COPYRIGHT NOTICE

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 73 (2015) 403 – 407

Procedia Computer Science

The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

A method to improve transparency of electronic election process without identification

Roghayeh Najjari Alamuti[a]*, Hassan Barjini [a], Manoj Khandelwal[b]

, Mohammad Jafarabad[c]

[a] *Department of Computer Engineering, Imam Khomeini International University, Qazvin, Iran*
[b] *Faculty of Science and Technology, Federation University Australia, Victoria, Australia*
[c] *Young Researchers And Elite club, Robatkarim Branch, Islamic Azad University, Robatkarim, Iran*

Abstract

Transparency of bank accounts, nowadays, is an undeniable necessity, but no one denies that definite transparency throughout election process is not realized thus far in the world. This calls for fundamental changes in traditional electronic election methods. The new method must close the way for any complaints by the candidate as to the voting process as the public completely trusts in the voting mechanism. Synchronizing voting and votes counting improves the public's trust in the results of election. The proposed secure room-corridor of electronic voting employs election watchers and reports real time results of election along with observance of confidentiality of the votes.

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Keywords: transparency of election, electronic election laws, confidentiality of votes; voting room-corridor.

* Corresponding author. Tel.: +98- 0912 83 88 758;
E-mail address: www_vb@yahoo.com

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)
doi:10.1016/j.procs.2015.12.016

1. **Intruduction**

In spite of general commercial trend everywhere that support cutting expenditure, implementation of electronic (i.e. the Internet based voting) nationwide, which is more economic than the traditional techniques, is not realized yet [1]. The main purpose of transferring the current election process is to create a secure and fast election system. Faster election process enables the authorities to keep political stability of a country in emergency situations like unexpected death of president of a country. On the other hand, people expect better and more efficient implementation of democracy. Despite advent of electronic systems and election protocol and equipment, the expected transparency of e-election is not realized yet. This shows necessity to revise all the aspects of election process in different countries to achieve a general solution to eliminate errors and cheating in elections [2]. Among the key players that might abuse the security holes of election process are the state (the authority for running the election), watchers and candidates, suppliers of election software and hardware, and suppliers of electronic communication networks. They may manipulate election process or the votes in favor or a specific party and change fate of one nation [3].

Given the above introduction, any recommendation to hold a secure and clear election is quit welcomed and is worthy of attention. The present paper introduces a parallel room and a corridor design that enables the authorities to count the votes from the moment that election starts. The proposed setting is designed for elections at province level while implementation at national level where only one candidate is elected nationwide needs costly changes. Election at national level can be held with similar transparency using the Internet counting based on receipts with barcodes. Secure digital room-corridors can be used along with traditional voting processes; and those who do not trust in traditional elections method may use the new method. Moreover, observance of prerequisites for holding this model of election may improve security of traditional voting systems as well.

2. Prerequisites of elections by secure rooms-corridors

Any design for holding election is proposed to meet specific needs of a specific population group [3]. The proposed election room-corridor can be employed independently and simultaneously for elections at province level (e.g. parliament elections). The design is featured with general and specific prerequisites. In some cases, meeting the requirement needs new legislations and by-laws by the parliament or the state.

2.1 General requirements of secure election rooms-corridors

By the general requirements, we refer to the default regulations adopted by the majority of countries. There is a need for complete information of eligible voters, polling stations, vote boxes, candidates, number of voters, number of votes based on the candidate and polling stations, number of nullified votes, and number of empty votes to be available from national election websites [1].

The voters are required to attend the polling station once during the election process. As mentioned the present article surveys the general and critical elections and taking into account the paramount importance of such election in destiny of province and national trend of development, any chance of selling or forging votes must be eliminated. This means that identity check must be performed along with preserving privacy of the voters. Unfortunately, this is not feasible using the currently available voting infrastructures [4]. All the eligible voters should provide their national ID numbers and the eligible voters living abroad should provide an election-code.

2.2 Special requirements of secure voting room-corridor design

The special requirements of electronic election are those that realizing them needs decision making by authorities at state level. Such requirements might be in contrast with national election codes or national interests. However, reaching a clean and secure election process comes with its costs. Implementation of taping the election process in election room-corridor where human observers are absent is one of these special requirements.

