Candidate Identification in Remote/Conventional E-Voting using Iris Detection

Vani Rastogi
Associate Lecturer
Shobhit University, Meerut

Rajesh Pandey
Assistant Professsor
Shobhit, University, Meerut

ABSTRACT
The conventional methods like ID card verification or signature for voting does not provide perfection and reliability. Identification by biological features gets tremendous importance with the increasing of security systems in society.

Various types of biometrics like face, finger, iris, retina, voice, palm print, ear and hand geometry, in all these characteristics, iris recognition gaining attention because iris of every person is unique, it never changes during human lifetime and highly protected against damage. This unique feature shows that iris can be good security measure. Iris recognition is an automated method of biometric identification. The function of the iris is to control the amount of light entering through the pupil, and this is done by the sphincter and the dilator muscles, which adjust the size of pupil. The complete iris recognition system can be split into four stages: Image acquisition, segmentation, encoding and matching.

Secondly, the need for Remote electronic voting using biometric systems has been arrive because of security issues irregularity of voters as the peoples who are not present in their respective towns are not able to vote . Thus a process should be designed such that there should be a portal through which one can vote even if the person is not in his own city. Iris scanners are available in the smartphones we are using now a days. Election booth would still work as the people who cannot afford the high quality smartphones may cast their votes too.

The second concern regarding voting is the instant counting of votes casted by voters, Conventional voting takes much time and the possibilities of mistakes are comparatively high.

Keywords
Remote, iris detection, i-voting

1. INTRODUCTION
Iris recognition is an analysis of the iris of eyes, which is a colored ring of tissue surrounds the pupil of eye. It is based on visible features. Digital template is created with the help of features and their locations. It is considered to one of the safest and accurate biometric technology as it has the capacity to match one pattern with large set of data successfully with extremely high speed without compromising with accuracy of match. This system can be used successfully in presence of eye glasses and contact lenses. This system has been experimented to work with people from different genetic groups .

Advantages

- Uniqueness
- Robust
- Highly Distinctive

2. IRIS RECOGNITION SYSTEM

2.1 Image acquisitioning
The first step of the iris recognition system is image acquisition. This step is very complicated because of differences in size and color of the iris from one person to another. The acquisition distance for average capturing is 2 to 3 feet and the average time is 1 to 2 seconds. Sometimes the acquisition process produces different results for the same person due to the different environmental conditions like lighting effect, positioning and different separation of distance.

2.2 Pre-processing
Image pre-processing is a very important step in iris recognition system in order to get rid of the image noise, and prepare the iris image to better feature extraction. The captured image contains many parts of the eye not only the region of interest (iris) for that its necessary to implement main step which is localization of iris to isolate the iris region from the rest of the acquired image. Furthermore, the distance between camera and eye may be altered. The brightness also plays an important role, as it may have non-uniform caused by the position of the light source. These may impair the result of the texture analysis, for that it is necessary to pre-process the image and localize the iris to extract the important features to perform matching.

2.3 Feature Extraction
Feature extraction identifies the most distinct features for classification. Some of the features are x -y coordinates, radius, shape and size of the pupil, intensity values, orientation of the pupil ellipse and ratio between average intensity of two pupils. The features encoded to suit a format for recognition.

2.4 Pattern Matching
In the matching process, the extracted features of the iris are compared with the iris images in the database. If enough similarity is found, the subject is then identified. The matching process between two templates aims to maximize the probability of a true match for authentic identification tries and minimize false matches for impostors. In other words, images of the same iris taken at different times should be identified as being from the same person and images from different irises should be marked as coming from different persons.

2.5 Storing and Comparing the Image
The set pixels which cover the iris on the image are then transformed into a bit pattern that preserves required information for template comparison but allows faster and statistical meaningful comparison. Dr. Dousman's algorithm, referred to as IrisCode^{TM}, translates the visible characteristics

from the image into a 512 byte code, the template, which allows extremely quick searches and a very low false acceptance rate. When a subject tries to authenticate or identify himself, the generated Iris code is compared with templates stored in the database. A test of statistical independence determines whether the Iris Code resulting from the scan and a stored IrisCode template are from the same iris.

3. I–VOTING USING IRIS DETECTION

3.1 Online Registration Phase

In this phase we will provide the one highly secured website for registration purpose. After that user have to SIGN IN there and fill its whole information including NIC and SIM card number and the IRIS SCAN ,then server sends one secret symmetric key to user. User must have to keep this key (pin) secret. Because this key is required on day of election. Election commission server should keep two updated databases. First database consists of public NIC's cards & the iris scan of every individual and second database contained SIM from the concern authorities for user verification.

3.2 Voting Phase

1. In this phase, ECS will send candidate list to authenticated voter according to their constituency via SMS encrypted with voter symmetric key. This will ensure that the candidate list message only send to the authenticated voter. This method also prevents unauthorized voter to cast their vote.
2. After that voter will receive the SMS of candidate list on voting day.
3. In this step voter will select their candidate from the candidate list. After selecting their candidate voter will then send the message to ECS with public key, candidate PIN encrypt both with user symmetric key and again concatenate NIC number and send to ECS via SMS.
4. ECS will find user symmetric key using NIC number. Then it will decrypt the remaining SMS part with user symmetric key. ECS will mark only the PIN part of the message for the record purposes and to avoid double voting. The remaining encrypted candidate list message will be forwarded to the vote collecting and result phase server.

3.3 Vote Collection and Result Phase Server

1. Before the start of the election, we used time lock mechanism which will not accept vote after time end on VCRPS. It will keep the vote in encrypted form until the official time of the election ended. Implementing this restriction on this server, the decryption of the votes will be started after the end of the election time. The third party will not see the result before the official time ends, thus it prevents to seeing of the election results.
2. After ending of voting phase, vote will be decrypt by using ECS private key.
3. At end of the process, votes will be counted and the results will be officially display to the public.

4. CHALLENGES & FUTURE SCOPE

1. Democracy

It permits only eligible voters to vote and, it ensures that eligible voters vote only once. Hence the one with no natural eye wants to vote, cannot be registered.

2. Security Problems

One can change the program installed in the EVM and tamper the results after the polling. By replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favour of a chosen candidate. These instructions can be sent wirelessly from a mobile phone. With the deployment of biometrics based recognition systems in various sectors, security of the stored biometric data is increasingly becoming crucial. There is always scope for further improvements even if the system seems perfect, taking above points in to consideration the future work regarding the system can be carried out in order to make the system flawless.

5. REFERENCES

[1] Kalyani R. Rawate, Prof. P. A. Tijare, Human Identification Using IRIS Recognition 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099 Themed Section: Engineering and Technology

[2] Mohammad Aakif Kausar, Gautam Purwar, Rajul Raghuwanshi, Prof. Sachin Deshmukh User Identification Using Iris Scan International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 4, April 2016 ISSN: 2278 – 7798.