SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIESNO. 144

ELECTRONIC VOTING – THE USE OF BIOMETRIC METHODS FOR GRANTING, WITHDRAWAL AND RECOVERY OF VOTERS' PERMISSIONS

Marcin SOBOTA[1*], Kamil BŁOŃSKI[2], Oliwia BROŻEK[3]

[1] Silesian University of Technology, Faculty of Applied Mathematics, Gliwice; marcin.sobota@polsl.pl, ORCID: 0000-0001-9564-472X
[2] Silesian University of Technology, Faculty of Applied Mathematics, Gliwice; kamiblo932@student.polsl.pl
[3] Silesian University of Technology, Faculty of Applied Mathematics, Gliwice; oliwbro901@student.polsl.pl
* Correspondence author

Purpose: The research paper presents the issues of voting with the use of electronic communication, with emphasis on the mechanisms of granting, withdrawal and recovery of permissions covered by biometric methods.
Design/methodology/approach: The work presents a theoretical model.
Findings: The proposed solutions ensure compliance with the basic requirements for e-voting, including verification of permissions, ensuring the secrecy of the vote and the possibility of verifying the vote cast by the voter.
Practical implications: The presented model of granting, withdrawal and recovery of voters' permission can be used as a part of practical electronic voting systems.
Originality/value: The authors presented a conceptual model of the use of biometrics to grant rights. The authors have not encountered in literature any examples of the use of biometrics for this purpose. Actually, anyone practically used system does not use biometry in the described scope.

Keywords: electronic voting, e-voting, electronic elections, biometrics, permissions.

Category of paper: Conceptual paper.

1. Introduction

Due to the widespread use of online services, such as electronic banking, online stores, e-mail, trusted profile or e-pity (electronic tax settlement system), more and more Poles are giving up traditional solutions for electronic services. In 2018, at least one computer was available in Poland in almost 82.7% of households, and 84.2% of them had access to the Internet (Statistics Poland, 2018). Based on this trend and the repeatedly discussed subject of electronic voting, it was concluded that replacing traditional voting with e-voting is only a matter of time.

Of course, this requires appropriate changes to the electoral law, but it is assumed that democratic elections should have the following characteristics (Election Code, 2011):

1. Only entitled voters can vote.
2. No one can vote more than once.
3. No one can determine who anybody voted for.
4. No one can duplicate anyone's vote.
5. No one can change anyone's vote without detecting this fact.
6. All voters can check if their votes have been counted in the final summary of the election results.

These characteristics reveal a paradox. On the one hand, the voter must be identified in order to verify their permissions to vote, and on the other hand, any information about their identity should be lost, so that it cannot be linked to the cast vote, while the voter can check how their vote has been counted.

For example, to ensure the secrecy of voting, when authenticating a person entitled to vote, appropriate protocols should be used that will prevent a situation in which the vote will be associated with the voter (Schneier, 2002).

The simplest protocol could look like this:

1. Each voter encrypts their vote with own private key.
2. Each voter encrypts their vote using the public key of the Central Election Commission (Główna Komisja Wyborcza – GKW).
3. Each voter sends their vote to GKW.
4. GKW decrypts votes, verifies signatures, calculates votes and announces election results.

Due to the fact that a digital signature was attached to the vote, GKW is able to link the vote with the voter, and there is only a matter of "trust" in GKW that such a link will not be made.

The scheme of granting permissions without the possibility of linking the voter with the permission is provided by the group of Professor Kutyłowski (Kutyłowski, 2009). The entitled person declares the will to vote via the Internet, which results in sending to their registered address via courier with a sealed envelope containing the document confirming the vote permissions (a similar mechanism is used, e.g., in the process of remote opening of bank accounts, where login credentials are placed in the envelope). The courier has a certain number of envelopes (the envelopes are indistinguishable), from which the addressee chooses one at random. This approach causes the voter to receive the permissions while the authority granting the rights (Permissions Committee) loses information about people using the given data. The envelopes are, of course, pre-numbered forms, so that a "leakage" of permissions does not occur. However, this solution does not take into account one important aspect – what if the envelope is lost?

