Facial Recognition for Remote Electronic Voting – Missing Piece of the Puzzle or Yet Another Liability?

Sven Heiberg[1], Kristjan Krips[2,3], Jan Willemson[2][0000−0002−6290−2099], and Priit Vinkel[2,4][0000−0003−0049−1287]

[1] Smartmatic-Cybernetica Centre of Excellence for Internet Voting
Soola 3, Tartu, Estonia
sven@ivotingcentre.ee
[2] Cybernetica, Narva mnt 20, Tartu, Estonia
{kristjan.krips,jan.willemson,priit.vinkel}@cyber.ee
[3] Institute of Computer Science, University of Tartu, Narva mnt 18, Tartu, Estonia
[4] State Electoral Office, Lossi plats 1a, Tallinn, Estonia

Abstract. Reliable voter identification is one of the key requirements to guarantee eligibility and uniformity of elections. In a remote setting, this task becomes more complicated compared to voter identification at a physical polling station. In case strong cryptographic mechanisms are not available, biometrics is one of the available alternatives to consider. In this paper, we take a closer look at facial recognition as a possible remote voter identification measure. We cover technical aspects of facial recognition relevant to voting, discuss the main architectural decisions, and analyse some of the remaining open problems, including dispute resolution and privacy issues.

1 Introduction

Recent years have set the stage for biometrics to be widely adopted by end-users. Fingerprint readers have become available for a large variety of smartphones, while more and more devices are being integrated with facial recognition systems. In parallel, FIDO Alliance and W3C have been working on the FIDO2 project to support passwordless authentication via browser API-s. This resulted in the WebAuthn specification, which was first published in 2019 [5]. It is complemented by the Client to Authenticator Protocol (CTAP), allowing FIDO2 enabled browsers to communicate with external authenticators like smartphones [6]. As a result, WebAuthn makes it possible for websites to authenticate users via smartphone-based biometric sensors [33].

The prospect of having easy access to biometric verification can have a significant impact on the field of remote voting. Apple has already hinted that they are thinking about iPhone based voting[5], which would likely have to contain a

[5] https://www.businessinsider.com/apple-ceo-tim-cook-on-voting-technology-iphones-smartphones-2021-4

built-in authentication system. Thus, it is conceivable that in a few years, identity could be tied to users' smartphones. However, biometrics can also be utilized by the identity providers, be it the state government itself or commercial service providers.

Due to the hardware-based restrictions on end-user devices, there are two options to consider for biometric verification – based on fingerprints or facial images. The former can be bypassed by copying the fingerprints, creating master fingerprints or even by forcibly using the victim's finger to unlock the device [35,45,50]. The latter has had issues with liveness detection being bypassed [54]. However, the emergence of end-user devices that use special sensors for face recognition has raised the bar for attacks [17].

In principle, facial recognition has the potential to solve several issues that plague remote Internet voting (i-voting). First, it could act as an additional authentication factor, which could help to deploy remote voting to the settings where voters do not have a strong electronic identity. Second, facial recognition could be used as an additional measure to fight coercion. Third, active liveness detection could reduce the risk of voter's credentials being used without their knowledge. The latter could also partially mitigate the threat posed by malware located in the voter's device. By combining liveness detection based facial recognition with individual verifiability, it would be more difficult for malware to silently access voter's credentials or cryptographic tokens to cast a vote.

The aforementioned aspects seem promising, but they come with significant downsides, with the privacy issues being on the top of the list. For the additional security guarantees to work, facial recognition would have to be a mandatory part of the voting process. However, that would automatically disqualify the voters who do not have cameras of sufficient quality. In addition, by relying on biometrics, there are always cases of false positives and false negatives. Thus, biometric systems will inevitably fail to correctly identify some eligible voters and thereby limit access to their democratic rights.

Therefore, it seems that even in case facial recognition could be used for remote voting, it would have to have an alternative to allow all eligible voters to participate in elections. This brings us to the question of proportionality and the cost-benefit analysis. Thus, one of the goals of this study is to find out whether it is feasible to find a balance between the additional security features, privacy issues, and usability aspects. In addition, we aim to encourage further discussion and research in the context of using biometrics in elections.

This paper gives an overview of the possibilities for integrating facial recognition with remote electronic voting and discusses the risks of introducing such a feature. Section 2 gives an overview of state of the art, election-related aspects and deployment examples. Next, in Section 3, we give an overview of the architectural questions. This is followed by Section 4 that covers the general issues of integrating facial recognition into voting systems. Finally, Section 5 presents a discussion on further technical aspects, and Section 6 draws some conclusions.

2 State of the art

2.1 Facial recognition

Facial recognition consists of two main steps. First, faces have to be detected from an image and converted into a vector of facial features. Second, the captured facial features have to be compared with a reference value.

The complexity of the comparison task depends on whether there is a single predefined reference value available or the task is to find the matching facial feature vector from a large database. The former task is called facial verification, and it occurs, for example, when biometrics is used to unlock the phone or when a document photo is used as a reference value. The latter is called facial identification, and it may occur, e.g. in cases when a law enforcement agency needs to identify suspects. In this paper, we only focus on facial verification and consider this an addition to the existing authentication measures. Thus, we assume that election organizers already have a list of eligible voters and do not have to rely solely on facial recognition to identify voters.

