post-election, improper counting of votes Electronic voting is both electronically casting a vote and an electronic means of counting votes. In our project, we are giving importance to the authentication process of our designed voting machine. The securities that are provided will totally eliminate the fraud in the voting system. As a total number of fraudulent votes that are cast are considerably reduced, the probability of obtaining a stable and working government is increased manifold. Also, due to the implementation of immediate and Name-wise counting, there arises a possibility of finding out the number and the names of the non-voters who failed to cast their votes. When this data is utilized properly to penalize the non-voters, a future where almost a hundred percent or the complete casting of votes can be achieved which also increases the chance of a proper government. Also due to this, there is very minimal possibility of manipulation by external forces pre and post-election. When these elements are considered together, a nearly working voting system can be developed. Upon the elimination of these flaws, we can safely entail a safe and secure voting process, which results in the establishment of a stable and working government. The main objectives that are encompassed within this project are listed as, Fingerprint Confirmation as the Primary form of Verification, facial Recognition as the Secondary and Final form of Verification, two memory implementation for the prevention of manipulation, easy to use and an inviting UI for the better understanding of the voting process.

2. METHODOLOGY

The order of execution of the project requirements is done so as to achieve an optimal solution within the shortest possible timeframe. The overall workflow is such that the most difficult to execute is done first and foremost, and the easiest is done at the last. This is so that, enough time is available for the testing process and some additional time, in the case of sudden, unprecedented emergencies [1]. The overall workflow can be classified into two phases; they are the Development Phase and the Testing Phase. In the development phase, the design of the circuit, purchasing of the components, developing the security detail, final integration of all the details into one and fabrication of components to make the final product look appealing is completed. Secondly, the testing phase involves the testing of the final, finished product for the various contingencies and areas of problems. When these tests are carried out, faults and defects are found out and they are rightly corrected.

3. FLOWCHART

The overall flow of the project can be illustrated and understood from the below flowchart

ACQUISITION

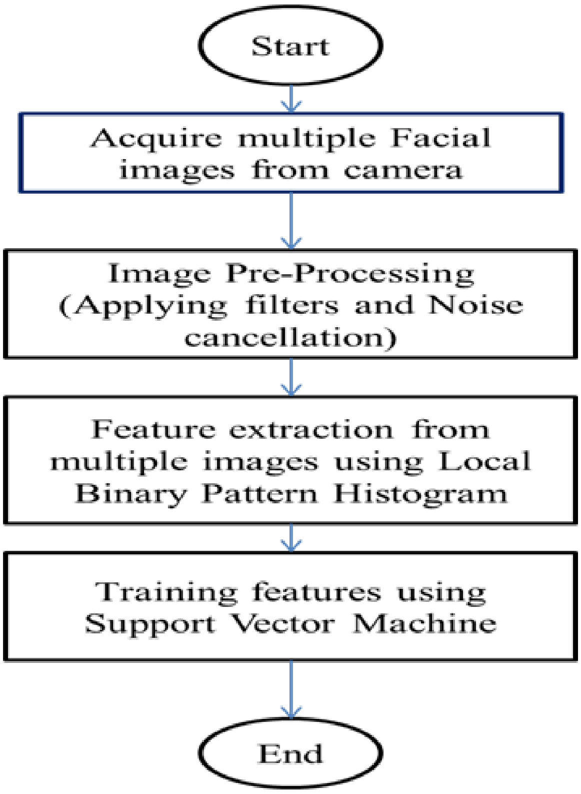

Start
Acquire multiple Facial images from camera
Image Pre-Processing (Applying filters and Noise cancellation)
Feature extraction from multiple images using Local Binary Pattern Histogram
Training features using Support Vector Machine
End

