SMART VOTING SYSTEM USING RETINAL IMAGE DETECTION

Kajal Jewani,
Asst Prof.
CMPN Dept
VESIT ,Chembur,Mumbai

Baldev Sundarani,
B.E.Computer Engineering
VESIT ,Chembur,Mumbai

Abhishek Waghmare,
B.E.ComputerEngineering
VESIT ,Chembur,Mumbai

Simran Gurnani,
B.E.Computer Engineering
VESIT ,Chembur,Mumbai

Hitesh Santani,
B.E.ComputerEngineering
VESIT ,Chembur,Mumbai

Abstract - In every election the election commission is facing a lot of troubles and different types of problems throughout the election. The most familiar issue faced by the election commission is inappropriate confirmation with respect to the arrangement of casting the votes, duplication or illegal casting of votes. In this paper, a secure and new voting system is developed to improve the existing voting system using smartcard and retinal images.

In this voting system, the voter identity card is replaced by smart card in which all the details of the person is updated and retinal images from different angles are stored. Only the specified person can poll using their smart card. Here the smart card reader reads the smart card and the details of that person is displayed and the retinal images taken at every angle, and then if the iris pattern matches then the person can poll. The person is allowed to poll once using this smart card. Once we vote, if we use a smart card again, it will give a beep sound which indicates that the person has already voted. Using Blockchain technology the system will be made more secure and free from any frauds. Basically, the system will eradicate dummy votes by use of smart cards.

I. Introduction

We all know democracy is a form of government in which people have right to choose their governing legislators so democratic government completely depends on result of election. So this system needs to be updated frequently. Since our traditional voting system is very slow according to this era we need to update it by using all the technologies so that it becomes more secure, fast process. Election commission will also not face any problems like illegal casting of votes and many other problems.

II. Traditional Voting System

In the Traditional Ballot Voting System, the ballot provides the voters with blue buttons labeled with corresponding party symbol and candidate names. The voter can cast his vote by once pressing the blue button on the ballot against the candidate and symbol of his choice. After the last person has voted, the administrator closes the voting and later the votes are counted .This system can be manipulated by some illegal methods due to which the wrong person can get elected.

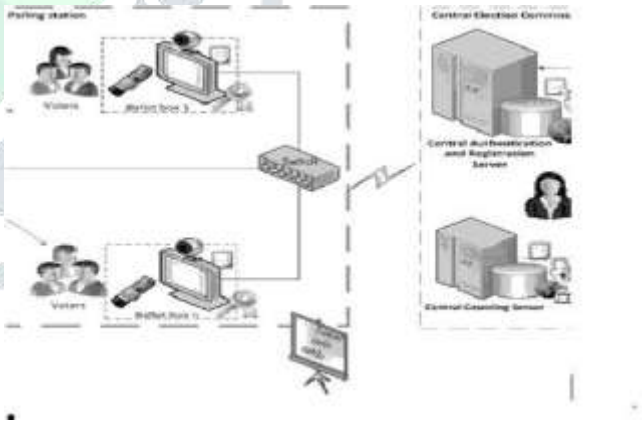

Fig. 1 -. Traditional Voting System

III. Smart Voting System

The main intention of this system is to develop new idea about the voting system ,ensure security of the system and also to reduce the dummy votes. In this system, the voter identity card is replaced by the smart card in which all the details of the person are updated and retinal images from different angles are stored at the time of registration. The system uses Blockchain which ensures security of voting data and also ensures that only the respective person can poll using their smart card. At the time of voting the smart card reader reads the smart card and the details of that person is taken into the system and data is trained for

Image Recognition. Then the administrator takes a fresh image of the voter from the iris camera which is matched with the trained data and if the user is verified , the person would be allowed to vote. After voting the vote will be encrypted using blockchain which makes the system more secure and reduces the number of dummy votes and the respective voter's data will be updated and the person won't be allowed to vote again and hence this will eradicate duplication of votes.

IV. What is a Smart Card ?

A smart card is a physical electronic authorization device, used to control access to a resource. In this card microprocessor and memory chip are attached for processing and storing information respectively. Smart cards provide strong security authentication. Smart card has the capacity of storing and accessing data. Smart card are encryption devices, so that the user can encrypt and decrypt information without relying on unknown.

