Security System for Mobile Voting with Biometrics

Laurențiu MARINESCU
IT&C Security Master
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies
ROMANIA
laurr.marinescu@gmail.com

***Abstract**:* For centuries, voting has been a democratic right and way to choose our politicians. Nowadays, the voting process became a major issue in order to avoid crucial vulnerabilities like multiple voting, missing ballot papers, electoral fraud and miscount votes in an election.
To prevent those leaks in our current voting system and to improve other factors like time-consuming and reducing cost of resources, I decided to implement a secured mobile voting system on android.
In today's era, the number of people that possess a smart-phone is larger and larger and also the advanced stage of technology can concur to a reliable solution for voting.
The architecture of this system will contain the mobile application that need to be installed on a mobile device, also will contain a server to compute multiple operations (face detection, face recognition and matching the face with the existing ones, matching unique id of the smart-phone with the one stored in database based on user personal identification number) and a server database. Firstly, an introduction about the subject and system is presented. Problem formulation will contain a research about this topic. Solution of the problem is presented in four subsections: architecture of the system, implementation, face recognition verifier and other solutions.

***Key-Words**:* Mobile Voting, Android, Biometrics, Face detection, Face Recognition, SSL, Encryption, Local Binary Patterns, OpenCV

1. Introduction

The right to vote is one of the vital democratic rights and in today's era there is a need for this process to be linked with most advanced technologies against traditional way of voting by people going to an election office and verify their identity with an identification card. Right now, there are multiple countries that are using different electronic voting systems. The biggest issue we have to face in order to implement a voting system is how we increase the security level compared to popular method of vote where government institutions handle this critical problem. Therefore the need to design a secure voting system is very important. Also another factor to take in consideration, it is mobility, that in modern society affects almost all ages categories and this leads to a dependency on our devices like smart-phones and tablets. For example, an important number of people use their devices to pay their debts using secured systems to perform these actions.

In this article I present the details of a proposed secured mobile voting system by using encryption and biometrics. The encryption it is used to keep the privacy of voting choice and also to secure the communication between mobile application and server. As a student, I see an opportunity to explore a very complex topic and to share my solutions to others.
As a citizen of Romania and an eligible voter, I am very interested in ensuring that my vote is taken in to consideration and also I am very interested to make sure that all of eligible voters from inside the country and outside have the possibility to vote and do not depend on election offices speed of validating voters.
As a software engineer, I see this topic very challenging with a lot of problems to be explored and covered. For mobile voting system most of the problems are related to technical part and how the system can be optimal secured.
I used biometrics to verify the user identity with face recognition algorithms.

ISSN 2067 – 4074

2. Problem Formulation

In this existing voting process there is a large amount of people involved in order to maintain the validity of the vote. Also, persons who would like to vote have to come to an election office, most likely in a school or community buildings with the identification id. Place and time for voting are predefined and each election office it is open only in the predefined time range. The first step in order to vote is to verify the identity of the person, this step being made by one of the persons from the election commissions. The next step for user will be to sign in the register and he will receive the election stamp and the election paper. After the user mark his vote he will put the election paper in the ballot box and leave the stamp at the commission desk. When the vote period ends the members of the commission have to open the ballot box, count the votes and send the result with the ballot to a voting office center. The voting system described above is the most popular system used also in Romania.
To assure the correctness of vote, in my opinion, any voting system should cover those important factors: Democracy, Security, Privacy, Flexibility and Mobility. A voting system is democratic if it allows only eligible persons to vote and to ensure that each person must vote only once. Security factor it is covered by a system if the vote cannot be altered or destroyed or canceled by any external factors or villains. Moreover to increase the security level of the system, latest technology should be used rather than human power. Security should also avoid possibility of fraud by a group of insiders. The privacy of the system it is kept if neither election authorities nor anyone else can link the vote to a particular person. Flexibility and Mobility levels can have a considerable increase if it is used a mobile voting system like the one I will describe below. The most important assets for a voting system are user authenticity and to keep the person's decision secret. In order to do this, we have to uniquely authenticate and identify each person eligible to vote.

