

Full Length Research Paper

Web based secure e-voting system with fingerprint authentication

Adem Alpaslan ALTUN^{1*} and Metin BİLGİN²

¹Selcuk University, Technical Education Faculty, 42031, Konya, Turkey.

²Selcuk University, Natural and Applied Sciences Institutes 42031, Konya, Turkey.

Accepted 23 May, 2011

The elections that are made by using traditional methods are no longer preferred because of the long period of preparation, fake voting, faulty voting, mistakes made in counting the votes, long period of counting and high cost of voting process. In order to avoid these disadvantages affecting directly the economy and policy of the country, it is obligatory to carry the available voting system to an electronic system. In this study, an electronic voting system, E-voting for a general election is developed and fingerprint authentication based e-voting system is applied. As a result, security of the voting system is greatly improved by using biometric authentication system.

Key words: Electronic voting, biometric systems, fingerprint, authentication, election.

INTRODUCTION

Nowadays, voting for general and local elections is done by electors with voting papers and voting boxes in which the voting papers are placed. This method reveals some kinds of negative situations. Not been able to determine which party the stamp belongs to, the probability of placing the voting papers in wrong box, problems with counting the votes, loss of time when there happens to be some objections, paper printing and expenditures done for personel are some of the disadvantages of classical election system. The secret ballot is a fundamental instrument for protecting the freedom of choice of voters. For this reason, it is necessary to use new technologies for making the election system more trustable, economic and faster.

Electronic election system is set into use in some countries, especially in USA and Europe, at the beginning of nineties as a result of innovating technology and it became more trustable by improving itself at the present

day. Electronic voting is an activity of realising the voting in electronic environment. Electronic election is a system which enables fast counting by electronic voting. Electronic voting is used in some countries in the world and there are also studies about it (Babu and Padmavathamma, 2006; El-qawasmeh and Owais, 2010; Folorunso et al., 2005; Hajjar et al., 2006). Electronic voting is used for parliamentary elections in Australia in 2001 (Schoen and Faas, 2005), for student union elections in Austria in 2003 (Prosser et al., 2003), for municipal elections in Canada in 2003 (Nakhaie, 2006), for both general and local elections in India in 2003 (Gorla, 2009). As a result of developments on information technologies in recent years, public opinion polls and nation-wide general elections will be realized faster and more effectively on electronic environment.

Nowadays, security problems are experienced with the fast developing technology. Besides developing the system, there are also so many studies and new methods for solving the security problems of the developing system. As a result of developing technology, individual password is started to be used to meet the security requirements. In time, new methods are developed and

*Corresponding author. E-mail: altun@selcuk.edu.tr. Tel: +90 332 2233355. Fax: +90 332 2412179.

card technologies are used due to closing the security holes about burglary of the cards or forgetting the individual passwords. Usage of the ID cards and Private Identification Numbers (PIN) become widespread at card technologies (Sonkamble et al., 2010; Alkan and Bulut, 2010). Researches on security and identification operations according to physical characteristics are realized due to limitations of this technology in time.

Biometric systems are the methods which make identification of people according to their physical characteristics. Biometric methods consist of fingerprint, face, hand shape, retina, iris, and voice track methods (Sonkamble et al., 2010; Kadry and Smaili, 2010; Razzak et al., 2010). These methods may be used alone or together in the developed systems.

Fingerprint recognition method and ID system in biometric methods are frequently preferred because applications of them are easy and low-cost (Maltoni et al., 2009). Fingerprint recognition system is the leading method because everyone has different fingerprints, can not be changed easily and probability of loosing, forgetting and stealing of it is impossible. Besides, every finger has distinctive characteristics because fingerprints of every finger of a person are different (Altun et al., 2008).

For this reason, fingerprint method is used mostly alone or together with other biometric methods for providing security of the systems. Fingerprint method is also used for identification of the internet applications.

In this study, biometric election system is aimed instead of traditional election systems. By developing the deficiencies of the present system, biometric based election system has been developed.

