Biometric identification in electronic voting systems

Eduardo Ibañez[1], Nicolás Galdámez[2], Cesar Estrebou[1], Ariel Pasini[3], Franco Chichizola[3], Ismael Rodríguez[1], Patricia Pesado[4]

Institute of Research in Computer Science III-LIDI – School of Computer Science – UNLP
{eibanez, ngaldamez, cesarest, apasini, francoch, ismael, ppesado}@lidi.info.unlp.edu.ar

Abstract. An extension of previous developments of electronic voting and e-government systems carried out at the School of Computer Science of the UNLP is presented, where a digital fingerprint recognition feature is added to the existing system used for faculty elections at this School.

The characteristics and performance of the biometric recognition system are analyzed, as well as the modification of the on-site electronic voting system used in La Plata (hardware and software) and the adaptation to an Internet voting system that can be used at Regional Centers.

Finally, the generalizations of the use of the technology developed for e-government are discussed and current research and development lines are mentioned.

Keywords: Biometric recognition, fingerprints, E-government, E-Democracy, Electronic voting, Voting systems, Distance voting, Internet.

1 Introduction

1.1 E-government and electronic voting

The electronic government, or e-government, arena includes activities aimed at speeding up information management, thus allowing greater control and auditability. Government information systems present a set of distinctive characteristics (for example, they must be very reliable, they are distributed systems, they must respond in real time, etc.) that make their development and administration different from those of traditional systems [1][2].

Electronic democracy, through electronic voting, offers citizens the possibility of continuously participating in political decisions. This participatory form appears in the 1960's, when researchers realized the civic potential that the new electronic

[1] Full-time Assistant in charge of assignments – UNLP.
[2] Semi-Full-Time Graduate Assistant Professor - UNLP.
[3] Full-Time Associate Professor - UNLP.
[4] Head Professor - UNLP. Researcher of CIC Bs. As.

technology had. It becomes more relevant as technology evolves and the digital gap is reduced, and is finally massively incorporated to everyday life.

In these last few years, the fast expansion of technology in communication devices, such as mobile phones, PDAs (Personal Digital Assistant), portable computers with mobile connection to the Internet, allow the community to participate in political decisions from any place [3].

1.2 Biometric recognition.

A biometric system can be used for the verification (identity certification) or identification of a person (establishing the person's identity). Each technique has its specific characteristics, but they all have two stages: training (digital fingerprints are recorded for all individuals that are entered into the system) and use (the information stored is used to verify the identity or identify individuals).

Unquestionably, the most widely used biometric system is that of recognition through fingerprints: various characteristics from different angles and sectors of the fingers are extracted and stored. Fingerprints do not change (through natural processes) throughout the life span of a person, but they can be altered by wounds, humidity, scars or dirt. Various low-cost devices to allow a general use of fingerprints have been developed [4][5][6].

1.3 Biometric recognition in electronic voting systems

One important aspect that has to be taken into account when using e-voting technology (and e-government in general) is personal identification of voters. The irrefutable identification of voters in real time is a complex goal of biometric recognition [7]. These techniques resort to physiological (face, fingerprints, iris and retina, among others) or behavioral (signature and voice) characteristics of people in order to identify them [8][9].

In Section 5, the incorporation of voter recognition through fingerprints and its integration to the electronic voting system developed at the School of Computer Science of the UNLP is analyzed.

2 Contribution

The extensions to the electronic voting system developed at the School of Computer Science of the UNLP to incorporate a biometric recognition feature (through fingerprints) for voter identification are analyzed, and the necessary hardware and software modifications are considered.

System reliability and response times are studied, including the case or regional centers where the votes cast are transmitted through the Internet.

Finally, e-government applications where the developed technology can be used, beyond the electronic voting application, are presented.

3 Electronic voting systems. Previous experience.

III-LIDI has been working on the area of electronic voting since 2003, with several specific experiences, among which the following can be mentioned:

- Software development for electronic voting for faculty and graduate elections in 2003.
- Development of an integral electronic ballot box for the company TESUR for the national elections [10], in accordance with all requirements of the National Electoral Law [14] and reconfigurable to other types of elections (year 2004).
- Base software development for the control of peripherals in the electronic voting machines used in Capital Federal, Argentina (year 2006).
- Development of an integral electronic voting system for student elections at the School of Computer Science since 2007, including industrial, electronic, and software design [11].
- Auditing of electronic voting systems used in the Province of Río Negro, Argentina, and the equipment developed by ALTEC SE. (2007 and 2008)
- Development of remote voting record technology and equipment for the elections carried out in various locations and connected through the Internet with e central counting station (tested for regional centers of the School of Computer Science in 2008) [12].
- Currently, work is being done regarding the evolution of the EV machines developed by ALTEC SE for the Province of Río Negro and the multi-purpose positions developed by III-LIDI for the UNLP, which can be adapted to various e-government applications.