2. Scheme of granting permissions

The possibility of casting a vote should depend only on voting permissions held, and the authorisation scheme should take into account situations such as lost or stolen tokens, envelopes with an identifier or in case a password is forgotten. Therefore, the authors propose the use of biometrics in order to grant, withdraw and recover the permissions to vote. Schemes of procedure are presented below.

2.1. Scheme for obtaining the identifier for the first time

1. Verification by the Central Election Commission (GKW) whether the person applying for an identifier is entitled to vote.
   1.1. If the person is entitled, go to step 2.
   1.2. If the person is not entitled, end the procedure.
2. Downloading biometric data.
3. Linking downloaded biometric data with an identifier.
4. Issuing an identifier by the official in such a way so that no one, aside from the recipient, would know this identifier, e.g. by issuing it in the form of a sealed envelope.

2.2. Scheme for obtaining the identifier again

1. Download biometric data and check if it is available in the database.
   1.1. If the biometric data is available in the database, go to section 2.
   1.2. If the biometric data is not available in the database, go to the scheme in section 2.1.
2. Removal of the identifier found on the basis of biometric data.
3. Linking biometric data with a new identifier.
4. Issuing the new identifier by the official in such a way so that no one, aside from the recipient, would know this identifier, e.g. by issuing it in the form of a sealed envelope.

The use of biometric methods can solve two basic problems related to the anonymity of voters and the principle of “one man, one vote”. These methods can be used in the above schemes for granting or recovering an identifier. In order to obtain the identifier, the person must go to GKW. After showing the ID card and the official finding that this person is entitled to vote (they are an adult, a citizen of the country, etc.), biometric data (e.g. biometrics of arrangement of blood vessels) are taken from them by the chosen method. After linking the biometric data with the identifier generated earlier by the computer, it is saved in the database. It is issued by an inserting machine in a sealed envelope to maintain the anonymity of the person receiving the identifier. The identifier is not linked with the personal data, but with the person (their biometric data).

Thanks to the use of identifiers, GKW is not able to verify for whom a given person has voted, but it has the ability to control the number of votes cast (one identifier constitutes one vote).

The thing which cannot be disregarded is the situation in which the voter loses their identifier (e.g. as a result of theft or fire). In the case of theft, there is the possibility of unlawful use of the identifier by another person. Therefore, it is important to delete the lost identifier and assign a new one to the given person. Even if the voter remembers their identifier, they are obliged to report such an event to GKW. A lost identifier is found using the biometric data linked with it. The found identifier is deleted, and then a new identifier is assigned to the person, as in the case of obtaining it for the first time. This is the only situation when the identifier is assigned again. It allows limiting the amount of work of offices, which is sufficient for the number of single-use identifiers.

The voter should have the possibility to cast a vote in a correct manner. Thanks to the application of identifiers, GKW can publish the list of votes cast with individual identifiers. This is the proven form of verification if there were no attempts to interfere in the results of elections.

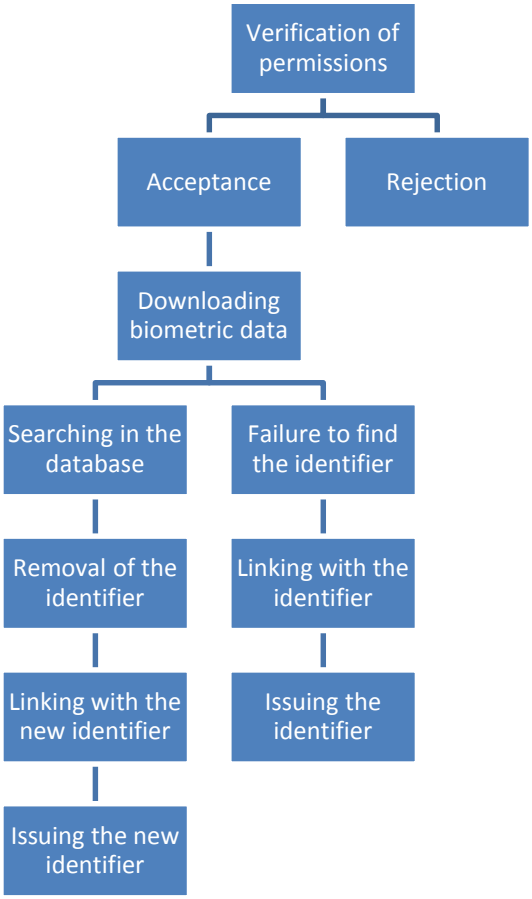

Figure 1. Scheme of granting, withdrawal and recovery of voting permissions. Source: own work.