Fig. 2 - Smart card reader

V. Why Smart Voting is Needed ?

In the traditional voting system duplication of votes and security is the main concern. Many unauthorized people try to vote in traditional voting systems without proper verification details due to which the right person is not elected. Election commission also faces lots of problems so by using smart voting system all these problems can be solved.

VI. What is Iris Recognition ?

Iris Recognition is a biometric technique that uses unique patterns on a person's retina blood vessels. There are four steps in iris recognition : segmentation, normalization, encoding and matching. This is the reason apart from using any other biometric method we have implemented retinal and iris detection in our system so that it is unique and there is no chance of dummy votes.

VII. Proposed Method

- The voter's original data will be fetched from a smart card.
- The system will check if the person has voted before or not.
- If yes, the person won't be allowed to vote.
- Else retina will be scanned using the retinal Camera.
- After capturing the image, the captured image will then be matched with the smart card database and if valid the person will be allowed to vote.
- After the person casts a vote ,the vote will be encrypted using blockchain.

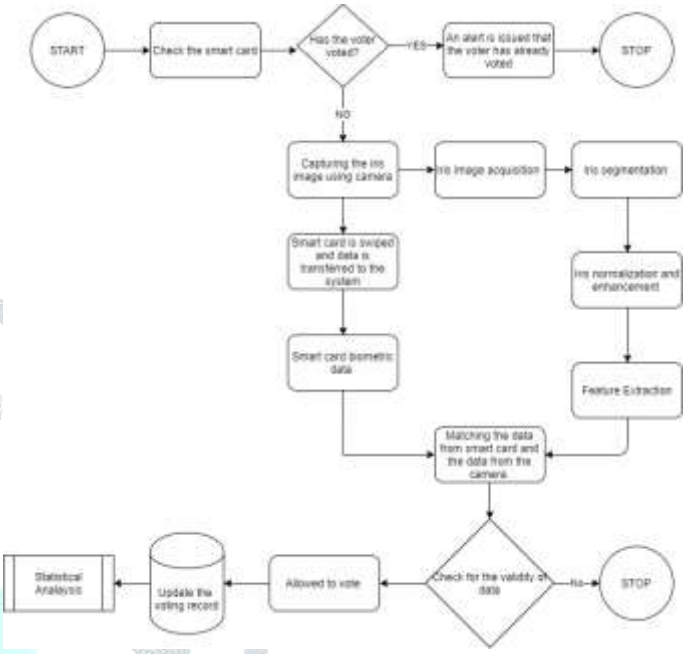

Fig 3 – Voting System Flowchart

VIII. System Design

As you can see in the diagram, we have created two modules admin and user. At the admin end the admin can see candidates list, voters list, swipe smart card of voter.

At the initial stage of voting the admin will swipe the smart card of the voter and then will check all the details and verify it. If all details are valid then the person will be allowed to vote and the admin would be redirected to the voting page. And then the database would be updated.

The end user needs to first register if he/she doesn't have an account. While registering the user would need to fill each and every detail like Aadhar number ,address etc. After registering if the user wants to login, he/she needs to enter username and password. The user can see vote status of election. The user can see the live voting status and statistics of election.

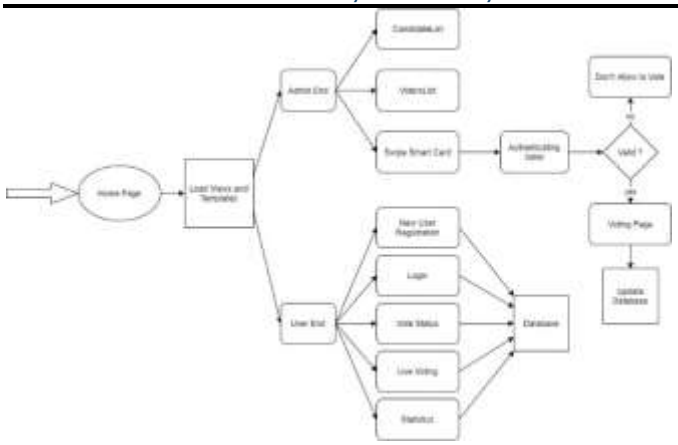

Fig 4 - System Design Diagram

IX. Iris Recognition Algorithms:

X. Daugman's Integro-differential Operator

In this method an integro-differential operator is used for locating the circular iris and pupil regions in the Iris Image, and also the arcs of the upper and lower eyelids. The integro-differential operator is defined as

$$\underset{(r,x_0,y_0)}{Max}\left|G_\sigma(r)*\frac{\partial}{\partial r}\oint_{(r,x_0,y_0)}\frac{I(x,y)}{2\pi r}ds\right|$$

where I(x, y) is the eye image, r is the radius o search for, Go(r) is ta Gaussian smoothing function, and s is the contour of the circle given by r, x0, y0.The operator searches for the circular path where there is maximum change in pixel values, by varying the radius and center x and y of the circular contour. The methodology applied is that the operator is applied iteratively with the amount of the smoothing reduced in order to attain precise localization.