Biometric solutions have an inherent issue with reliability as the biometric sensors do not always capture exactly the same measurements [41]. Thus, clever optimizations are used to compare the relevant values. However, as the biometric readings can vary even with the same person, there must be a threshold for identifying users. This results in false positive and false negative identifications. Their ratio depends on the selected matching threshold, which means that an optimal balance has to be found between these properties. For example, according to the Face Recognition Vendor Test by NIST, when the false positive rate is tuned to be below 0.00001, the corresponding false-negative rate is around 3% for the current best algorithms in case the images are taken in an uncontrolled (*wild*) environment.[6]

As facial verification may be performed in an uncontrolled environment, there have to be measures that prevent spoofing attacks. One obvious problem is detecting subject liveness, i.e. making sure that a still image is not shown into a camera instead of a real person. Active liveness detection methods ask the user to follow the given guidelines to either blink one's eyes, rotate the head, move the lips or raise an eyebrow [54]. A passive liveness detection functionality checks the consistency of the captured data. For example, it is possible to compare the texture of the face to identify spoofing attacks [40,28] and to use smartphone's motion sensors with the captured data to detect video replays [32]. However, a paper by Xu *et al.* published in 2016 showed that the aforementioned liveness detection measures could be bypassed by utilizing virtual reality systems to create 3D representations of faces [54]. One way to detect such an attack is to use hardware that contains sensors that measure the depth of the face.

[6] `https://pages.nist.gov/frvt/html/frvt11.html`

2.2 Elections and biometrics

Biometric identification of voters in the election process has been a viable alternative to manual identification at least for the last 20 years. Such identification methods have found acceptance in coherence with the introduction of other election technology innovations like ballot-scanning or electronic voting in polling stations [13]. The use of biometric data shows the greatest promise in situations where printed voter lists and physical identification documents do not offer the needed level of trustworthiness and accuracy. For example, according to [26], there were 28 countries in Africa using biometric voter registration (verification) in 2019. In the case of remote voting, the need to use biometric data for identifying the voters stems mainly from the lack of access to a viable electronic identification alternative [44].

In almost all of the current cases linked to elections or voting procedures, the use of biometrics is limited to a regulated and controlled environment, e.g. the polling station. The most common biometric characteristics used to identify voters are fingerprints and the visual appearance of the voter.

A report by Wolf *et al.* states that the accuracy of biometry used for identifying or verifying voters is strongly influenced by the quality of the data and the capturing environment [52]. All principles have to be seen as best practice and experience because there is no normative regulation or internationally regulated recommendations on this matter.

Besides false positive and false negative rates, there are two other important technical parameters of biometric identification or verification that have to be taken into account. The failure-to-capture rate describes the cases that prevent biometric data from being captured. The failure-to-enrol rate, at the same time, represents the cases where the quality of captured biometric data prevents a match to be found.

Voters affected by either of these issues can not be reliably identified or verified by biometrics. However, it is not possible to predict, which voters will not be able to use biometry. The aforementioned issues could occur regardless of whether the reference values are provided by the election organizer or the voter. Thus, all automatic identification or verification procedures should have a human fallback procedure and/or alternative solutions for problems that could disenfranchise numerous voters.

2.3 Some facial biometry deployment examples

Fiji has used biometrics (both facial images and fingerprints) for voter registration and maintaining the accuracy of the voters list (e.g. removing duplicates) [52].

Mongolia has gone a step further. Biometric information is also gathered in the voter registration process, but fingerprints are also scanned in the polling stations. The voter's fingerprint is matched against the registration database, and the voter's picture is displayed on a screen so that everyone in the polling station can identify the voter. The voter is then issued a paper receipt and may proceed to cast her vote [52].

Nigeria has had several generations of electronic identification projects. The latest one has been used for elections since 2011. The electoral roll (voter list) has biographical data of the voter along with 10 fingerprints and a facial image. In recent years the biometric data set has been loaded on permanent voter cards, which are used in the polling stations to verify voter identity. On election day, the voter is verified based on the pre-captured picture (manually by polling station workers) and by comparing the voter's scanned fingerprints to the available data. As the failure-to-capture rate of the verification process was regionally very different (due to equipment malfunction, faulty cards, etc.), all voters who were identified manually but had troubles authenticating based on biometrics were allowed to vote nevertheless [52].

Canada started to use mobile application based voting in early 2021 to facilitate House of Commons voting during COVID-19 conditions. Voting has to be performed on a parliament-managed smartphone which verifies the identities of Members of Parliament (MP) by using a facial recognition procedure. The official picture on file with the office is compared to a live photo taken with the help of a mobile device. As a fallback and an additional security layer, the whip of every party group has the right to verify the identity of the MP in case discrepancies are still present after two attempts of facial recognition. The MPs have 10 minutes to take up the voting procedure [42,25].

West Virginia, U.S. is one of several states piloting different versions of remote electronic voting for a limited number of voters residing abroad. In 2018, the state introduced voting via mobile phone for abroad voters. The voting procedure relied on a standalone application, which used facial recognition to verify voter identities. More specifically, the reference data was acquired by photographing an ID document, which was later compared to a live photo of the voter. After facial recognition, if available for the device, the voter provided a fingerprint for additional identification when prompted during the voting process. No alternative authentication methods were applied in case of facial recognition failure [21,36].