3. Description of selected biometric methods

The proposal to use biometric features as a component connecting the voter with their permissions results from the fact that biometric features accompany us (with some exceptions) throughout life, and they are something that cannot be "lost" or transferred to a third party. In addition, the selection of a rare method guarantees that no one else keeps records of these features, and there is no possibility to associate (using other databases) a person with their personal data. The following describes several possible biometric methods that present the aforementioned characteristics, and the specific selection of which lays beyond the scope of this study.

3.1. Voice biometrics

The human voice, just like fingerprints, is unique. Voice-based verification is a safe, simple and low-cost solution. The voice authentication system is particularly convenient when the user wants to get fast and secure access to protected data and services, e.g. bank account or insurance information by phone (Anonymous, 2016).

There is a distinctive difference between the concepts: Biometric identification and biometric verification. The identification process consists in selection of one voice sample from many, while verification consists in confirmation of the declared identity.

In terms of voice biometrics, the voice sample constitutes a password. However, it is not the spoken content, but the characteristics of person's voice. The password should not be too long and complex, nor should it be a tongue twister and hard to say, which could cause errors. In order to correctly extract the voice characteristics, the password must be phonetically diverse and not difficult to pronounce. In practice, such passwords should have from 8 to 15 syllables.

The database stores the voice-print – statistical summary of the recording, instead of recordings of individual persons. This summary makes it impossible to play the recording and to be used by unauthorised persons.

There are methods by which you can determine if the sample does not come from a copy of the sample or the recording being played back. The human always pronounces the password in a different way. Therefore, the system should only accept voice samples of quality sufficient for the purpose of analyses. The factors which negatively affect the quality of the sample are noise and severe throat diseases (e.g. laryngitis) of the person providing the sample. Hoarseness and the common cold do not have a significant impact on quality of the recording.

Operation of the system depends on implementation of the algorithm used within it. Such a system learns the characteristics of the voice based on the master data from the sample, using, for example, a neural network. Both biological and behavioural features, the way of speaking, vowel length (a phenomenon characterised by differentiation of the duration of

syllables or sounds), speed and combinations of these factors are analysed. Human is unable to describe these dependences clearly enough to, for example, forge a sample.

Unfortunately, this method for confirming the identity of a person is optimal when we know their other data, such as name, surname, PESEL No. (Personal Identification Number). When it is required to compare the sample with many others, the effectiveness of this method will be much lower. Thus, the advantage of using this solution to authenticate voters is its affordability and simplicity. A microphone is definitely a simpler, cheaper and more common device compared to, for example, fingerprint readers. The disadvantage, however, is the poor efficiency in searching for a specific sample in the database.

3.2. Iris biometrics

In 1885, when prisoners were identified in a Paris prison based on the iris of the human eye, it was noted that it had unique characteristics. This identification consisted mainly in recognising the colour of the iris by a human. In the works of Adler from the 1960s, there is information confirming the uniqueness of iris of the human eye.

The colorant, also known as melanin, which is located in the opaque part of the choroid, forms a unique pattern, through which identification can be performed. The human iris is formed during the first two years of life and disappears within five seconds after death. There are no changes in the characteristics of the iris throughout the life of an individual, except for mechanical damage or cancer. One of the most important properties of this method is that it has 266 characteristic points. There are almost five times more than when using fingerprint biometrics. The iris remains unique even in identical twins.

In the first step, the iris scanner performs a general facial recognition to find the eyes. A dedicated video camera then takes a high resolution picture. In the next stage, it changes the image into a rectangular form, from which eyelashes and pupils are removed. Subsequently, the image is converted into a binary code, which contains a short description of the characteristic points. In the last step, the downloaded code is compared to the codes stored in the database. Data encryption is possible. Based on the binary code, it is not possible to reproduce the human iris.

However, iris biometrics feature many significant disadvantages. The first of them is the high cost of equipment compared to other biometrics methods. Currently available scanners are difficult to adapt for people of different height. The most important disadvantage of this solution is that the scanner can be cheated with a good-quality photograph of the eye (Czajka, 2002).