Figure 1.1

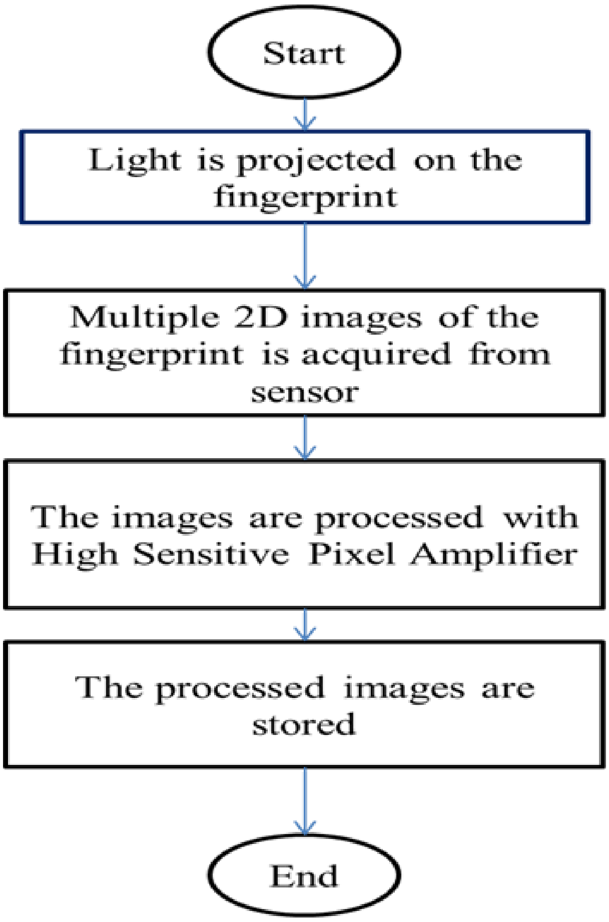

Start
Light is projected on the fingerprint
Multiple 2D images of the fingerprint is acquired from sensor
The images are processed with High Sensitive Pixel Amplifier
The processed images are stored
End