In addition to the above-mentioned examples, facial recognition has also been piloted or used for voter registration or identification purposes in several countries including Afghanistan[7], India[8], Ghana [9] and Tanzania [18].

[7] `https://www.afghanistan-analysts.org/en/reports/political-landscape/afghanistans-2019-election-23-disputed-biometric-votes-endanger-election-results/`

[8] `https://www.thehindu.com/news/national/telangana/telangana-state-election-commission-successfully-tests-facial-recognition-technique/article30627812.ece`

[9] `https://www.idea.int/sites/default/files/managing-elections-under-covid-19-pandemic-conditions-the-case-of-ghana.pdf`

3 Architectural questions

Before it is possible to assess the impact of facial recognition, it has to be analysed how it can be integrated into i-voting systems. It turns out that there are both process-related and technological restrictions, which limit the applicability of facial recognition.

3.1 At which stage to use facial recognition?

Voting is a multi-step process and there are potentially several steps where facial recognition can be integrated into.

The election organizer must already have a list of eligible voters as otherwise remote authentication would not be possible. Thus, we leave the process of voter registration out of scope and consider authentication as the main use case for facial recognition. This brings us to one of the core problems of i-voting, which is the necessity to reliably authenticate voters in a possibly malicious environment.

Following the approach familiar from the paper voting, biometric authentication can be used as a part of eligibility verification. The voter has to convince the authentication module of her identity before she is allowed to proceed. A separate question is whether biometric authentication is sufficient or should other identity verification mechanisms be used as well. In general, the answer to this question depends on the type of elections, used biometric technology, and whether an alternative authentication system is available. However, according to NIST's Digital Identity Guidelines, biometrics should only be used together with a physical authenticator [22].

It also has to be decided whether failure in facial recognition should block the voter from voting, potentially leaving the voter without the option of exercising her constitutional voting rights. In case no alternative authentication measures are available, the failure must be blocking as facial recognition is the only way to check eligibility.

If several authentication mechanisms are used in parallel, one needs to decide what to do if they do not concur. There is no universal, straightforward answer to this question, and it eventually comes down to dispute resolution mechanisms (see Section 4.1).

It may also be possible to integrate facial recognition into the vote submission stage. However, the above-mentioned problems remain. Additionally, the user experience will suffer as the voter would now be allowed to almost complete the voting process and is informed about a potential facial recognition failure only in the very end.

3.2 Compatibility with different i-voting protocols

The possibility to integrate facial recognition into an existing i-voting protocol depends on the general architecture of the protocol along with the provided security guarantees. More specifically, the requirements for voter identity verification and participation privacy have to be evaluated. To get a better understanding of the area, we give our assessment on whether facial recognition could be integrated with different types of voter verification schemes.

There are several possible strategies for verifying voters in the remote electronic voting setting. In this paper, we will look at interactive authentication protocols, digital signatures, ring signatures, zero-knowledge proofs, anonymous credentials and blind signatures.

First, in the simplest case, the voters have to authenticate themselves before they are authorized to cast a vote. In general, there are two approaches for authentication – either the voter is given voting credentials during registration, or the voter uses a general-purpose authentication system. For example, this type of authentication has been used by Helios based voting schemes [1,16,9], Norwegian i-voting system [51], Swiss Post i-voting system [48], and the Estonian i-voting system [24]. In such cases, authentication is decoupled from vote casting, which in principle makes it easy to add facial recognition into the authentication step of the voting protocol.

Second, voters could be identified based on their ability to issue digital signatures. This is usually implemented by requiring voters to sign the ballots that are going to be submitted to an append-only bulletin board. This type of voter identification is used, for example, by the Estonian i-voting system[10] and by Selene [46]. As abstention can also show political preference [15, par. 54], votes with signatures pointing directly to the voters should not be simply uploaded to a public bulletin board. Similarly, it becomes questionable whether biometric verification results could be posted to a bulletin board. It is unlikely that even a numeric representation of biometric data could be shared on a bulletin board due to legislation, privacy concerns, and issues related to the reuse of biometric data. Thus, an additional authentication step would have to be introduced before voters are authorized to cast a vote. To adhere to the system's transparency, proof of a successful biometric match could be added to the bulletin board. This could be represented by a signature issued by the party responsible for performing the biometric verification. However, that would complicate the auditing process while still leaking the list of voters who participated in the election.

Third, eligibility verification can be built on top of ring signatures [43]. By issuing a ring signature, the identity of the signer remains anonymous. For example, this kind of approach is used by Eos [39]. Thus, voters are not explicitly authenticated, and bulletin boards do not contain information that could identify the voters. As the general idea of such an architecture is to protect the voter's anonymity, the thought of adding facial recognition seems to be counterproductive to the overall goal.

Fourth, voters can prove their identity by creating zero-knowledge proofs, for example, about the knowledge of their secret keys, while also protecting their participation privacy. This approach is used by KTV-Helios [31]. It becomes apparent that in case the election system is designed to achieve participation privacy, facial recognition would conflict with that goal.

[10] The Estonian i-voting system also requires voters to explicitly authenticate themselves before they are allowed to sign their ballots.