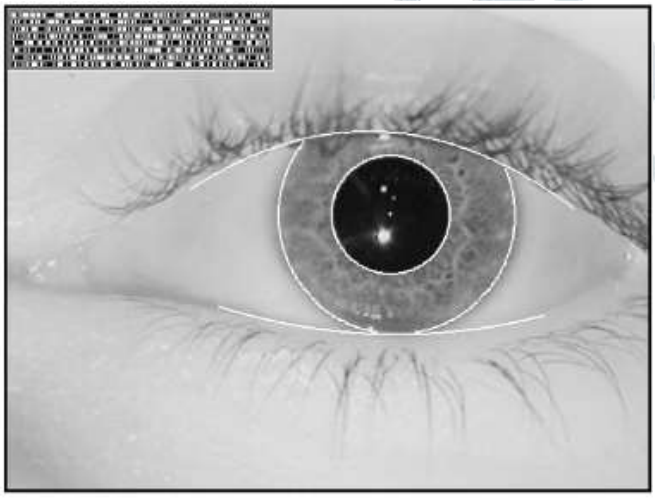

Fig 5- Image result after using the operator for iris and eyelids

XI. Hough Transformation

The Hough Transform is a computer vision algorithm that can be used to determine the lines and circles, present in an image. In our proposed system we have used the circular Hough Transform algorithm to find lines and curves inside the iris image to find the iris and pupil boundaries from an eye image.

We further normalize the regions of the iris using the Wildes method using registers. This method deforms and aligns the iris region to perform the validation.

XII. Log-Gabor filters

In this process, the features are extracted from the iris image and a biometric model is created. The biometric model has the most important information and is encoded. In the proposed system we have used log Gabor filters to extract the features from the iris images.

1D Dimension:

$$g(x)=\exp\left\{-\frac{1}{2}\left(\frac{x}{\sigma}\right)^2+2\pi ikx\right\}$$

2D Dimensions:

$$G(x,y)=e^{-\pi\left[\left(\frac{x-x_0}{\alpha}\right)^2+\left(\frac{y-y_0}{\beta}\right)^2\right]}\cdot e^{-2\pi i\left[u_0(x-x_0)+v_0(y-y_0)\right]}$$

XIII. Hamming Distance:

- The Hamming distance gives a measure of how many bits are the same between two-bit patterns and by using the hamming distance of two bits pattern, we can verify whether the two patterns generated are same or different.
- In the comparison in bit patterns X and Y, the Hamming Distance, HD, is defined as the sum of the exclusive or between X and Y over N, the total number of the bits in the pattern

$$HD=\frac{1}{N}\sum_{j=1}^{N}X_j(XOR)Y_j$$

- In theory, two iris templates generated from the same iris will have Hamming Distance of 0, practically this will not occur. The result of Normalization is not very accurate, and also there will be some noise that goes undetected, so there will be some variation while comparing two iris templates.
- In the proposed system to overcome the inconsistencies one template is shifted left and right bit-side and various Hamming distance values are calculated from successive shifts.
- The template or the created model is two-bits for each filtered pixel from the original iris image, this two-bits represents the possible quadrants. Besides that, a noise mask is used which is responsible to inform the verification process which areas are corrupted because of the eyelids

XIV. Blockchain System

- In the Proposed System for Integrating the voting app with Blockchain so as to make it more secure we used React Framework along with crypto currency app Ganache and Metamask to link various cryptographic keys with the voting app.
- Smart contracts are integrated into the system to ensure security of the system and ensure that a voter vote's only once.