Figure 1.2

AUTHENTICATION

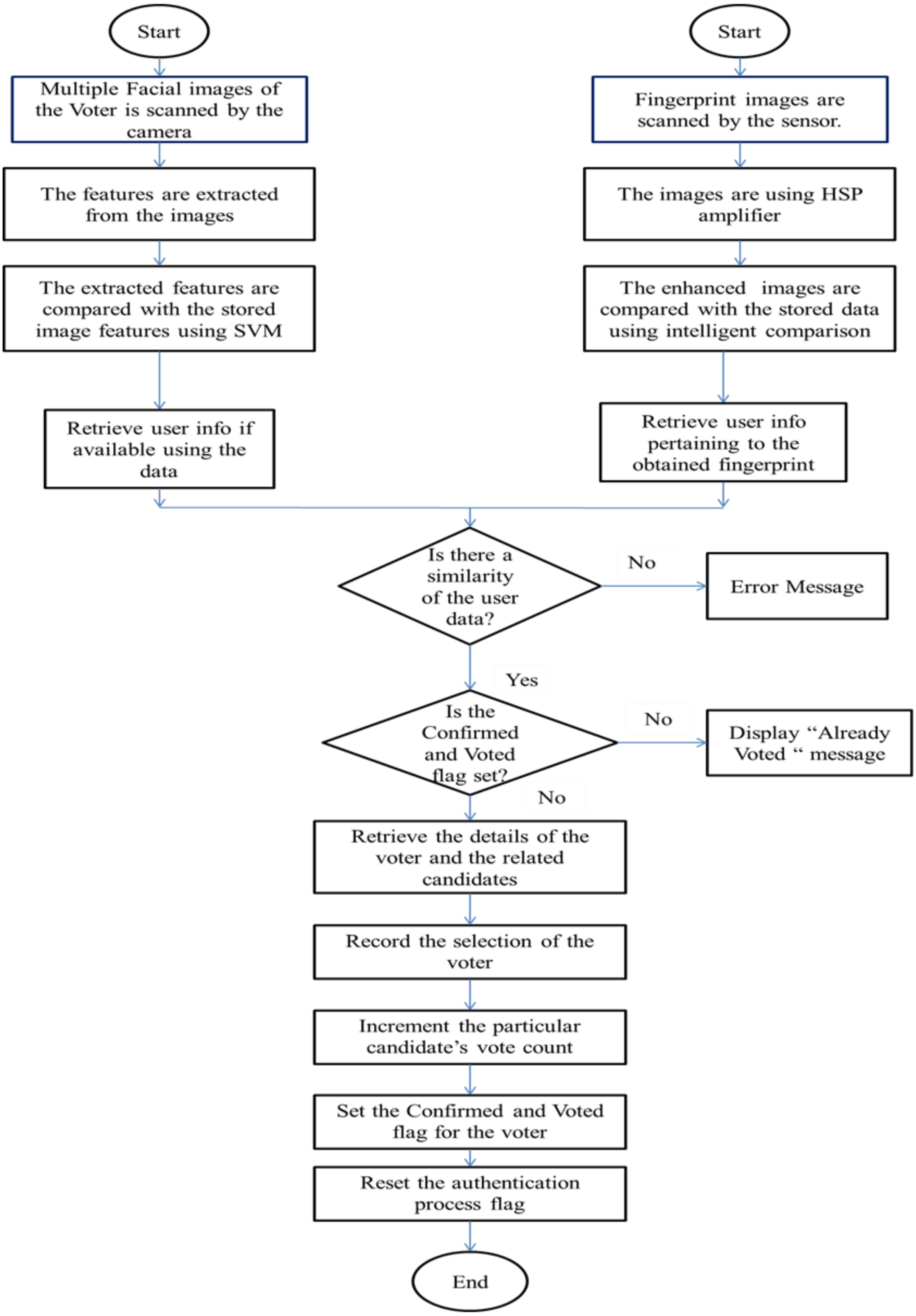

Start
Multiple Facial images of the Voter is scanned by the camera
The features are extracted from the images
The extracted features are compared with the stored image features using SVM
Retrieve user info if available using the data
Start
Fingerprint images are scanned by the sensor.
The images are using HSP amplifier
The enhanced images are compared with the stored data using intelligent comparison
Retrieve user info pertaining to the obtained fingerprint
Is there a similarity of the user data?
No
Error Message
Yes
Is the Confirmed and Voted flag set?
No
Display "Already Voted " message
No
Retrieve the details of the voter and the related candidates
Record the selection of the voter
Increment the particular candidate's vote count
Set the Confirmed and Voted flag for the voter
Reset the authentication process flag
End

Figure 1.3

4. WORKFLOW

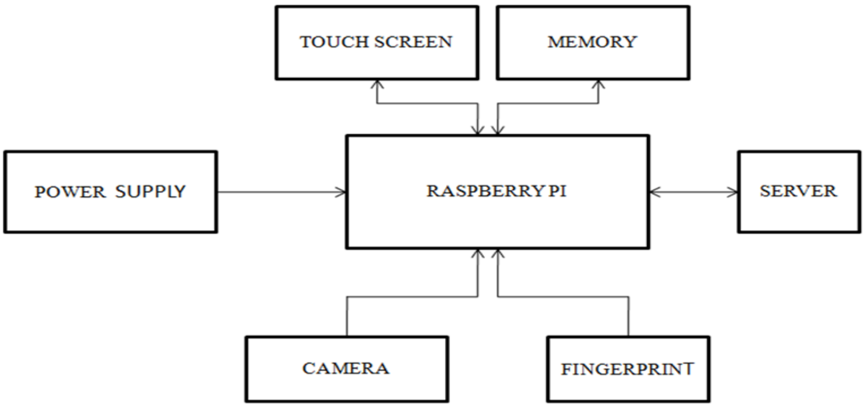
From the above flowchart, the work flow can be easily understood. First, the entire workflow is classified into two stages. The first being the acquisition phase, and the second being the authentication stage. Figure 1.1 and Figure 1.2 represent the two parts of the acquisition stage. When we look at the first figure, here the multiple images of the user's face is collected and they are pre-processed. This pre-processing stage involves removal of unwanted noise and filtering out the background noise, so as to improve the overall quality of the image. Then using LBPH, a technique that processes data or images into tiny cells that contain some information, the features are extracted [23]. SVM, a technique that points the information of each cell in a specific point in space, is used to pre-position the points of the features information. The second figure is the acquisition stage of the fingerprint sensing [19]. Here, first, the fingerprint of the user is illuminated. Then a series of multiple images of the fingerprint is captured as in the face recognition. But instead of LBP, here the images are further enhanced in details by passing them through a High Sensitive Pixel Amplifier (HSPA) [21]. Then these processed images are stored for later retrieval. Now, the third and final figure, Figure 1.3 represents the second phase that is the Authentication Phase. In this phase, the primary authentication process, i.e., fingerprint verification is done by capturing new images of the user’s fingerprint and comparing them with the stored data in the memory. Here too, the images are enhanced using HSPA. If the fingerprint is available in the database, then the corresponding user data is retrieved. The secondary authentication, i.e., facial recognition is done by capturing a series of images and then training the features via SVM after their extraction. The trained feature details are compared with the SVM data in the database. If a face with the similar facial features exists, the user data corresponding to that face is retrieved. Now user data retrieved from both the primary and the secondary authentication processes are compared. If they are similar, then the next step proceeds as planned, else the system is programmed to throw out an error message, stating that there is a mismatch of user data. In the next step, the system checks if the Confirmed and Voted flag are set for the user. If the flag is set, it means that the user has already voted and therefore the application exits and resets while throwing out an error message [15]. If it is not set, it means that the voter has not yet cast their vote and so they are allowed to cast their vote. In the next step, the candidate information related to that particular voter is retrieved and they are displayed on the screen. As soon as the voter reaches a decision, he cast his vote selecting the respective candidate. The overall vote of that candidate is incremented by one while the Confirmed and Voted flag are set for this particular voter. Then the authentication process flag is reset and the whole process is repeated again.