Fifth, voters can use anonymous credentials, which are blindly compared by the election system against the list of registered voters. Such an approach is used by JCJ [27] based voting systems like NV-Civitas [37] and Selections [14]. JCJ is built on top of the coercion resistance definition by Juels *et al.* [27], which also states that it should not be possible to force voters to abstain. Thereby, it must not be possible to prove whether a voter participated in the elections. To protect voter's privacy, the anonymous credentials are validated by relying on zero-knowledge proofs and mix-nets. Thereby, facial recognition is not compatible with the voting phase as the vote casting act is designed to be anonymous. However, the critical step in the aforementioned schemes lies in the registration phase, which is assumed to be performed by eligible voters. Thus, the registration process could be augmented with biometrics-based authentication like facial recognition.

Sixth, the identification protocol can rely on blind signatures as proposed by David Chaum already in the 1980s [11,12]. For example, the voting system proposed by Okamoto integrated blind signatures into the authorization phase [38]. This allows the voting system to check eligibility during registration while remaining oblivious of whether the voter has cast a vote or not. Thus, facial recognition could only be used to check eligibility before issuing a blind signature.

3.3 Is a semi-controlled voting environment achievable?

One of the key characteristics of remote electronic voting has been the uncontrolled voting environment. For the polling stations, there are rules determining what a polling station should be like – there usually are mandatory elements (e.g. ballot boxes), mandatory activities (e.g. sealing of those ballot boxes), forbidden elements (e.g. campaign materials) and people responsible for maintaining the order (e.g. election officials). In the case of remote electronic voting, no such preconditions hold, which often leads to the question of coercion.

In a polling station, election officials help to ensure that everybody has a chance to vote alone. In the remote setting, this kind of prevention is not possible. A number of mitigating measures have been proposed in the literature; see [30] for an overview. In practice, for example, the option of re-voting has been implemented in Estonia [34] and Norway [51]. However, this measure has also been disputed both legally and in the academic literature [19,9,34].

Given that facial recognition could be used to verify that the voter is really present when the corresponding credentials are being used to cast a vote, it is appealing to extend this idea and check the suitability of the voting environment to make sure that the voter is truly not in a coercive situation. In case video streams are already used for facial recognition and liveness detection, the length of the stream could be extended to cover the entire voting process such that the and the whole remote voting environment could be monitored.

This approach would not be novel, e.g. it has been already used in remote examinations to prevent cheating [2]. Such systems ask the examinee to switch on the microphone and use the camera to show the room before the examination can start. Additional passive and active restriction and monitoring methods may be used. Sometimes the examinee is under-recorded surveillance throughout the process. It may last hours with specific restrictions such as the requirement to stay visible, not to talk, not to cover ears or mouth, etc.

This approach is technologically feasible and may be politically appealing but comes with several caveats.

1. The proctoring systems come with negative cognitive side-effects. For example, a study published in 2021 described the accompanying risks like the anxiety of being watched on camera [3].
2. The proctoring systems complicate the requirements for the device suitable for voting and for the network throughput to ensure a steady stream throughout the process.
3. Since proctoring systems usually involve a human being in monitoring the process; it is going to reduce the throughput and increase the cost of online voting.

This kind of approach also raises questions about voter privacy. More specifically, whether the efficiency of this measure in mitigating the risk of coercion is sufficient to justify voting under surveillance. While privacy-preserving facial recognition could solve some of the privacy issues, its low performance prevents large scale deployments [10]. In addition, it is rather unclear if it would convince the layman of the trustworthiness of the system.

Without relying on privacy-preserving technologies, there is a significant risk that the voter could accidentally reveal the voting credentials or the vote itself, thereby violating the vote secrecy requirement. For example, this could happen in case the voter has written down the credentials or candidate names, but also in case the camera is pointed towards reflective materials [4,53]. In addition, a video of hand gestures can leak information even when the keyboard is not visible [49,47]. Thus, it is the opinion of the authors that such an anti-coercion measure will not be accepted by democratic societies due to the accompanying privacy issues.

4 General issues with facial recognition

4.1 How to resolve disputes?

Biometric authentication is probabilistic, which means that facial recognition is not guaranteed to produce the correct outcome. In addition, the algorithms can be biased due to the used training data.

For example, a study performed in 2018 revealed that the facial analysis benchmark datasets Adience and IJB-A over-represented lighter-skinned subjects, with the former consisting of 86.2% and the latter 79.6% of the samples [7]. The study also tested three commercial gender classification systems and found that the classification error for dark-skinned females can reach up to 34.7%. Such an outcome is illustrated with real-life examples. As an extreme case, it was claimed by the Detroit Police Chief that facial recognition software misidentifies subjects 95% of the time[11].

A NIST study from 2019 compared more than one hundred facial recognition algorithms and identified that many of them tend to have a demographic bias due to the used training data [23]. Still, the best performing identification and verification algorithms did not show a significant demographic bias.

However, it was already mentioned in Section 2 that even the best algorithms could have a false negative rate of around 3%. This share is significant enough to require dispute and compensation mechanisms to be implemented. If automated facial recognition algorithms fail to identify or verify the voter reliably, the only real alternative is a human. This means that the voter identification or verification protocol must allow for a fallback to a human operator and that a team of operators must be available throughout the whole voting period.