3. Problem Solution

To summarize the whole process, the end-user which would like to vote opens the application and the first step will be to register in order to have the possibility to vote. When he will try to register he has to enter his personal identification number and in the meantime a picture is taken with the front camera of the smart-phone and send it along with his personal identification number and unique id of the smart-phone to the server over Secure Socket Layer. The server based on personal identification number of the user, retrieves user's personal information from database(set of pictures needed for face recognition) and match the captured face with the existing photos and also verify if the unique id of smart-phone matches with the one stored in the database. After the identity is validated, the user can click on the vote button and make his choice, the result will be send over SSL with a REST request to the server and stored in the database. By using REST requests, the server can manage multiple requests and that proves the scalability of the voting system. I he tries to vote again, a message will appear on the home-page that it is allowed to vote only once.

3.1 Proposed System Design

Firstly, we need to create the government database in which voters information exist. These database will contain a people table and each row will be created for each eligible person with an unique identification number, the unique id of the smart-phone/ phone-card, a flag which assures if the voter has already voted or not and a reference to a picture table, which will store a set of images for each voter in order to verify their identity using face recognition on the server part. For database, I used MySQL that come along with the apache server because of its ease use of administration and high security level.

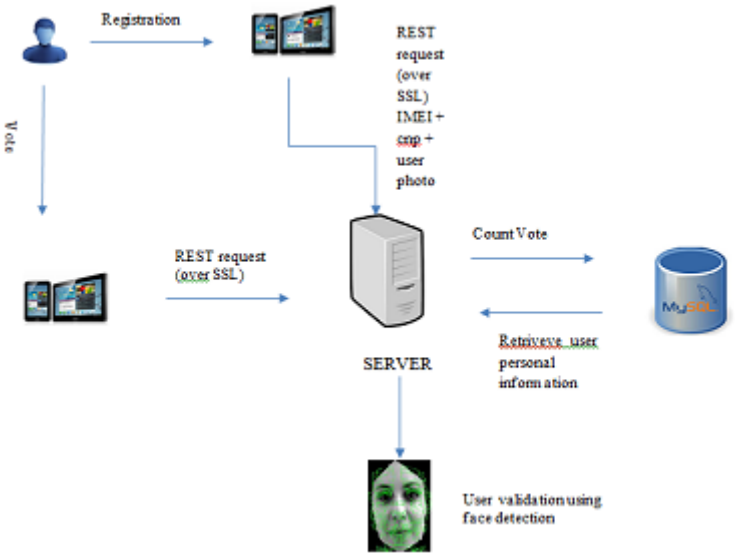

Figure1. System Architecture

MySQL database can be administrated very easily by using the apache server. In the database there is also one table which will contain the voter's choices with a random id in order to prevent the anonymity of the vote. During the voting day or previous days, voters need to download the mobile application from a specific source in order to communicate with the server. In the predefined time range for voting, the user open the app and before actually voting, he need to register to vote. The mobile application it is designed for Android 5.0 Lollipop operating system but it can be compatible with previous android version (from 3.0).
When he clicks the register button, a new form it is opened and voter it is asked to insert his unique identification number and press ok. In the meantime, on the back-end side a picture of the voter is taken without his knowledge using the front-camera of his smart-phone. Also on the Android side I used Asynchronous Tasks to prevent eventual crash of application. While the user waits for validating his identity in the back-end a REST request is made containing the unique identification number, unique id of smart-phone/phone-card and the image. The request is made over SSL (HTTPS) and can be done if previously the application contains a valid client certificate recognizable by server.

On the server side, by using the unique identification number received it is retrieved all the personal information stored in database for current user. After that the face recognition process will begin, comparing the stored images with the one received from mobile application. First step to compare those pictures is to detect the face in the picture received from client by using "Haar Cascade face detection". After that we use "Local Binary Patterns" algorithm or "Eigen Face" algorithm to recognize the face. If the faces match, a response message is sent to the mobile application. On the mobile application side the user is notified if the validation was made or not. If the validation was made he will return to the home page and proceed the vote. After he selected the choice, on the back-end part a REST request is made to the server side and the vote is counted in the database in the Count Vote table and also the flag in the People table is set to true which means the user can not repeat the vote process. On the home page there is also an information button which opens a form with information about current election. Also in the right corner of the home page, a timer is configured to help user to find out how many hours remain until the vote process it is over. In the home page of the mobile application there is a button in case the voter has lost his phone. When he pressed the button a form is opened in

ISSN 2067 – 4074

order to enter his unique identification number. Then, a REST request will be made to the server in the same way as for registration but this time if the user face match the set of images stored in database the unique id of smart-phone it is set in the database for respective unique identification number. On the server side there is also a web page which contains a form, where an authority officer can insert a new eligible Person with specific information, this will conduct to a new row being created in the People table in database. These operation can be done only in the previous days before voting day, only in exceptional cases can be added persons to these table in the voting day.