MATERIALS AND METHODS

Electronic voting

Electronic voting systems have to respect the constitutional election principles. For technological solutions, this translates into security requirements that have to be fulfilled by the operational environment in which the voting takes place.

First study on electronic voting is patented as "Electronic Vote-Registering Apparatus" (US Patent 90.646) by Thomas Edison on 1st of June 1869 (Edison, 1869). Edison developed this invention for using on congress elections (Roth, 1998). Computers are used on counting of the votes for the first time on Punch Card system in 1964 (Fleischmann, 2009). Direct Recording Electronic Systems (DRE) manufactured in 1980 is the first full computer based system. DRE systems consist of buttons and areas on the touch screen. Electors in the election area get a PIN or smart card by showing their ID. They enter DRE machines by using PINs or smart cards. Elector makes his or her choice and after that DRE machine shows the choice on the screen and finally gives elector an opportunity to change his or her choice. And as a result of this, DRE records the vote accurately. Lever Machines are first used in New York Elections in 1982. The interface in this system is arms related with

the questions on voting paper or every island. People vote by moving the proper arm in this system.

European Commission started the E-voting project on September 2010 for showing online elections, reality of which can be proved (Trechsel and Mendez, 2005). Stable and mobile internet terminals are used within the scope of this project. The Project includes partners from industries, universities and potential users. First experiment is done in a village in France on 11th of December 2002. 860 electors chose city council representatives on electronic environment. Second test is done in Bremen University in Germany on 13 to 15th of January 2003. In this application, university council is chosen by 47 electors on electronic environment. The last experiment is done in Sweden by 226 old electors on July 2003.

Biometric methods and applications

It is necessary to provide security of the systems due to developing technology. Securities of most of the systems are provided by passwords, PINs and ID cards (Hajjar et al., 2006). In time, these methods did not meet the security needs and searched for new methods. For this reason, some researches are done for alternative methods. Physical characteristics of people came up for providing people to login the system by making identification and studies about biometric methods are started (Monrose and Rubin, 1999).

Biometric methods provide identification by using specifications such as fingerprints, face, hand shape, iris, retina, voice track and signature. These specifications vary from person to person. By this way, reliableness of the system is preferred according to the system used.

Biometric solutions are generally client/server solutions, giving system administrators the ability to audit usage, manage security levels, and remove unauthorized users. These solutions are emerging rapidly that allow deployers to integrate biometric functionality into Web sites, replacing password authentication. Biometric methods are used for verification or identification of a person. On recognition and identification system, you give your information to the system; the system brings your information in the data base, makes one-to-one comparison and answers the "Do I know you?" question. In verification, you claim to the system who you are and the system tries to find if you are really the person you claimed. There is comparison and the system tries to answer the "Are you the person you claimed?" question. Biometric classification is also the classification of the biometric incomes in similar specifications. During the identification, classification makes comparisons between conspectuses in the same group but not the whole data base. This application saves performance.

RESULTS

In this study, a biometric based e-voting system is designed for providing a secure election on electronic environment for the electors. XSL language which is compatible with Asp.Net, Framework 2.0, Java Script, Xml is used in this system and it can also run with Microsoft Windows operating system (Tubishat et al., 2010; Cömert et al., 2010). Besides, biometric based software libraries are also used for integrating the fingerprint control to the system. The elector identification