Due to the uneven distribution of voting events, it might not be possible to do human verification in real-time. Thus, a question arises on how to store the captured images so that voter's privacy would not be violated. What happens in case a human verifier decides that the captured photo does not match the reference image? If the verification is done in real-time, the voter could restart the process and take another photo. However, with a delayed verification there are two paths to take. Either the voter is allowed to cast a vote with the pending facial verification result, or the voter is put on hold. In the former case, the voters may get a false sense of their ballots being accepted, while the latter might prevent voters from voting at all.

Another interesting question focuses on the post-election audits in case the facial verification images are stored. What happens if an auditor decides that some of the facial verifications resulted in an incorrect match? If the voting system is designed to protect ballot secrecy, it should no longer be possible to match ballots with the voter identities. Thus, such audits and disputes should be handled during the election period.

4.2 Privacy

Regardless of the other factors, the main barrier to implementing facial recognition is the risk to voter's privacy. Depending on the implementation, voter's private data could be leaked in multiple ways.

The main presumption for facial recognition-based identity verification is the existence of a reference data set, which the captured facial image could be compared to. Unless voters have already shared their biometric data with the government, it is unlikely that facial recognition could be used for remote voting. Thus, the first step for the election organiser is to check whether any existing government databases could be used for this purpose. An alternative is to use government-issued ID-s that contain a photograph.

[11] https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time

There are several commercial services that offer document-based facial recognition. In general, they require the state-issued document to be scanned with the smartphone, with the resulting image used as a reference for performing facial recognition-based identity verification. However, relying on a commercial service to handle biometrics for something as critical as elections raises multiple questions. First, voters may not feel comfortable revealing to a third party that they participated in the elections. Second, the service provider could, in principle, create a data set consisting of all eligible voters. Third, by performing facial recognition, some background is also captured by the camera. This raises the question of who has access to these images as they might contain private information about voters homes.

Initially, it may seem that the answer to the aforementioned issues lies in locally performed facial matching, for example, by using the voters' smartphones. However, it quickly becomes clear that offline facial recognition involves risks that could lead to the measure being bypassed. For example, the facial recognition application running in a hostile environment could be tampered with. Thus, an active process involving the server is required to prevent the matching result from being locally modified. On the other hand, voters may not be comfortable with their photos being sent to the voting system or a third-party service provider. Such a design would also not work with voting protocols that protect voter's privacy already when the ballot is being submitted as described in Section 3.2.

Another interesting question concerns the transparency of the facial recognition system. The owners of proprietary services are not motivated in disclosing how their liveness check is implemented to prevent it from being bypassed. Thus, it is unlikely that the facial recognition components would be fully open source. This is not a major issue in case facial recognition is decoupled from the voting application, as in such a design it would not prevent the voting client from being fully open-source.

5 Discussion

In case facial recognition is integrated into the authentication phase, it would effectively become an additional authentication factor. Therefore, the question of whether facial recognition should be included in remote online voting becomes a question about voter authentication.

There are multiple ways how voter's credentials could be accessed without the voter's knowledge or permission. This could happen due to the usage of an insecure distribution channel like email, SMS, or post. However, the credentials could also be maliciously accessed by malware or family members. By including facial recognition in the authentication phase, such attacks become more difficult to conduct.

In case existing authentication solutions already rely on cryptographic tokens that are delivered over a secure channel, facial recognition could be added as a liveness check. This could deter malware from using the cryptographic tokens without the voter's knowledge and make it more difficult for family members to use the tokens. However, the latter holds only in case the facial recognition technology includes a liveness detection system that is difficult to spoof.

Even when such a system could be implemented, its reliability would depend on the environment, end-user devices, and usability aspects. As facial recognition is sensitive to the surroundings, the background and reduced lighting conditions can lower the accuracy of voter identification [55]. Besides that, voters might be reluctant to adopt the technology due to privacy issues, demographic bias [7], or cultural aspects. For example, it has been argued that some women won't be able to vote in Afghanistan due to the usage of facial recognition[12].

The unconstrained voting environment creates the need to support cameras with varying levels of quality. For example, the web cameras integrated into laptops tend to be outperformed by external web cameras[13]. In addition, our interviews with the facial recognition service providers revealed that smartphone-based face recognition is preferred due to their cameras being superior to cameras used on desktop computers.

In case the voting system has to rely on low-quality web cameras, it would be difficult to predict the error rate. Thus, there is a strong incentive only to support smartphone-based facial recognition. However, as a negative side-effect, that would disenfranchise the voters who do not have or can not use a smartphone. Of course, the election system might support other voting options, but these may also not be available to some voters. In case of technology would significantly simplify the voting process for only a part of the electorate, it would effectively result in an increase of inequality regarding voting freedom.

The possibility to introduce biometry depends on multiple aspects like the jurisdiction, end-user devices, and the quality of reference datasets. For example, the EU's GDPR sets limitations for processing special categories of personal data. According to Article 9 of GDPR, the usage of biometric data is very limited unless the subjects give their explicit consent [20]. Thus, each voting event should be analysed in the given context when planning to introduce biometric identity verification.

6 Conclusions

We have described in this paper that facial recognition has the potential to solve several issues that plague remote online voting. It could act as an additional authentication factor, it could be extended to an additional measure to fight coercion, or it could be used to reduce the risk of voter's credentials being used without their knowledge, which would hinder both malware and human adversaries.