3.2 Implementation

For development of mobile application I've used Android Studio IDE and Android SDK tools. Development of the Server Side was done in Eclipse using Jersey API for communication between client and server. The biometric part was implemented using OpenCV and connection with the server database was made using JDBC.

3.2.1 Scenarios

1. User A tries to use the phone of user B to vote. After he enters the unique identification number and client request it is processed on the server side, he will not be able to vote even though the face match with the one stored in database, because previously he registered his personal information with a unique id of his smart-phone.
2. User A register to vote on his smart-phone and then tries to vote again repeating the same steps. When he will press the vote button, on the back-end part a verification is made if for the current user the vote flag is set to false or not. In this case is set to false and he cannot duplicate votes.
3. User A downloads the application from an unknown source and does not have the client certificate in order to make the hand-shake certificate validation with the server.

Regarding key criteria's that should be covered for a trustworthy voting system mentioned in Section 2, this application covers security level by communicating over Secure Socket Layer and using certificate needed for client to be validated on the server part. Also covers democracy criteria by using a proper database which contains only persons eligible for voting. Privacy criteria it is done in this implementation by saving in the vote table only the answer with a random id and not knowing who the choice belongs. The authenticity part it is done by the whole process of verifying the unique id of the smart phone and by matching the user face with the ones stored in the database. Flexibility and mobility are covered because clients register to vote and perform the voting on a mobile device or a tablet device.

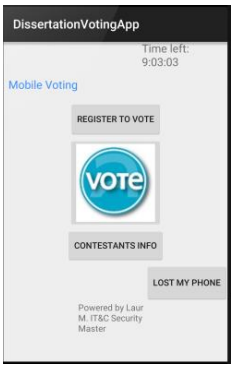

Figure 2. Home page layout

3.3 Face recognition

The process of recognizing a face have two steps: detecting the face and proceed face recognition.

Face recognition brings in several problem which are completely unique to this domain and which make it one of the most challenging in the group of machine learning problems.

- Illumination problem - even a slight change in the illumination of a picture can have a major impact on the results
- Pose changes – any rotation of the face of a person can affect the result
- Time Delay – picture from database do not have to be too old

3.3.1 Face detection

"Face detection is a computer technology that determines the locations and sizes of

human faces in arbitrary (digital) images. It detects facial features and ignores anything else, such as buildings, trees and bodies. Face detection can be regarded as a more general case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one)"[10].
OpenCV algorithm is currently using Haar-like features which are the input for the basic classifiers. Those are:

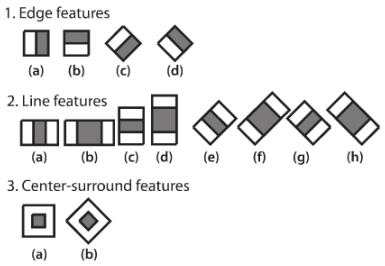

Figure 3. Basic Features

The algorithm that using Haar-like features consider an image to be a human face if it's passes all the stages. This algorithm is performed by cascade.

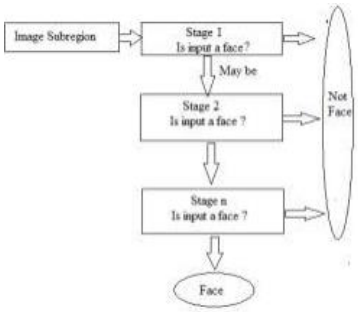

Figure 4. Cascade algorithm

Experimental results

The pictures color was changed also to gray-scale in order to perform easier the face recognition.