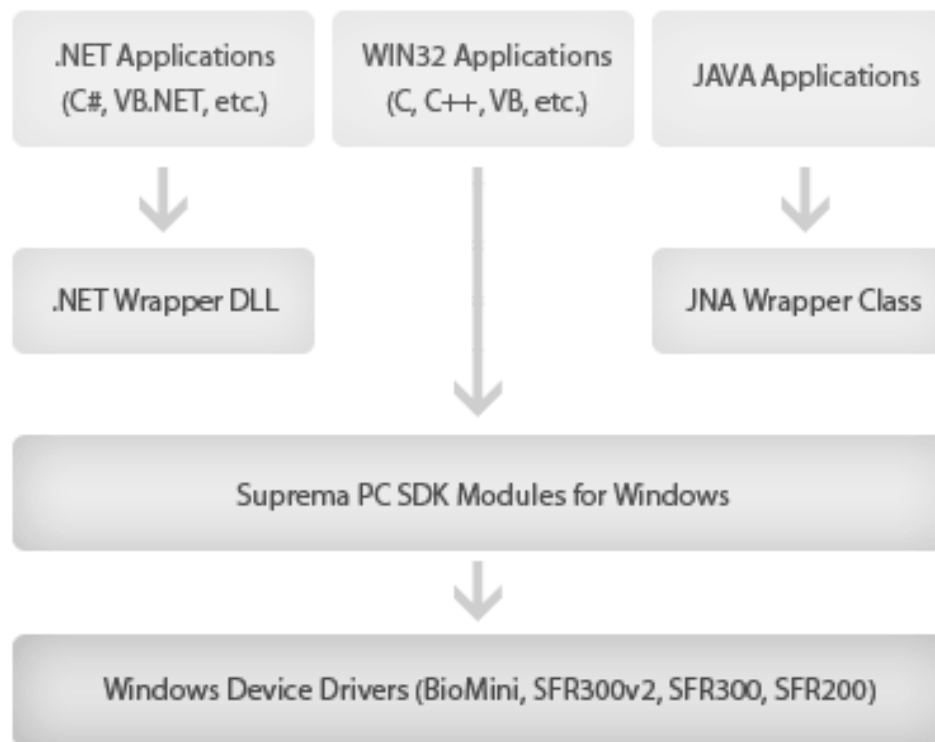


Figure 1. General structure of fingerprint device programming.

system is programmed with C# language and equipped with an optical fingerprint scanner SDK (Suprema Inc®) to accept a scan, recognize the elector, and open the correct elector record in the database and verify system (Suprema, 2010). This module uses a dynamic link library (DLL) that can be displayed in a web application as shown in Figure 1.

This allows the electors' biometric data to be read by a web application and sent to a web service for verification. All of the biometric logon modules have two parts: A web application, which is a webpage with program logic running behind it, for data collection and a web service for verification. The e-voting web application is allowed to interface with the physical biometric device but not the database containing the enrolled user data, while the web service can do the exact opposite. The following scenario shows the flow of data between the web application and the web service during a fingerprint logon.

Working principle of the system is as follows:

1. Election, party, candidate, region, street, polling clerk and village headman information is defined by system administrator.
2. Electors' information is recorded into the system with their fingerprints by village headman.

3. System administrator starts the election on the day determined before.

4. Polling clerk starts the election on the box within his or her authorisation.

5. Elector comes to the box announced before and scans the fingerprint for voting.

6. If the scanned fingerprint is not in the electors' database, elector can not vote.

7. If the scanned fingerprint is in the electors' database, elector's ID information is shown on the screen.

8. If there is no problem with the ID check, elector votes by pressing on the vote button.

9. If elector voted before for the election in question, the system warns about the situation. If elector has not voted yet, the system brings the vote screen.

10. Elector votes for any party by pressing on the "YES" button. Elector is warned as final step for preventing misvoting by a message on the screen. If the elector wants to continue voting, elector finishes voting by pressing on the "YES" button.