[12] https://www.rferl.org/a/biometrics-to-end-fraud-in-afghan-election-may-discourage-some-women-from-voting/30131049.html

[13] https://www.logitech.com/assets/41349/logitech--why-a-better-webcam-matters.ENG.pdf

On the other hand, introducing facial recognition for remote electronic voting has implications. In order to gain most of the benefits, facial recognition must be a mandatory component of the online voting process. This requires reliable technology both on the system side end and on the voter end since recognition failure disenfranchises the voter.

The nature of facial recognition raises privacy issues which are most evident in the potential semi-controlled remote voting environment, where the voter would have to prove that the space is suitable for remote voting. Also, capturing a video stream for liveness detection raises the question of whether this level of privacy breach is proportional to the gained benefit.

There are a few positive use cases of facial recognition in the context of voting. The example from Canada highlights that facial recognition can work well for public remote voting, which is often required in parliaments and the governing bodies of local municipalities. The example from Fiji highlights that facial recognition can be an efficient tool for voter registration.

We conclude that the added complexity and privacy breach does not justify the use of facial recognition for remote online voting in case there is a well established, cryptographically secure mechanism for verifying the voter's eligibility. We would expect this mechanism to be multi-purpose to reduce the incentive for the voters to hand this mechanism over to somebody else.

However, in the cases where there is no existing mechanism for authentication in the remote setting, the introduction of remote voting implies the need to register online voters and provide them with credentials. One way to do this would be to create a PKI based system for distributing credentials. However, in case this is not possible, facial recognition could be a suitable tool to support registration, act as an additional authentication factor, and reduce the misuse of the credentials. When done locally by using the document photo as a reference, some of the accompanying risks can be mitigated.

Of course, introducing any form of biometrics to elections is not an easy decision to take due to the associated risks and ethical issues. However, when considering the integrity of elections, it has to be discussed how to replace the authentication mechanisms in voting systems, which rely on credentials delivered over post or email [29,8]. Thus, one of the aims of our work is to encourage further discussion on the possibilities and issues related to different authentication methods, including biometrics.

Acknowledgements This paper has been supported by the Estonian Research Council under grant number PRG920. The authors are grateful to the Estonian Information System Authority and State Electoral Office for their support of the research process.

References

1. Adida, B.: Helios: Web-based Open-Audit Voting. In: van Oorschot, P.C. (ed.) Proceedings of the 17th USENIX Security Symposium. pp. 335–348. USENIX Associ-

ation (2008), http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf

2. Arnò, S., Galassi, A., Tommasi, M., Saggino, A., Vittorini, P.: State-of-the-Art of Commercial Proctoring Systems and Their Use in Academic Online Exams. International Journal of Distance Education Technologies (IJDET) **19**(2), 55–76 (2021). https://doi.org/10.4018/IJDET.20210401.oa3
3. Asgari, S., Trajkovic, J., Rahmani, M., Zhang, W., Lo, R.C., Sciortino, A.: An observational study of engineering online education during the COVID-19 pandemic. PLOS ONE **16**(4), 1–17 (04 2021). https://doi.org/10.1371/journal.pone.0250041
4. Backes, M., Chen, T., Dürmuth, M., Lensch, H.P.A., Welk, M.: Tempest in a Teapot: Compromising Reflections Revisited. In: 30th IEEE Symposium on Security and Privacy (S&P 2009), 17-20 May 2009, Oakland, California, USA. pp. 315–327. IEEE Computer Society (2009). https://doi.org/10.1109/SP.2009.20, https://doi.org/10.1109/SP.2009.20
5. Balfanz, D., Czeskis, A., Hodges, J., Jones, J., Jones, M.B., Kumar, A., Liao, A., Lindemann, R., Lundberg, E.: Web authentication: An API for accessing public key credentials level 1. W3C recommendation, W3C (March 2019), https://www.w3.org/TR/2019/REC-webauthn-1-20190304/
6. Brand, C., Czeskis, A., Ehrensvärd, J., Jones, M.B., Kumar, A., Lindemann, R., Powers, A., Verrept, J.: Client to authenticator protocol (CTAP). Proposed standard, FIDO Alliance (January 2019), https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html
7. Buolamwini, J., Gebru, T.: Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Conference on Fairness, Accountability and Transparency, FAT 2018. Proceedings of Machine Learning Research, vol. 81, pp. 77–91. PMLR (2018), http://proceedings.mlr.press/v81/buolamwini18a.html
8. Cardillo, A., Akinyokun, N., Essex, A.: Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? In: Electronic Voting - 4th International Joint Conference, E-Vote-ID 2019, Bregenz, Austria, October 1-4, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11759, pp. 67–82. Springer (2019). https://doi.org/10.1007/978-3-030-30625-0_5, https://doi.org/10.1007/978-3-030-30625-0_5
9. Chaidos, P., Cortier, V., Fuchsbauer, G., Galindo, D.: BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme. In: Proceedings of ACM CCS 2016. pp. 1614–1625. ACM (2016). https://doi.org/10.1145/2976749.2978337
10. Chamikara, M.A.P., Bertók, P., Khalil, I., Liu, D., Camtepe, S.: Privacy Preserving Face Recognition Utilizing Differential Privacy. Computers & Security **97**, 101951 (2020). https://doi.org/10.1016/j.cose.2020.101951
11. Chaum, D.: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Commun. ACM **28**(10), 1030–1044 (1985). https://doi.org/10.1145/4372.4373
12. Chaum, D.: Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA. In: Günther, C.G. (ed.) Advances in Cryptology - EUROCRYPT '88, Workshop on the Theory and Application of of Cryptographic Techniques. LNCS, vol. 330, pp. 177–182. Springer (1988). https://doi.org/10.1007/3-540-45961-8_15
13. Cheeseman, N., Lynch, G., Willis, J.: Digital dilemmas: The unintended consequences of election technology. Democratization **25**(8), 1397–1418 (2018)