3.3. Biometrics of arrangement of blood vessels

The biometrics of arrangement of blood vessels is currently one of the safest technologies used for authentication. These days, methods such as fingerprint scanning or voice authorisation are commonly used (fingerprint readers and microphones are now available in every laptop or smartphone), which may compromise the security of these methods in the future.

The biometrics of the arrangement of blood vessels is more accurate than using the iris of the human eye, fingerprint or appearance of the face. It is harder to copy or forge data obtained with this method.

The reader of arrangement of blood vessels is a small device, on which the individual places their palm. It uses infrared radiation that is absorbed by haemoglobin in the venous blood and creates a shadow. Such a shadow reveals the network of blood vessels. The image is then processed into an encrypted, shortened biometric code, which is a unique password.

In order to verify the person, the downloaded data is analysed and compared to the pattern via software, and the compliance or non-compliance of the sample and the pattern is determined.

The pattern includes not only the blood vessel arrangement of the hand, but also recognition by the system of the veins that blood flows through, so the arrangement itself is insufficient for the sample to be accepted.

In terms of the level of security of the described method, it is definitely safer than, for example, scanning the iris or fingerprints (Kopańko, 2018). Cameras are taking better and better photographs, so impersonating someone using their photo is getting easier. This is also the case with a fingerprint, which can be reproduced based on photographs.

The circulatory system is more difficult to reproduce, as during the scan it checks if there is blood flowing through the veins. Theoretically, a copy of blood vessels in the hand can be produced, but this process is very expensive. The circulatory system cannot be photographed with a digital camera or reproduced like a fingerprint on the basis of the imprint left on the item.

This solution can be used for human verification and identification. Therefore, the use of this solution in the authentication of voters would have many advantages, and the only disadvantage would be the costs associated with implementation of this method.

3.4. Three-dimensional face biometrics

The face of every human being is the basis for identification. One's picture is placed on all kinds of documents, such as ID cards, passports, driving licenses or student cards. The human eye has become specialised in face recognition. Even a new-born, several-day-old child is able to recognise faces sometimes.

Three-dimensional face identification features significant advantages compared to the two-dimensional technique. It allows for the elimination of defects occurring in case of using two-dimensional identification algorithms, such as change of lighting, facial expression, aging process or position of the face in relation to the reader.

For proper operation of a biometric system based on 3D face recognition, a 3D, 2D or infrared camera is necessary. The image processing process enables detection of the face, its identifying marks and removal of the unnecessary area that does not include the face. Hair, surrounding space and changes caused by the face's position in relation to the camera are

reduced. In the three-dimensional identification process, the most characteristic feature is the nose.

Depth and face texture maps can be produced using various techniques. One of them is stereoscopy, which utilises the system of multiple cameras. Another technique is application of laser devices and 3D scanners. The first approach corresponds to a system in which the data format used at the training stage would be the same as during testing. The results of this method are promising, but it cannot be used in identification systems based on drawing the texture of the face image from one video camera or reader. The second technique can be used in situations where 3D data is used during the training, whereas 2D data is used only during testing. The disadvantage of this approach is the enormous demand for computing power needed to match downloaded 2D images to their three-dimensional models.

The first works on a geometric face recognition model was started over a decade ago. In 2007, Riccio and Dugelay proposed an approach based on sixteen geometric invariants calculated on the basis of characteristic points. The 2D and 3D face images are linked thanks to the determined geometrical invariants, and the efficiency of this technique depends, to a large extent, on the accuracy of location of characteristic points. In 2009, Elyan and Ugali presented a model in which the main objective was to determine the profile of symmetry along the face. This profile was determined by calculating the intersection of plane of symmetry with the face grid, which resulted in the creation of a curve which shows the symmetry of the face. After the correct determination of the axis of symmetry, several characteristic points are calculated. They are necessary to calculate other facial features. It has been assumed that the tip of the nose constitutes a symmetry profile (Naser, 2011).

Due to computational complexity and expensive equipment, 3D technology is still not widely used. Moreover, the image obtained from 3D cameras needs much more storage space compared to 2D images. Further research on improving this method is being carried out. In the near future, this may prove to be one of the best biometric identification methods.