11. If the elector tries to vote for the second time for the election in question, the system does not allow this.

12. Then, election is finished by the system administrator.

13. Election results and statistical information can be provided just after the election is finished.



Figure 2. User interface for system login

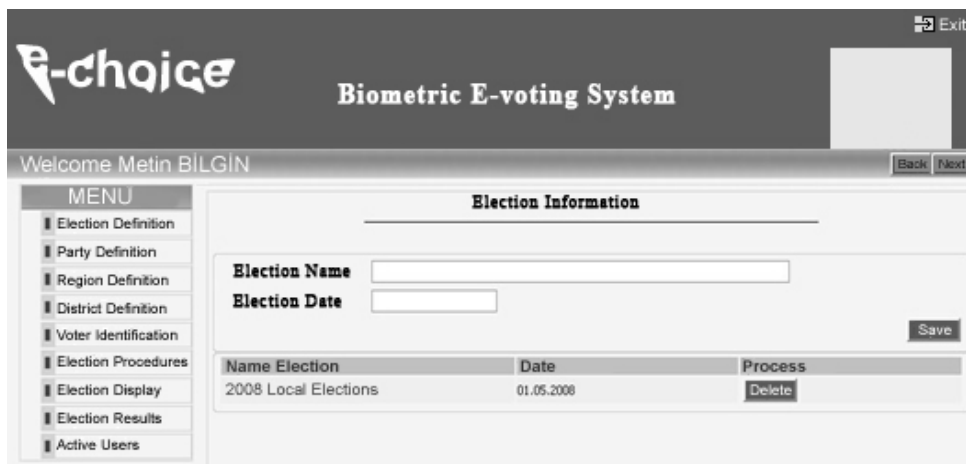


Figure 3. Election defining screen.

Working principle of the system during elector's voting procedure is as follows:

1. Elector's fingerprint is scanned by using fingerprint scanner.
2. Elector's fingerprint is searched for in the electors' database.
3. If the elector's fingerprint is not in the electors' database, elector can not vote.

Otherwise, the elector's information on the screen is checked:

1. After checking, elector presses on the "Vote" button. Then, the system controls if the elector voted before for the election in question. If so, the system warns about the situation. Otherwise, the system brings the vote screen.
2. Elector votes for any party.
3. If the elector is sure about the vote, voting is finished.

Biometric election system is designed as a web based system. By this way, votes of the electors are collected in

a center through internet network which does not cost much. The security of the information is provided because the fingerprints are converted to dual code, encrypted and recorded in the database when entering the system. When the system is run for the first time, the image on the screen as user's interface is shown in Figure 2. There are three different login methods to the system. The first one is the system administrator. The system administration is the part of the system where all the regulations are done and authorisations are determined. It consists of screens where election determination, party determination, region determination, street determination, elector determination, election affairs, election screen, election results, and active users can be viewed.

After logging in, election name and date is defined by the administrator as shown in Figure 3. Parties to participate in the election are defined. Then, regions where the election will be done and streets in those regions are defined in the system. By this way, attendances of only the related electors are provided.

Electors registered before are searched in the database

Biometric E-voting System

Welcome Metin BILGIN

MENU

- Election Definition
- Party Definition
- Region Definition
- District Definition
- Voter Identification
- Election Procedures
- Election Display
- Election Results
- Active Users

Your fingerprints haven't been defined.

Serial Number	9090978	ID Number	000000000000000000
Name	HALIT	Surname	ERKÖK
Father's Name	SULEYMAN	Mother's Name	HANİFE
Birth Place	KONYA	Birth Date	18.08.1981
Marital Status	BEKAR	Religious	ISLAM
City	Konya	Town	KARATAY
Village	ISTIKLAL		
Volume Number	909	Family Number	5
Serial Number	4545665	Blood Group	O RH +
Place of issue	Konya	Issue Because	YENİLEME
Register Number	768700	Issue Date	07.05.1968

Finger Print Definition Save

Figure 4. Voter information.

Biometric E-voting System

Welcome Metin BILGIN

MENU

- Election Definition
- Party Definition
- Region Definition
- District Definition
- Voter Identification
- Election Procedures
- Election Display
- Election Results
- Active Users

Selection Input Screen

Press the button to read fingerprints

Finger Reader




Figure 5. Fingerprint information is scanned and stored in the database.

and necessary corrections are made. In addition, new electors are added. Fingerprints must be scanned while the electors are registered. Otherwise, registration of the electors can not be done. Electors are registered by using elector defining screen as shown in Figure 4. While defining electors, all of the information about the electors must be recorded. If the information is not recorded properly, registration of the electors can not be done. Electors see the fingerprint defining screen on the recording phase which comes after recording of the information as shown in Figure 5. Fingerprint defining

result screen comes in front of the elector during the scanning and defining phase of the fingerprint.