14. Clark, J., Hengartner, U.: Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. In: Danezis, G. (ed.) FC 2011, Revised Selected Papers. LNCS, vol. 7035, pp. 47–61. Springer (2011)
15. Code of Good Practice In Electoral Matters: Guidelines and Explanatory Report (2002), https://rm.coe.int/090000168092af01, European Commission for Democracy Through Law (Venice Commission)
16. Cortier, V., Galindo, D., Glondu, S., Izabachène, M.: Election Verifiability for Helios under Weaker Trust Assumptions. In: Proceedings of ESORICS 2014, Part II. LNCS, vol. 8713, pp. 327–344. Springer (2014). https://doi.org/10.1007/978-3-319-11212-1_19
17. Das, A., Galdi, C., Han, H., Ramachandra, R., Dugelay, J., Dantcheva, A.: Recent Advances in Biometric Technology for Mobile Devices. In: 9th IEEE International Conference on Biometrics Theory, Applications and Systems. pp. 1–11. IEEE (2018). https://doi.org/10.1109/BTAS.2018.8698587
18. Dziva, C., Musara, E., Chigora, P.: Democratisation and securitisation of Zimbabwe's national elections: opportunities and challenges of biometric voter registration. Journal of Public Administration and Development Alternatives (JPADA) **5**(1), 48–62 (2020)
19. E-valimiste turvalisuse töörühma koondaruanne (2019), Estonian Ministry of Economic Affairs and Communications, https://www.mkm.ee/sites/default/files/content-editors/e-valimiste_tooruhma_koondaruanne_12.12.2019_0.pdf, in Estonian
20. European Parliament, Council of the European Union: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
21. Fowler, A.: Promises and perils of mobile voting. Election Law Journal: Rules, Politics, and Policy **19**(3), 418–431 (2020)
22. Grassi, P., Fenton, J., Newton, E., Perlner, R., Regenscheid, A., Burr, W., Richer, J., Lefkovitz, N., Danker, J., Choong, Y.Y., Greene, K., Theofanos, M.: Digital Identity Guidelines: Authentication and Lifecycle Management [includes updates as of 03-02-2020] (2020-03-02 2020). https://doi.org/10.6028/NIST.SP.800-63b
23. Grother, P., Ngan, M., Hanaoka, K.: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
24. Heiberg, S., Martens, T., Vinkel, P., Willemson, J.: Improving the Verifiability of the Estonian Internet Voting Scheme. In: Electronic Voting - First International Joint Conference, E-Vote-ID 2016. LNCS, vol. 10141, pp. 92–107. Springer (2016). https://doi.org/10.1007/978-3-319-52240-1_6
25. House of Commons, Canada: Fact Sheet of Hybrid Voting Process in the House of Commons (2021), https://www.ourcommons.ca/Content/Newsroom/Articles/Factsheet-ElectronicVotingSystem-e-Final-02-25.pdf
26. Jacobsen, K.L.: Biometric voter registration: A new modality of democracy assistance? Cooperation and Conflict **55**(1), 127–148 (2020)
27. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proceedings of WPES 2005. pp. 61–70. ACM (2005)
28. Kim, G., Eum, S., Suhr, J.K., Kim, I., Park, K.R., Kim, J.: Face liveness detection based on texture and frequency analyses. In: 5th IAPR International Conference

on Biometrics, ICB 2012, New Delhi, India, March 29 - April 1, 2012. pp. 67–72. IEEE (2012). https://doi.org/10.1109/ICB.2012.6199760