5. TECHNOLOGIES AND TOOLS USED

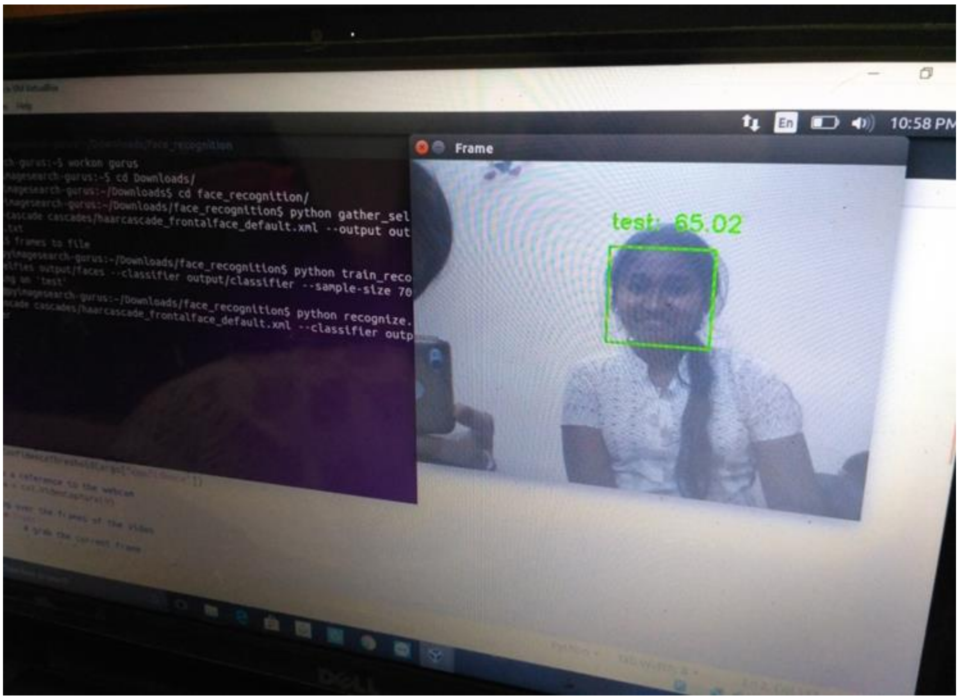
The various technologies used are selected such that they are compatible with one other and have no interfacing problems. Also, they must fall within the budget limit such that compromises shall not be made. The different technologies and tools used are listed below Python Development Environment, Linux Interfacing Engine and, Visual Basic. The PDE is used to develop the working program for the verification devices and the LIE is used to convert it to Linux compatible code. Here, a development environment is a combination of a text editor and the Python interpreter. The text editor allows you to write the code. The interpreter provides a way to execute the code you've written. A text editor can be as simple as Notepad on Windows or more complicated as a complete integrated development environment (IDE) such as PyCharm which runs on any major operating system [18]. An application programming interface (API) is a set of specifications that define how one piece of software interacts with another, particularly an application program with an operating system. A primary purpose is to provide a set of commonly-used functions, such as to draw windows or icons on the screen, thereby saving programmers from the tedium of having to write code for everything from scratch [20]. The PDE is used to develop the working program for the verification devices and the LIE is used to convert it to Linux compatible code. The capacitive fingerprint sensing is the type of fingerprint sensor used in the project. Instead of creating a traditional image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. The charge stored in the capacitor will be changed slightly when a finger’s ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which can then be recorded by an analogue-to-digital converter [17]. Local binary patterns is a type of visual descriptor used for classification in computer vision. LBP is the particular case of the Texture Spectrum model proposed in 1990. LBP was first described in 1994. It has since been found to be a powerful feature for texture classification; it has further been determined that when LBP is combined with the Histogram of Oriented Gradients (HOG) descriptor, it improves the detection performance considerably on some datasets. In machine learning, support vector machines (also, support vector networks) are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier. An support vector machine model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall [22]. The facial recognition uses Local Binary Pattern Histogram and Support Vector Machine algorithms for its functioning. Finally visual basic is used to develop the user friendly user interface of the project.