Electors are registered to the related region. By this way, elector can vote only in the region where he is registered. The election is started for voting by system administrator just after the elector defining procedure is finished. Only one election is started in the system at the same time. Thus, the errors with the system are prevented. After starting the system, electors login and vote. If the fingerprint verified belongs to an elector registered in the system, the information of the elector appears

Ballot		
	Parties	Deputies
<input type="radio"/>	A Party A	METIN BILGIN - BESIM BILGIN
<input type="radio"/>	B Party B	BILGEHAN ÖREN - VEYSEL GÜNDOĞDU
<input type="radio"/>	C Party C	MUSTAFA BALCI - MESUT YALVAÇ
<input type="radio"/>	D Party D	ORHAN İNCEÇAM - MURAT AKSU
<input type="radio"/>	E Party E	SERDAR DÜZ - SUAYİP YALNIZ

Figure 6. Parties list for voting.

The screenshot shows the 'Election Results' window of the 'e-choice Biometric E-voting System'. The interface includes a 'MENU' sidebar with options like 'Election Definition', 'Party Definition', 'Region Definition', 'District Definition', 'Voter Identification', 'Election Procedures', 'Election Display', 'Election Results', and 'Active Users'. The main area displays a table of results for the '2008 Local Elections' in the 'Bursa' region. The table shows that Party B and Party C each received 1 vote, for a total of 2 votes.

Election	Region	Parties	Vote	%
2008 Local Elections	Bursa	B Party B	1	50,00
		C Party C	1	50,00
		TOTAL	2	

Figure 7. The election results relevant to the region.

on the screen. Purpose of this application is identification control by system administrator. Elector can vote by pressing on the elector voting button just after authentication. Elector can vote clicking on the “YES” button of the party that he/she chooses on the e-voting screen as shown in Figure 6. After voting, a message appears on the screen and voting procedure is completed for the elector. Election results of any region or regions in any time are observed by the system administrator. These operations can be done on election results part of

system administrator window as shown in Figure 7.

DISCUSSION

Modern technology is used for elections and/or referandums commonly. Number of the reseraches on electronic election systems is increasing in recent years. As a result of being in search of more efficient, more trustable and faster election, different kinds of voting

boxes are manufactured and put into service of the countries. Mercuri, MIT/Caltech and E-Vox are three of these boxes.

Biometrics is also expected to be increasingly used in conjunction with other technologies like the knowledge-based authentication (e.g. passwords and PIN) on the Internet. In this study, user friendly electronic voting system based on biometric verification is designed and proposed. Thus, electronic voting boxes are offered instead of voting boxes of the present election system. The advantages of the e-voting system based on biometric verification are as follows:

1. The number of the voting boxes decreases by using biometric election system. The expenditures of the elections decrease too.
2. Vote repetition is eliminated. By preventing voting of someone instead of some other elector, the security of the election is provided.
3. Possible mistakes during voting and counting of them are eliminated.
4. Incorrect and invalid votes are eliminated.
5. Results of general or local elections can be viewed faster.
6. The expenditures of voting paper, envelopes, stamps, voting boxes, stationery etc. are eliminated.

For making the election activities easier in biometric voting system, kiosks or LCD touchscreens are used. Thus, negative situations arising from personal deficiencies of the electors can be prevented and electors vote faster. Besides, by integrating vocal expression on the system, visually impaired electors can vote by using headphones. The security of the system is so important. For this reason, required security precautions should be taken and security system should be set up for preventing any attack from the outside.

ACKNOWLEDGEMENTS

This work had been funded under the thesis project "Design and Application of Biometric Based Electronic Voting System" approved by the Selcuk University (Turkey) in 2008.