3.1 General description of the electronic voting system developed in 2007

Electronic voting is not just the act of casting the traditional vote using electronic devices. It also provides tools that allow speeding up the operations carried out on the day elections take place, such as voter identity record and verification, vote counting, and the transmission of results to the corresponding organization. Some electronic operations can be combined, whereas others can be done manually, such as manual identity verification and electronic generation of results. Considering that, in general, votes translate into political power, accuracy and quantification quality are aspects that should be particularly considered. Also, there are many electoral security and reliability issues that can be strengthened with technology [13].

In the case of elections for political authorities, the National Constitution and the laws governing the issue [14] (electoral or referendum laws) establish 4 essential requirements or characteristics for voting [1]: *Universal* (all citizens that fulfill a set of conditions must be able to vote, and those who do not fulfill such conditions must not be able to vote), *Equal* (all citizens belonging to the electoral universe must be able to vote only once and all votes have the same value: one citizen, one vote), *Secret* (the identity of citizens cannot be linked, in any way, to the vote they cast) and

Mandatory (all enabled citizens have the obligation to vote; compliance with this depends on electoral scope).

Based on the set of conditions mentioned above, a voting structure that has, for each election precinct, a computing equipment (for precinct board members) connected to a voting machine was developed. One of these machines is shown in Fig. 1. Precinct board members are in charge of identifying voters (through the presentation of an identity card with a picture or student picture ID) from the electronic electoral register stored in the equipment. This identification allows transmitting the corresponding authorization to vote to the voting machine. After the vote is cast, the voting machine transmits a signal to the machine used by the precinct board members so that they can continue with the process. Each voting machine has an LCD touch screen, a CPU, a UPS, a thermal printer, a storage ballot box for printed votes, a device that allows viewing the vote and that automatically drops votes into the ballot box, and 2 flash memories where vote counts will be stored. The equipment used for this election does not have an Internet connection.

Fig. 1. Electronic ballot box used in 2007- 2008

After voting days are over (in the case of the UNLP, elections take place during 3 running days, which adds to the complexity of voting system management), votes are counted in a different machine. Results are transferred through the removable memory devices mentioned above (2 per session, one of them used as backup) which are stored in a wax-sealed envelope at the closing of each session.

3.2 Electronic voting through the Internet at the regional center

The distance at which the regional center is located complicates the transportation of electronic ballot boxes and the safe transfer of votes to the headquarters of the School of Computer Science. For this reason, as well as the reduced student population at the regional center, it was decided not to use the machines described in 3.1., and instead developing a voting system that can be used through the Internet.

This new ballot box has two pieces of equipment (*Local voting equipment* and *Printing equipment*) connected over a VPN to ensure the integrity of the information sent during the electoral process.

The *Printing equipment* is located at the headquarters, and is in charge of printing the voting vouchers that will be stored in a physical ballot box, as well as updating (in two flash memories) the corresponding counters for the votes cast from the *Local voting equipment.* Additionally, on the screen of this equipment, a notice indicating the reception of a vote from the *Local voting equipment* is shown. This *Printing equipment* is located at one of the two enabled election precincts in the headquarters.

Vote counting was done using the same system used for the ballot boxes located at the headquarters.

4 Election model at the UNLP as from 2010.

In 2009, the UNLP has modified its bylaws and as a result, authority elections from this year on have to combine 5 different representations in each School: Professors, Assistants in charge of assignments, Graduates/Auxiliary, Students and Non-teaching staff. Each of these "classes" of voters has different ways of expressing majorities and minorities, which means that, for the application of a general system, programming aspects should be adapted and made more flexible.

Of these 5 groups, we will focus on student elections because this is the most complex group (due to the number of registered voters, voter categories, representation of the majority group and up to 2 minority groups, among other particular characteristics).