- At the time of voting the admin swipes the smart card of the voter through the smart card reader and the crypt Key of the respective voter is taken into the system after which the voter is verified using Iris Recognition and if the voter is true and has one vote in his account , only then the voter will be directed to the voting app.
- At the voting app the admin will have to select the voter's account from Metamask after which the voting transaction will initiate and after which a vote will be casted.
- After the voting is done , smart contracts ensure that the crypt Key which voted once won't be allowed to vote again and the vote count will be increased.
- The Blockchain system also ensures that the vote count is secure and cannot be tampered by anyone else.

XV. Voter Registration Blockchain system

- Verifying a voter is essential in establishing security within the system, especially when voting is considered, where every vote matter.

- For registering on the voter's blockchain, voters provide their details, this detail creates transactions on the voter blockchain for agreeing with the government that they are asking for a vote.

- The details of the voter get checked with a voting dataset, if the voter has not already registered then the details will be encrypted and added to the national voting blockchain. If already registered then the message will be sent to the user that they are already registered.

- Government miner takes that information from the national voting blockchain, and then verifies it. If details are verified then 1 vote will be authorized to the voter, if not then unverified message will be sent to the voter.

- Once the vote is authorized to the voter, Password will be sent to the voter via SMS and Smart card will be sent via post.

- If an already registered voter wants to change the address or Mobile number then they can request to the government authorized centers who are having private keys for the encrypted details of the voter. That request will be sent to the national voting blockchain and details will be updated.

XVI. Votes Blockchain System

- The voting network is a multi-tiered, decentralized infrastructure. The network is divided into three abstract tiers, National, Constituency and Local.

- The local tier contains all the digital polling stations across the country, each of which is associated to a constituency node. The constituency tier contains all the nodes that are deemed to be at a constituency level. These nodes would be directly connected to each other and to a subset of polling stations depending on the location.

- The national tier is a collection of nodes that are not tied to the location, their pure purpose is to mine transactions and add blocks to the vote blockchain, all constituency nodes communicate to a national node and national nodes can communicate with each other.

- On the day of voting, Voter will swipe the smart card at the polling booth. Whether the voter has 1 authorized vote or not it will be checked. If yes then voter's Iris verification will be done, if not then Invalid credentials message will be shown.

- If Iris verification is valid the voter can choose the candidate to vote. Once a voter selects the candidate,1 vote will be removed from the vote and their vote will be encrypted with the constituency public key.

The encrypted vote will be sent to the Constituency node and the same will be sent to the National node. Once the vote is saved to the National node confirmation will be given to the voter

XVII. Results

- The proposed system is implemented in the form of a web application by using Django framework and React .The System comprises various applications to simplify the functioning of the system. The analysis part is implemented using python programming language.
- The metrics used for calculating and analyzing the efficiency of the system are False Acceptance Rate (FAR), False Rejection Rate (FRR) and True Acceptance Rate(TAR).
  - False Acceptance Rate (FAR): FAR is the possibility of the Iris Recognition system to accept an unauthorized voter or user in the system.
  - False Rejection Rate (FRR): FRR is the possibility of the Iris Recognition System to not allow the right user in the system even if the details provided by the user are correct.
  - True Acceptance Rate (TAR): TAR is the possibility of the Iris Recognition System to correctly authorize the correct user.
- To analyze the accuracy of the system 50 samples are taken from the CASIA dataset and by taking various thresholds the metrics FAR,FRR and TAR are calculated.

The values recorded for different thresholds are in the table below :

Threshold	FAR	FRR	TAR
0.2	0.5	0	1
0.27	0.574	0	1
0.3	0.68	0	1
0.33	0.84	0	1
0.35	0.89	0	1
0.37	0.94	0	1
0.4	0.96	0.02	0.98
0.45	1	0.019	0.981

Table 1 - Accuracy Analysis Table

The Graphs of Thresholds and these metrics were plotted to see the feasibility of the proposed system.