6. RESULT AND DISCUSSION

The working of this model is very straightforward and very easy to understand. First, the fingerprint reader scans the fingerprint of the voter and sends the output to the microcontroller. The microcontroller then pairs the scanned data with the data in the database and retrieves the information about the voter.

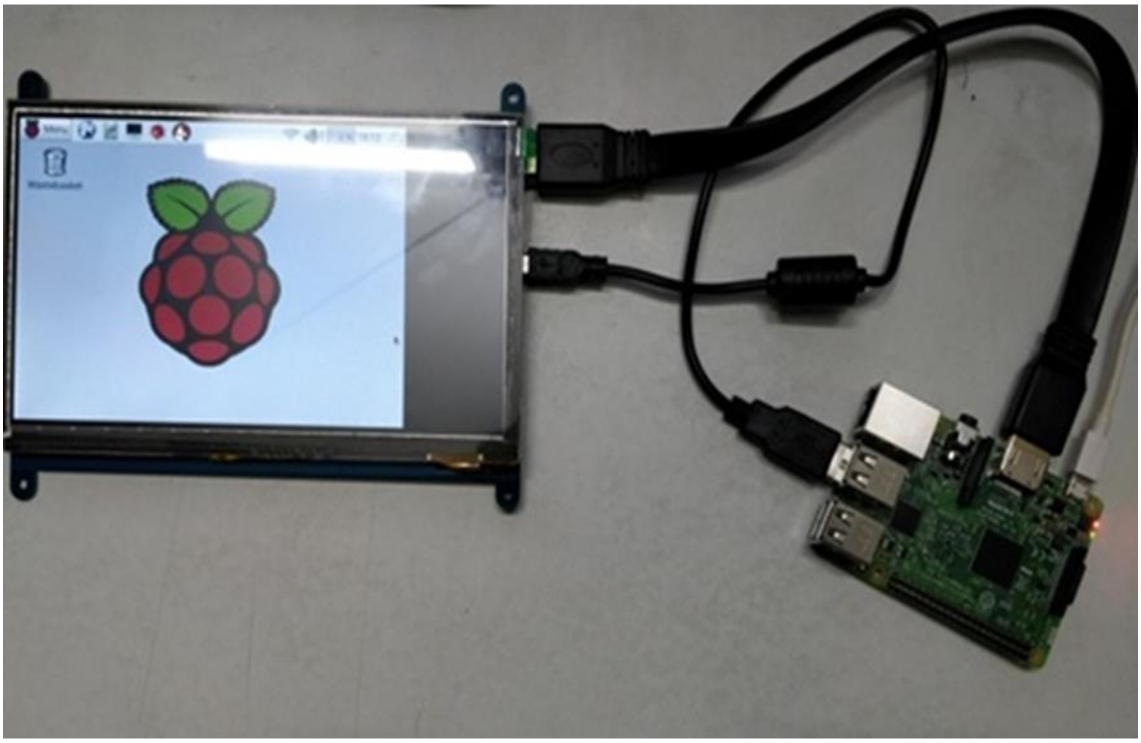


Now, the camera scans the face of the voter and checks whether it is similar to the face of the voter’s face data that is paired with the fingerprint [11].



```
ch-gurus:~$ workon gurus
imagesearch-gurus:~$ cd Downloads/
imagesearch-gurus:~/Downloads$ cd face_recognition/
imagesearch-gurus:~/Downloads/face_recognition$ python gather_sel
-cascade cascades/haarcascade_frontalface_default.xml --output out
.txt
5 frames to file
pyimagesearch-gurus:~/Downloads/face_recognition$ python train_reco
elfies output/faces --classifier output/classifier --sample-size 70
ng on 'test'
pyimagesearch-gurus:~/Downloads/face_recognition$ python recognize.
scade cascades/haarcascade_frontalface_default.xml --classifier outp
```

If it does not hold true, the process ends there with an error message but if it checks out, then the next step is carried out. Now the CPU displays the candidate details, in the area that is related to the voter, in a touch display. The voter then goes through the details and when he finalizes the candidate he want to cast his on, he then makes the selection on the display. Now is when the server comes into the picture. Now the voter has a verified and completed status on his ID and the vote count of the candidate is incremented by one.