REFERENCES

Alkan M, Bulut G (2010). GIS and remote-sensing-based urban-information system design and development: A case study for Kozlu, Zonguldak, *Sci. Res. Essays.*, 5 (19): 2889-2899.

- Altun AA, Kocer HE, Allahverdi N (2008). Genetic algorithm based feature selection level fusion using fingerprint and iris biometrics, *Int. J. Pattern Recog. Artif. Intell. (IJPRAI)*, 22(3): 585-600.
- Babu GA, Padmavathamma M (2006). Optimally efficient multi authority secret Ballot e-election scheme, *J. Theor. Appl. Inf. Technol.*, 2(1): 1-6.
- Cömert C, Uluta D, Akıncı H, Kara G (2010). Semantic web services for implementing national spatial data infrastructures, *Sci. Res. Essays.*, 5(7): 685-692.
- Edison TA (1869). Electric Vote-Recorder, US Patent, No: 90646.
- El-qawasmeh E, Owais S (2010). E-democracy in middle east: hard to approach, *Journal of Theor. Appl. Inf. Technol.*, 21(1): 57-63.
- Fleischmann KR (2009). Sociotechnical Interaction and Cyborg-Cyborg Interaction: Transforming the Scale and Convergence of HCI, *Inf. Soc.*, 25(4): 227-235.
- Folorunso O, Ogunseye OS, Okesola JO, Olaniyan OM (2010). Visualizing e-voting results, *J. Theor. Appl. Inf. Technol.*, 16(1): 57-69.
- Gorla N (2009). A Survey of rural e-Government projects in India: Status and benefits, *Inf. Technol. Dev.* 15(1): 52-58.
- Hajjar M, Daya B, Ismail A, Hajjar H (2006). An e-voting system for lebanese elections, *J. Theor. Appl. Inf. Technol.*, 2(1):21-29.
- Kadry S, Smaili M (2010). Wireless attendance management system based on iris recognition, *Sci. Res. Essays.*, 5(12): 1428-1435.
- Maltoni D, Maio D, Jain AK, Prabhakar S (2009). *Handbook of Fingerprint Recognition*, 2nd ed., Springer.
- Monrose R, Rubin A (1999). Keystroke dynamics as a biometric for authentication, *Future Gen. Comp. Syst.* 16(4): 351-359.
- Nakhaie MR (2006). Electoral Participation in Municipal, Provincial and Federal Elections in Canada, *Canadian J. Pol. Sci.* 39(2):363-390.
- Prosser A, Kofler R, Krimmer R (2003). Deploying Electronic Democracy for Public Corporations, *Lecture Notes in Comput. Sci. (Electronic Government)* 2739: 234-239.
- Razzak MI, Yusof R, Khalid M (2010). Multimodal face and finger veins biometric authentication, *Sci. Res. Essays.*, 5(17): 2529-2534.
- Roth SK (1998). Disenfranchised by design: voting systems and the election process, *Inf. Design J.* 9(1): 1-8.
- Schoen H, Faas T (2005). When Methodology Interferes With Substance: The Difference of Attitudes Toward E-Campaigning and E-Voting in Online and Offline Surveys, *Soc. Sci. Comput. Rev.*, 23(3): 326-333.
- Sonkamble S, Thool R, Sonkamble B (2010). Survey of biometric recognition systems and their applications, *J. Theor. Appl. Inf. Technol.*, 11(1):45-51.
- Suprema (2010). http://www.supremainc.com/eng/product/pc_20.php?mark=3 (last accessed 10.07.2010).
- Trechsel AH, Mendez F (2005). The European Union and E-voting: Addressing the European Parliament's Internet Voting Challenge, Routledge Press. pp. 1-25.
- Tubishat M, Alsmadi I, Al-kabi M (2010). Using XML for user interface documentation and differential evaluation, *J. Theor. Appl. Inf. Technol.*, 21(2):119-127.