29. Krips, K., Kubjas, I., Willemson, J.: An Internet Voting Protocol with Distributed Verification Receipt Generation. In: Third International Joint Conference on Electronic Voting E-Vote-ID 2018: 2–5 October 2018, Bregenz, Austria: Proceedings. pp. 128–146. TalTech Press (2018), https://digikogu.taltech.ee/en/item/0050d4bb-192b-4531-8e23-ccf8b565222e
30. Krips, K., Willemson, J.: On Practical Aspects of Coercion-Resistant Remote Voting Systems. In: Proceedings of E-Vote-ID 2019. LNCS, vol. 11759, pp. 216–232. Springer (2019). https://doi.org/10.1007/978-3-030-30625-0_14
31. Kulyk, O., Teague, V., Volkamer, M.: Extending Helios Towards Private Eligibility Verifiability. In: VoteID 2015, Proceedings. LNCS, vol. 9269, pp. 57–73. Springer (2015)
32. Li, Y., Li, Y., Yan, Q., Kong, H., Deng, R.H.: Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 1558–1569. ACM (2015). https://doi.org/10.1145/2810103.2813612
33. Lyastani, S.G., Schilling, M., Neumayr, M., Backes, M., Bugiel, S.: Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. In: 2020 IEEE Symposium on Security and Privacy, SP 2020. pp. 268–285. IEEE (2020). https://doi.org/10.1109/SP40000.2020.00047
34. Madise, Ü., Martens, T.: E-voting in Estonia 2005. The first Practice of Countrywide binding Internet Voting in the World. In: Electronic Voting 2006: 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. LNI, vol. P-86, pp. 15–26. GI (2006)
35. Marasco, E., Ross, A.: A Survey on Antispoofing Schemes for Fingerprint Recognition Systems. ACM Comput. Surv. **47**(2), 28:1–28:36 (2014). https://doi.org/10.1145/2617756
36. Moore, L., Sawhney, N.: Under the Hood: The West Virginia Mobile Voting Pilot (2019), https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf
37. Neumann, S., Volkamer, M.: Civitas and the Real World: Problems and Solutions from a Practical Point of View. In: Seventh International Conference on Availability, Reliability and Security, Prague, ARES 2012. pp. 180–185. IEEE Computer Society (2012). https://doi.org/10.1109/ARES.2012.75
38. Okamoto, T.: Receipt-Free Electronic Voting Schemes for Large Scale Elections. In: Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997, Proceedings. LNCS, vol. 1361, pp. 25–35. Springer (1997). https://doi.org/10.1007/BFb0028157
39. Patachi, S., Schürmann, C.: Eos a Universal Verifiable and Coercion Resistant Voting Protocol. In: Electronic Voting - Second International Joint Conference, E-Vote-ID 2017. LNCS, vol. 10615, pp. 210–227. Springer (2017). https://doi.org/10.1007/978-3-319-68687-5_13
40. Peixoto, B., Michelassi, C., Rocha, A.: Face liveness detection under bad illumination conditions. In: Macq, B., Schelkens, P. (eds.) 18th IEEE International Conference on Image Processing, ICIP 2011. pp. 3557–3560. IEEE (2011). https://doi.org/10.1109/ICIP.2011.6116484
41. Prabhakar, S., Pankanti, S., Jain, A.K.: Biometric Recognition: Security and Privacy Concerns. IEEE Security & Privacy **1**(2), 33–42 (2003). https://doi.org/10.1109/MSECP.2003.1193209

42. Rachel Aiello: A historic first: MPs hold House of Commons votes by app (2021), https://www.ctvnews.ca/politics/a-historic-first-mps-hold-house-of-commons-votes-by-app-1.5338151
43. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In: Boyd, C. (ed.) Proceedings of ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer (2001). https://doi.org/10.1007/3-540-45682-1_32
44. Rosacker, K.M., Rosacker, R.E.: Voting is a right: a decade of societal, technological and experiential progress towards the goal of remote-access voting. Transforming Government: People, Process and Policy (2020)
45. Roy, A., Memon, N.D., Ross, A.: MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. IEEE Trans. Inf. Forensics Secur. **12**(9), 2013–2025 (2017). https://doi.org/10.1109/TIFS.2017.2691658
46. Ryan, P.Y.A., Rønne, P.B., Iovino, V.: Selene: Voting with Transparent Verifiability and Coercion-Mitigation. In: FC 2016 International Workshops, Revised Selected Papers. LNCS, vol. 9604, pp. 176–192. Springer (2016)
47. Sabra, M., Maiti, A., Jadliwala, M.: Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks. In: 28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021. The Internet Society (2021), https://www.ndss-symposium.org/ndss-paper/zoom-on-the-keystrokes-exploiting-video-calls-for-keystroke-inference-attacks/
48. Scytl: Individual Verifiability, Swiss Post E-Voting Protocol Explained. Tech. rep., Swiss Post (November 2017), https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol-explained.pdf?la=de
49. Shukla, D., Kumar, R., Serwadda, A., Phoha, V.V.: Beware, Your Hands Reveal Your Secrets! In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014. pp. 904–917. ACM (2014). https://doi.org/10.1145/2660267.2660360, https://doi.org/10.1145/2660267.2660360
50. Shweiki, O., Lee, Y.: Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments. United States Attorneys' Bulletin **67**(1), 23–42 (February 2019)
51. Stenerud, I.S.G., Bull, C.: When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting. In: Proceedings of EVOTE 2012. LNI, vol. P-205, pp. 21–33. GI (2012)
52. Wolf, P., Alim, A., Kasaro, B., Namugera, P., Saneem, M., Zorigt, T.: Introducing biometric technology in elections. International Institute for Democracy and Electoral Assistance (2017), https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf
53. Xu, Y., Heinly, J., White, A.M., Monrose, F., Frahm, J.: Seeing double: reconstructing obscured typed input from repeated compromising reflections. In: Sadeghi, A., Gligor, V.D., Yung, M. (eds.) 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013. pp. 1063–1074. ACM (2013). https://doi.org/10.1145/2508859.2516709, https://doi.org/10.1145/2508859.2516709
54. Xu, Y., Price, T., Frahm, J., Monrose, F.: Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos. In: 25th USENIX Security Symposium. pp. 497–512. USENIX Association (2016), https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xu

55. Zhao, W., Chellappa, R., Phillips, P.J., Rosenfeld, A.: Face recognition: A literature survey. ACM Comput. Surv. **35**(4), 399–458 (2003). https://doi.org/10.1145/954339.954342