4.1 Characteristics to consider for student elections at the UNLP

Student elections at the UNLP take place on an yearly basis and have a duration of 3 days. Ballot boxes are changed daily; at the end of each day, they are wax-sealed and locked in a storage space. After the three voting days are over, the votes in all ballot boxes are counted.

Students vote two classes of authorities: student members (voters are those who comply with regularity conditions), and/or student government association (any student in the electoral register may vote). The electoral register indicates which type of votes students are enabled to cast: STUDENT GOVERNMENT ASSOCIATION ONLY or FACULTY AND STUDENT GOVERNMENT ASSOCIATION. The electoral register is divided in electoral precincts. Ballot papers are divided in two

sectors (student faculty authorities – student government authorities), and students can vote sections from different ballots. Those students who appear in more than one electoral register (because they are enrolled in more than one Academic Unit) can vote for the students government association at each Academic Unit to which they belong, but they must chose at the University (if they comply with regularity conditions) one Academic Unit where they will vote for student faculty members.

Electoral authorities are an Electoral Board, and, for each precinct, a President belonging to the Faculty, a graduate and a student.

The School of Computer Science has two regional centers, one at 500 km and the other at 200 km from the headquarters. The students at each regional center should have the possibility of voting under the same conditions as students at the headquarters, in both regional centers, elections last only one day.

5 Incorporation of biometric recognition to the electronic voting system

5.1 Schematic model.

Governments are very interested in modernizing their information systems. In general, the use of technology to provide access to management services to citizens, as well as the mechanisms that allow a direct participation of citizens in decision making, requires a verification procedure of the people who have access to sensitive information or who are enabled to perform specific operations.

The use of biometric recognition techniques such as fingerprints, even if it is not the only option, can provide a solution to many e-government needs. This process is accompanied by a decreased cost of equipment and an increased accessibility to high-speed communication systems [15]. For these reasons, identity validation through fingerprint recognition for voting procedures is analyzed.

Currently, voters go to electoral precincts with their picture ID and precinct board members compare the picture on the ID card with the holder of the ID. In many cases, ID cards are worn or the picture is not very clear, leaving the final decision to the judgment of the president of the precinct board. Biometric techniques offer an alternative and accurate identity verification method. To use this technique in electronic ballot boxes with precinct board members that verify the identity of voters, a fingerprint sensor can be added to the equipment in order to avoid the use of ID cards. Thus, the system would identify voters directly through their fingerprints. Once the voter is identified, the process proceeds just as with the old electronic voting system. Figure 2 shows a diagram of this system.

To identify voters during elections, fingerprints must already have been incorporated to the electronic register of voters.

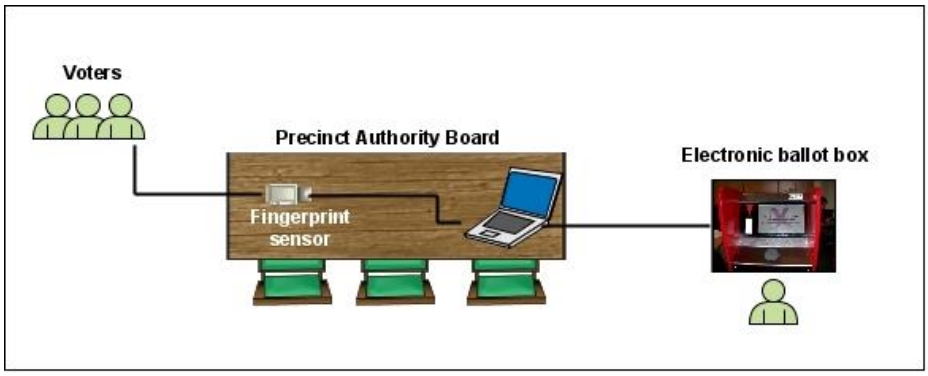

Fig. 2. Diagram of electronic voting with biometric recognition.

5.2 Performance analysis

In previous work [16], the reliability and performance of biometric recognition in e-government applications has been analyzed. The algorithm used in this case for fingerprint recognition processes between 5,000 and 14,000 fingerprints per second. If the database is pre-sorted, processing time could improve significantly, reaching a rate of 15,000 to 70,000 fingerprints/second. In this case, the probability of finding the matching print within the first records searched is very high.

5.3 Changes in use cases

The same as with the voting structure, the interaction of actors with the system is slightly affected. Namely, the way in which voters are identified changes: instead of entering the ID number of each voter to enable the electronic ballot box, voters are identified through their fingerprints. Therefore, the electoral register is not searched for in terms of ID number, but in terms of fingerprints.