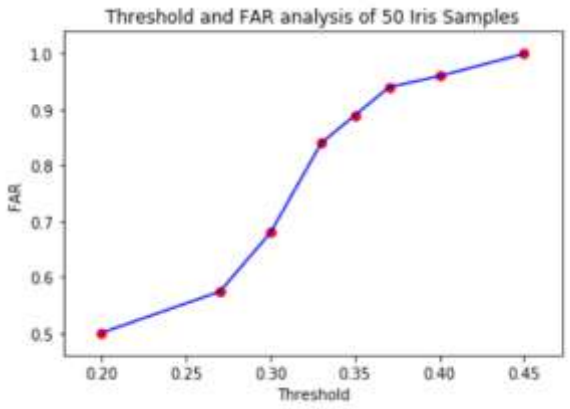

Fig 6 - Plot of Threshold and False Acceptance Rate (FAR)

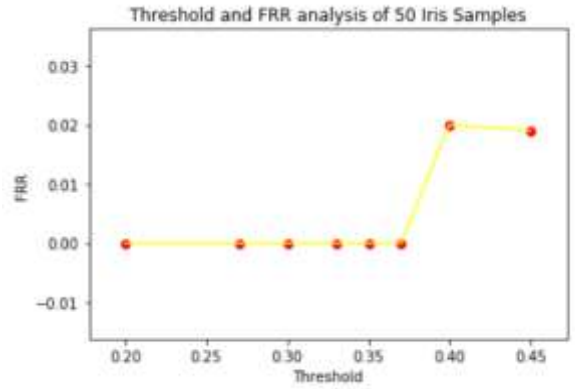

Fig 7 - Plot of Threshold and False Rejection Rate (FAR)

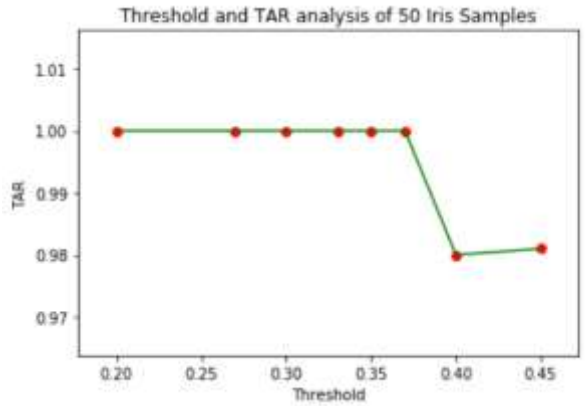

Fig 8 - Plot of Threshold and True Acceptance Rate (TAR)

XVIII. Conclusion

With the increase in population day by day, the improvement of the voting system is necessary. Many biometric methods are available but iris recognition has a high accuracy rate. Using the smart card, it is likely to poll from any polling booth rather than the particular polling booth. It reduces polling time which is most important. It totally rules out chance of invalid vote.

XIX. References

[1] Y. Preethi ,R. Anandha Jothi and V. Palanisamy, **"**A Iris Scanner Based Secure Identification Using LDA Techniques Based Voting System."
IJARET - Vol. 5, Issue 3 (July - Sept. 2018)

[2] Oktay Koc and Arban Uka **"** A New Encoding of Iris Images Employing Eight Quantization Levels "
ResearchGate **-** Journal of Image and Graphics, Vol. 4, No. 2, December 2016.

[3] Rajendran Anandha Jothi, P. Abirami and Vellaiyan Palanisamy **"**A survey on biometric E-Voting System using retina" International Journal of Pure and Applied Mathematics · January 2018.

[4] M. Z. Rashad , M. Y. Shams, R. M. El-Awady
"Iris Recognition Based on LBP and Combined LVQ Classifier" - (IJCSIT) Vol 3, No 5, Oct 2011

[5] Saravanan, Pavithra, Nandhini.C **"**Iris Based E-Voting System Using Aadhar Database"
International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017

[6] Dipti Pawade, Avani Sakhapara, Aishwarya Badgujar and Divya Adepu "Secure Online Voting System Using Biometric and Blockchain "**-** January 2020.

[7] Andrew Barnes, Christopher Brake and Thomas Perry **"**Digital Voting with the use of Blockchain Technology"- September 2016.

[8] Amah Nnachi Lofty , Ali Mansour and Muhammad Hamisu " Towards A Secure E-Voting Model with Blockchain and Biometric Technology "- April 2019

[9] Jagadeva Reddy, Nikhil. S, Sathisha. C, Shivanand A karur and Mr. Sidramappa **"**Centralized Voting System using Smart Card and Biometric" - ICRET - 2016

[10] K. Seetharaman and R. Ragupathy "LDPC and SHA Based Iris Recognition for Smart Card Security" – September 2013.

[11] Gowtham R , Harsha K N , Manjunatha B , Girish H S and Nithya Kumari R **"**Smart Voting System" IJERT -Vol. 8 Issue 04, April-2019