3.5. Biometrics of typing dynamics

Keystroke recognition is defined as the process of measuring and estimating the rhythm of writing on digital devices, including: computer keyboards, mobile phones and touchscreen panels.

Keystroke recognition, often referred to as “keystroke dynamics”, refers to detailed information on the manner of typing, which accurately describes when each key was pressed on the device and when it was released. Based on this information, the person can be clearly identified. Although biometric data is based on physical characteristics, such as a fingerprint or face or behavioural traits, many consider keystroke dynamics as a biometric method (King, 2016).

Keystroke dynamics identifies people based on the pattern of typing, the rhythm and speed. The measurements used for keystroke dynamics are known as “dwell time” and “flight time”. Dwell time is the time in which the key is pressed, and flight time is the time between keystrokes. Keystroke dynamics can therefore be described as a software-based algorithm that measures the dwell time and flight time to authenticate one’s identity.

In 2004, researchers from MIT (Massachusetts Institute of Technology) explored the idea of authentication using the biometrics of keystroke dynamics. The main advantages of this method are low expenditure on hardware and the ability to use low-bandwidth connections for data transmission. The main disadvantages are the effect of, for example, tense muscles or sweaty hands, or irregularity and inconsistency of patterns, and a high correlation between keystroke dynamics and the need to use different types of keyboards.

4. Summary

This research paper touches upon the problem of ensuring secrecy in electronic voting. The first part proposes the use of an identifier linked with biometric data, instead of personal data, in order to prevent the Electoral Commission from linking the voter with the cast vote. Thereafter, the scheme of assigning the identifier to the person entitled to vote and the authentication scheme of the person who lost the identifier are discussed. The next part of the paper describes selected biometric methods that could be applied in the described schemes of granting permissions.

References

1. *Biometria głosowa – merytorycznie o weryfikacji na podstawie głosu*. https://e-ochronadanych.pl/biometria-glosowa-merytorycznie-o-weryfikacji-na-podstawie-glosu/, 21.03.2016.
2. Czajka, A., Pacut, A. (2002). Biometria tęczówki oka. *Techniki Komputerowe, Biuletyn Informacyjny*, 5-18. http://zbum.ia.pw.edu.pl/PAPERS/IMM2002_Czajka_Pacut.pdf.
3. Kapczyński, A. (2016) Critical success factors in managing biometric authentication systems implementation projects. *Zeszyty Naukowe Politechniki Śląskiej*, pp. 291-296.
4. King, R. (2016). https://www.biometricupdate.com/201612/explainer-keystroke-recognition.
5. *Kodeks wyborczy*. https://pkw.gov.pl/pliki/1517307863_kodeks_wyborczy_-_2018.pdf. 05.01.2011.

6. Kopańko, K. *Stań się swoim własnym hasłem. Polacy pracują nad biometrią dla Fujitsu*, https://www.spidersweb.pl/2018/03/fujitsu-palmsecure.html, 02.03.2018.
7. Kutyłowski M. *E-voting: głosowanie elektroniczne*. http://orka.sejm.gov.pl/WydBAS.nsf/0/701C7F09ABFE5C84C12575BD002DE087/$file/Infos_57.pdf, 21.05.2009.
8. Naser, Z. (2011). *New Approaches to Characterization and Recognition of Faces*, https://www.intechopen.com/ books/new-approaches-to-characterization-and-recognition-of-faces/3d-face-recognition#B57.
9. Schneier, B. (2002). *Kryptografia dla praktyków*. Warszawa: WNT.
10. Sobota, M. (2015). Społeczno-ekonomiczne aspekty głosowanie elektronicznego. *Zeszyty Naukowe Politechniki Śląskiej*, *Seria: Organizacja i Zarządzanie, 86,* Gliwice, pp. 519-526.
11. Sobota, M. (2016) Wybrane aspekty głosowanie elektronicznego. *Zeszyty Naukowe Politechniki Śląskiej*, *Seria: Organizacja i Zarządzanie, 96,* pp. 417-425.
12. *Społeczeństwo informacyjne w Polsce w 2018 roku*. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2018-roku,2,8.html, 22.10.2018.