5.4 Considerations in case of error.

If some fingerprint cannot be identified (due to finger alterations, cuts, etc.) the President of the precinct board will have the possibility of manually entering the ID number of the voter.

5.5 Benefits

Among the advantages of using biometric recognition, the high degree of certainty in voter identification can be mentioned, which means that the final decision is not left to the judgment of the President of the precinct board when ID cards are worn or otherwise damaged.

It should also be noted that this fingerprint biometric technique is one of the most widely used technologies and that various low-cost devices have been developed.

5.6 Extension to regional centers and Internet voting

The voting scheme will be replicated in regional centers, where the precinct authorities board will have a device to identify voters and an electronic ballot box.

The *Printing equipment* will remain at the headquarters, where vouchers will be printed.

6 Conclusions and future lines of work

An extension of previous developments of electronic voting and e-government carried out at the School of Computer Science of the UNLP has been presented, where a digital fingerprint recognition feature is added to the existing system used for faculty elections at this School.

The characteristics and performance of the biometric recognition system are analyzed, as well as the modification of the on-site electronic voting system used in La Plata (hardware and software) and the adaptation to an Internet voting system that can be used at Regional Centers.

Some of the current and future lines of work are auditing and certification of e-government systems, particularly electronic voting systems, and extension of the developed technology to other e-government applications requiring secure identification.

References

1. De Giusti A., Feierherd G., Pesado P., Depetris B. “Una aproximación a los requerimientos del software de voto electrónico de Argentina”. Congreso Argentino de Ciencias de la Computación. 2004.
2. Tula M. “Voto Electrónico”. Ariel Ciencias Políticas. 2005.
3. Cantijoch Cunill M. “El voto electrónico ¿Un temor justificado?”. Revista TEXTOS de la CiberSociedad, 7. http://www.cibersociedad.net. 2005.
4. Arsaute G. A., Tutores: Nasisi Óscar Herminio M. M. “Reconocimiento de características en huellas dactilares para la identificación humana”. Universidad Nacional de San Juan. Facultad de Ingeniería. Instituto de Automática. 1997.
5. Beavan Colin. “Huellas dactilares. Los orígenes de la dactiloscopía”. Ed. Alba. 1990.
6. Arrieta A., Marín J., Sánchez L. G., Romero L., Sánchez L. A., Batista V. “Gestión y Reconocimiento Óptico de los Puntos Característicos de Imágenes de Huellas Dactilares”. Universidad de Salamanca.
7. Reid P. “Biometrics for Network Security”. Prentice Hall. 2004.
8. Chirillo J. y otros. “Implementing Biometric Security”. Wiley Publishing. 2003.

9. Woodward J.D. Jr. y otros. “Biometrics”. McGraw-Hill Osborne Media.
10. Barbieri A., Pasini A., Estrebou C. “Análisis de Urnas Electrónicas”. Reporte Técnico III-LIDI. Facultad de Informática UNLP. 2004.
11. Pesado P., De Giusti A., Pasini A., Estrebou C. “Voto Informatizado en la Facultad de Informática UNLP”. Reporte Técnico III-LIDI. Facultad de Informática UNLP. December 2007.
12. Pesado P., Pasini A., Ibañez E., Galdámez N., Chichizola F., Rodríguez I., Estrebou C., De Giusti A. “Voto electrónico sobre internet”. Congreso Argentino de Ciencias de la Computación 2008.
13. Pesado P, Feierherg G, Pasini A. “Especificación de requerimientos para sistemas de voto electrónico”. Congreso Argentino de Ciencias de la Computación 2005.
14. National Electoral Code, Decree 2135/83 Law 19,945 / 20,175 / 22,838 / 22,864 and as amended.
15. Srinivasan V. S., Murthy N. N. “Detection of singularity point in fingerprint images. Pattern Recognition”. Vol 25, pp. 139-153. 1992.
16. Carri J. I., Pasini A., Pesado P., De Giusti A. “Reconocimiento biométrico en aplicaciones de E-Government. Análisis de confiabilidad / tiempo de respuesta” Congreso Argentino de Ciencias de la Computación 2007.
17. Lee H. C., Gaensslen R. E. “Advances in fingerprint technology”. Elsevier, New York. 1991.