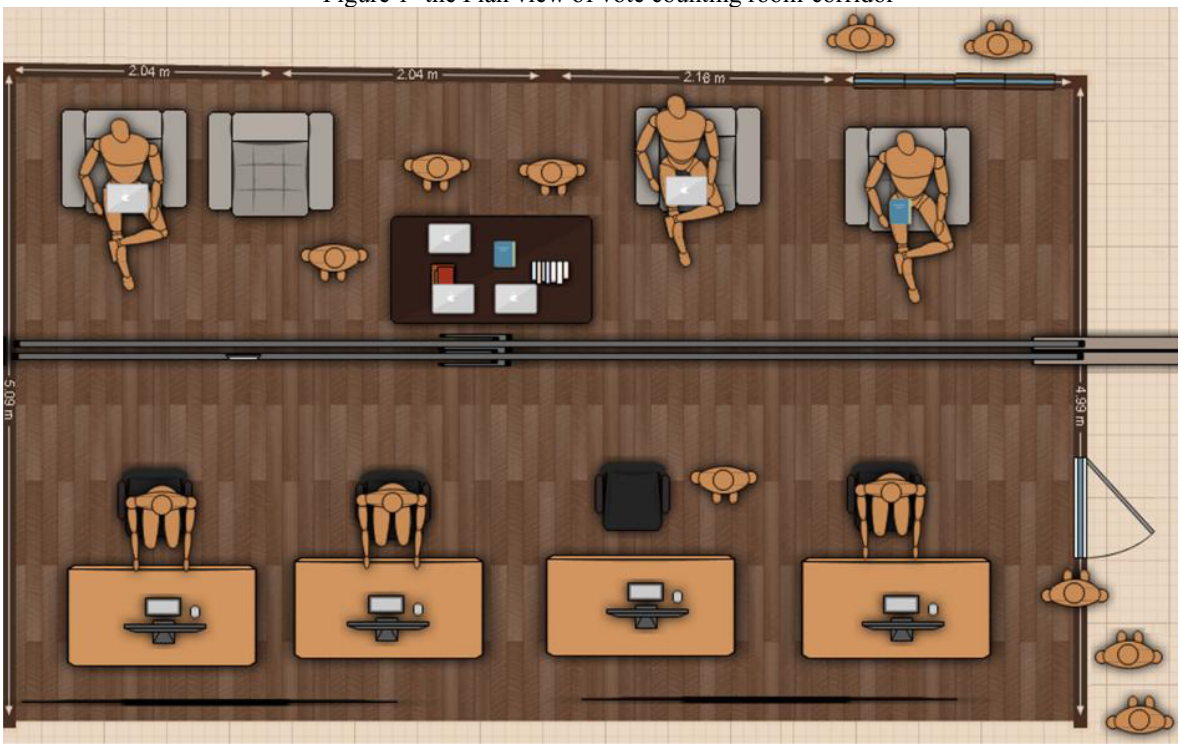
3. The main idea of secure election room-corridor

The main ideal behind secure election room-corridors comes from one of the main security holes in executive election plans. A key point in the different voting methods including voting machine, ATM voting, traditional voting, and so on is that the voters need to have complete trust in the election software and hardware [5]. This can jeopardize the whole election process. The main reason that health of an election is objected is that votes must remain closed until the election is over. The proposed method, however, counts the votes while the election is ongoing. In addition, the election needs enactment of two key laws [6]:

1. Protection of confidentiality of vote so that nobody (even the watchers and authority of the election) is allowed to ask or know peoples' vote.
2. To have transparency in simultaneous counting, the election watchers should check the votes at the moment of voting.

It is not easy to meet these two requirements simultaneously; however, specific design of the secure room-corridor solves this. As pictured in Fig.1, the corridor (bottom of the figure) should be parallel with the watchers' room (top of the figure). In this way, the participants' identity is checked outside the facility and then they enter the corridor to vote using computer interface in the facility.