Figure 5. Results

3.3.2 Local Binary Patterns Algorithm

Local Binary Pattern is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number.
LBP operator summarizes the local special structure of an image.
LBP is defined as an ordered set of binary comparisons of pixel intensities between the center pixel and its eight surrounding pixels. Decimal form of the resulting 8-bit word (LBP code) can be expressed as follows:

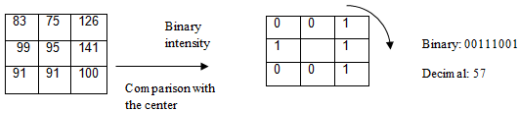

Figure 6. LBP algorithm

We can also do this comparison by applying the following formula

$$LBP\ (x_c, y_c) = \sum_{n=0}^{7} s(i_n - i_c)\, 2^n$$

, where i_e corresponds to the value of the center pixel (x_c, y_c) , i_n to the value of the eight surrounding pixels, and function s(x) is defined as:

$$\begin{cases} 1\ if\ x \geq 0 \\ 0\ if\ x < 0 \end{cases}$$

Local binary pattern it is used to determine the local features in the face and it works by using the LDP operator – in a matrix originally of size 3*3, the values are compared by the value of the center pixel, the binary code is produced. The LBP code is obtained by converting the binary code into decimal one.

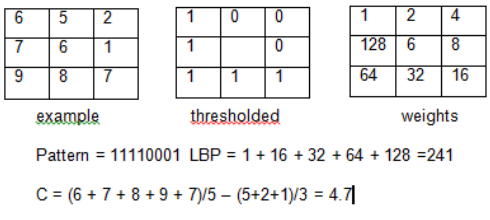

Figure 7. LBP code

LBP Histograms

- Each pixel of an image is labeled with an LBP code;

ISSN 2067 – 4074

- First it will divide the image to several blocks
- Then it will start calculating the LBP histogram for each block;
- After that it will combine every LBP histogram for that image.
- Then you will get all the LBP histograms into one vector

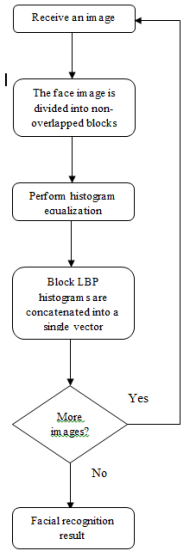

Figure 8. LBP Flowchart

3.4 Other solutions

Lately, there is a growing number of authors who have developed and done research in mobile voting systems. Some of these are presented:
Gentles and Sankaranarayanan (2012:57-68) developed a secured authenticated mobile voting system with biometrics, which is based on fingerprint biometric method and encryption using Secure Socket Layer to make the software more trustworthy and secure. Their system operates only on Android 3.0 operating system and the voter must have a smart-phone in order to use this mobile voting system as it requires to catch ridges of the fingerprints.
Another example is the SMS Based Voting machine developed by Warrier (2010) that allows persons to cast their vote by sending a SMS in a specific format (predefined) with a identification number and unique password in the comfort of their own homes. The voting machine receives the messages and decodes the message and verifies the identification number and the pin and if both number matches the voting machine will accept the vote otherwise the message is rejected by the machine.

4. Conclusion

Mobile voting systems have many advantages over the traditional way of voting. Some of these advantages are higher security level, greater accuracy, mobility, a faster way to count the results and lower risks of human errors. However it is very difficult to develop an ideal mobile voting system which can provide 100% security and privacy level. This article proposed a real-time mobile voting system based on android devices. For future work I will focus on improving security of the application and also improving the facial recognition result by extending the known-algorithms. There is still a large amount of research needed around this topic.

Acknowledgement

Parts of this paper were presented at The 7th International Conference on Security for Information Technology and Communications (SECITC 20115), Bucharest, Romania, 11-12 June 2015.

References

[1] Ofori-Dwumfuo, G. O., & Paatey, E. 2011. The design of an electronic voting system. Research Journal of Information Technology 3 (2) , 91-98.
[2] Gentles, D., & Sankaranarayanan, S. 2012. Application of biometrics in mobile voting. I. J. Computer Network and Information Security, 57-68.
[3] “Electronic Voting,” Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.
[4] “Voting – What is, What Could be,” Caltech/MIT Voting Technology Project (VTP) Report, July 2001.
[5] “Electronic Voting,” Ronald L. Rivest, Technical Report, Laboratory for Computer Science, Massachusetts Institute of Technology.

[6] “Secure Voting Using Disconnected, Distributed Polling Devices,” David Clausen, Daryl Puryear and Adrian Rodriguez, Department of Computer Science, Stanford University.
[7] 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).
[8] Electronic Voting (2009), Available from http://www.hwskioskprinter.com/terminology electronic voting.pdf.
[9] OpenCV project, http://opencv.org
[10] http://en.wikipedia.org/wiki/Face_detection