This data is stored both on a local memory and is also sent to another separate memory through an external server [20]. When the counting process begins, both the local data and the server data are compared to check for any manipulations. If the data don't match, then that shows signs of external manipulations and necessary actions can be taken on that [24]. Also, after the election is over, the overall voter - database can be retrieved and the persons without the verified and completed badge can be penalised and shown some tough love o encourage them to vote in the next election. This increases the number of voters gradually.

7. CONCLUSION

There are many fraudulent and illegal activities that are happening in regards to the current voting process. With these problems in mind, the electronic voting machine is developed with fingerprint and facial recognition. This dual authentication system reduces the chances of the above mentioned problems and so it has improves the security and efficiency of the voting process.

8. REFERENCES

[1] Phillips, P., Grother, P., Micheals, R.J., Blackburn, D.M., Tabassi, E., Bone, J.M.: Face recognition vendor test 2002 results. Technical report (2003)
[2] Zhao, W., Chellappa, R., Rosenfeld, A., Phillips, P.J.: Face recognition: a literature survey. Technical Report CAR-TR-948, Center for Automation Research, University of Maryland (2002) Phillips, P.J., Wechsler, H., Huang, J., Rauss, P.: The FERET database and evaluation procedure for face recognition algorithms. Image and Vision Computing 16, 295–306 (1998)
[3] Turk, M., Pentland, A.: Eigenfaces for recognition. Journal of Cognitive Neuroscience 3, 71–86 (1991)
[4] Etemad, K., Chellappa, R.: Discriminant analysis for recognition of human face images. Journal of the Optical Society of America 14, 1724–1733 (1997)
[5] Moghaddam, B., Nastar, C., Pentland, A.: A bayesian similarity measure for direct image matching. In: 13th International Conference on Pattern Recognition, pp. II: 350–358 (1996)
[6] Ojala, T., Pietikäinen, M., Mäenpää, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence 24, 971–987 (2002)
[7] Pantech, "Pantech unveils VEGA LTE-A, world's first LTE-A with fingerprint recognition and rear touch," 2013.
[8] M. Bishop, Computer Security: Art and Science, Addison-Wesley, Boston, Mass, USA, 2003.
[9] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, no. 3, pp. 614–634, 2001.
[10] K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP Journal on Advances in Signal Processing, vol. 2008, Article ID 579416, 17 pages, 2008.
[11] K. Jain, "Technology: biometric recognition," Nature, vol. 449, no. 7158, pp. 38–40, 2007.
[12]ISO/IEC, "Information technology—biometric data interchange formats—part 2: finger minutiae data," ISO/IEC International Standard 19794-2, 2011.
[13] ANSI and INCITS, "American National Statandard for information technology—finger minutiae format for data interchange," ANSI INCITS 378-2009, 2009.
[14] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1489–1503, 2007.
[15] www.androidauthority.com/how-fingerprint-scanners-work-670934/
[16] T.-Y. Jea and V. Govindaraju, "A minutia-based partial fingerprint recognition system," Pattern Recognition, vol. 38, no. 10, pp. 1672–1684, 2005.
[17] Android Debug Bridge, 2014, http://developer.android.com/tools/help/adb.html.
[18] Pantech VEGA Service, 2014, http://www.pantechservice.co.kr.
[19] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, NIST Special Publication 800-38A, National Institute of Standards and Technology, Gaithersburg, Md, USA, 2001.
[20] NIST Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), 2001.
[21] OpenSSL, "The Open Source Toolkit for SSL/TLS," 2014.
[22] Y.-H. Jo, S.-Y. Jeon, J.-H. Im, and M.-K. Lee, "Vulnerability analysis on smartphone fingerprint templates," in Advanced Multimedia and Ubiquitous Engineering, vol. 354 of Lecture Notes in Electrical Engineering, pp. 71–77, Springer, Berlin, Germany, 2016.