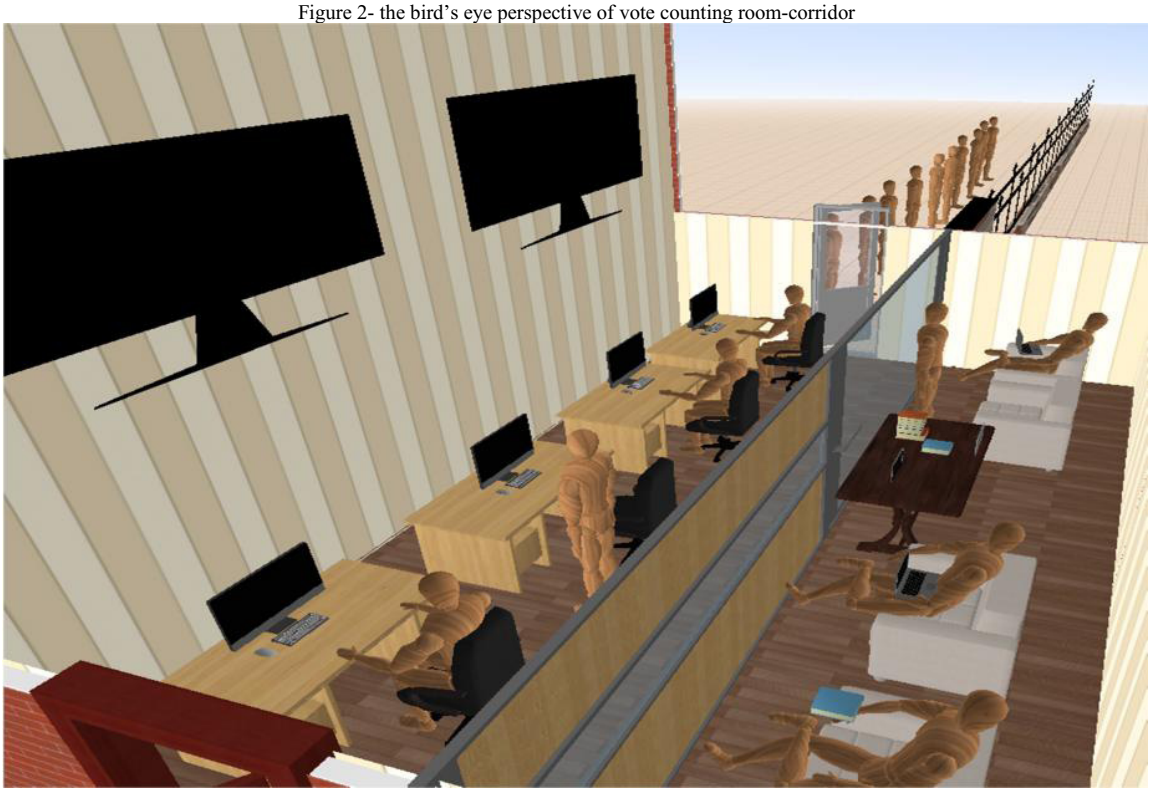
Figure 1- the Plan view of vote counting room-corridor



The voters can check their vote using two displayers while they are voting in the corridor. One of the displayers is directly in front of them and the other (larger displayer) is affixed on the wall. As illustrated in fig. 2, a semi-opaque glass wall separates the watchers' room and the voting corridor. The reason that glass wall is semi opaque is to let the watchers ensure that voters are in the corridor while they cannot see exactly who the voter is. Using this design, the voters can check their vote in the displayer on the wall and the watcher can record and count the new vote while they do not see the voter. The watcher also can tape the whole voting process using a camera.

The voter can check their vote using two displayers while they are voting in the corridor. One of the displayers is directly in front of them and the other (larger displayer) is affixed on the wall. As illustrated in fig. 2, a

Figure 2- the bird's eye perspective of vote counting room-corridor



semi-opaque glass wall separates the watchers' room and the voting corridor. The reason that glass wall is semi opaque is to let the watchers ensure that voters are in the corridor while they cannot see exactly who the voter is. Using this design, the voters can check their vote in the displayer on the wall and the watcher can record and count the new vote while they do not see the voter. The watcher also can tape the whole voting process using a camera.

4. Conclusion and recommendations

Several designs based on confidentiality, identity check, recounting the votes, and so on have been proposed to implement e-election since the late 1990s. Some of these designs have been successful in creating voting protocols, and some have focused on using laser card scanners and image processing techniques to read e-votes. More recent designs are actually a combination of electronic and traditional election methods. While you read this paper, many countries have managed to run electronic voting system and electronic information booths. What differentiates the proposed method here and others is that it does not trust in any software or hardware and all the votes are counted both by software and by human watchers. Implementation of this design sounds relatively expensive; however, with the descending trend of digital equipment, it will soon become an economic option.

References

[1] Hosseinpour M. (2010) Analyzing security features of e-election protocols based on blind signature, Qom Higher Education University, Qom 70-130, summer 2010.

[2] Taj Neishabouri N. and Jalani Aliakbar (2009), Security requirements of e-election in electronic city, 2nd Int'l conference of e-city, Tehran, ITC research center, Jahad Daneshgahi, Tehran Municipality

[3] Dix A., "Electronic democracy and its implication for political privacy", 23rd International Conference of Data Protection Commissioners, September 2001, Paris,

[4] D. Balzarotti, G. Banks, M. Cova, "An Experience in Testing the Security of Real-World Electronic Voting Systems" , IEEE Transactions on Software Engineering, Vol. 36, pp. 453 - 473, May 2010

[5] S.M. Jambhulkar, J.B. Chakole, P.R.Pardhi, "A Secure Approach for Web Based Internet Voting System Using Multiple Encryption", International Conference on Signal Processing and Computing Technologies(ICESC), vol 4, pp. 371-375, jan 2014

[6] Jefferson, D. and Rubin, A. and Simons, B. and Wagner, D. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Online, Available from http://www.servesecurityreport.org/, last accessed 2014.

[7] Aviel D. Rubin. Security Considerations for Remore Electronic Voting. Communications of the ACM, 45(12), 2