Technology Trends

Face Recognition

Enterprise Architecture, Chief Technology Branch

Version 1.1
Date 2019-06-25

Shared Services Canada Services partagés Canada

Canada

Table of Contents

Business Brief **3**

Technical Brief **3**

Industry Use **4**

Canadian Government Use **4**

Implications for Shared Services Canada (SSC) **5**

Value Proposition 5

Challenges 6

Considerations 8

References **10**

Business Brief

Face recognition is a biometric technology that is used to establish an individual identity and capable of uniquely identifying and verifying a person. It uses a computer application, which is also known as a facial recognition system, to extract a digital image from a picture, video frame or 3D scan and create a faceprint, a set of characteristic measurements of a face structure, that uniquely identifies one person's particular face for identity and authentication purposes. Generally, the authentication and identification is done by matching the corresponding facial features to the faceprints stored in a database record. The facial recognition technology has a wide variety of applications in access control, surveillance, and criminal investigations. It is also used in combination with other biometric technology to improve and enhance security measures.

Major technology companies like Apple, Google, Samsung, Facebook, and Amazon have begun to realize the impact that facial recognition can have on their existing security infrastructure. Apple has been attempting to add movement capabilities to the system. The subject of a scanned face can now be talking or moving during the scan, which allows facial recognition to combine with other biometric security measures like voice recognition. Since moving subjects can be scanned, individuals can be identified in a crowd without intrusion by using facial recognition systems.

Technical Brief

Facial recognition systems can use either a 2D/3D image or video feed to create a digital image, establish the faceprint, and identify a face by comparing its digital image with the faceprints in a database. Every face has several "landmarks" and the system will flag these as "nodal points". A human face can have up to 80 of these points. They represent areas of interest on the face that the system measures. Some examples of these measurements would be, distance between the eyes, width of the nose, depth of the eye socket, and more. These measurements will be stored in a database as a faceprint. When the system scans a face, it will compare all these measurements to the records, faceprints, in the database. Facial recognition systems employ an algorithm, such as the Facial Recognition Vendor Test, that can predict whether there's a match based on the "nodal points" on an individual's face. Usually, there is a 4-stage process involved in the operation of this technology [*]:

Capture – a physical or behavioral sample is captured by the system during enrolment

Extraction – Unique data is extracted from the sample and a template is created

Comparison – the template is then compared with a new sample

Matching – the system then decides if the feature extracted from the new sample is a match or not

Industry Use

Facial recognition offers another form of biometric identification and authentication. Several vendors have been leveraging face recognition as an access control and authentication tool either for their clients or for internal use. Its application is not limited to a form of security measure, but it can also be used for healthcare and retail. Although 2D face recognition may not be as accurate as other forms of biometric technology like fingerprint readers, it does have its advantages. The subject of a scanned face does not have to know when they were scanned, which demonstrates that the technology can be used in large crowds to identify threats quickly.

Several vendors in today's market are leveraging face recognition for their many applications. For example, Amazon has been developing a system, which allows users to pay for their items using an actionable image (selfie). A user can use a selfie in which he is moving or speaking a particular phrase as a password to verify their identity when paying for an item. The logic behind having the customer speak a phrase or make a movement, is to try to eliminate the possibility of fooling the system with a scanned 2D image of the person. Amazon Rekognition is another product that provides two API sets - Amazon Rekognition Image for analyzing images and Amazon Rekognition Video for analyzing videos. Both APIs perform detection and recognition analysis of images and videos to provide insights for use in your applications.

After purchasing Face.com in 2012, Facebook began using facial recognition technology to connect users with their photos. When a user uploads a photo, the software will automatically suggest other people to tag. When you are tagged in a photo, more content is shown in a grouped format about other tagged individuals.

Face ID is a technology developed by Apple and introduced in iPhoneX. It provides intuitive and secure authentication enabled by the state-of-the-art TrueDepth camera system with advanced technologies to accurately map the geometry of your face. With a simple glance, Face ID securely unlocks your iPhone or iPad Pro. You can use it to authorize purchases from the iTunes Store, App Store, and Apple Books, and make payments with Apple Pay. The iPhone XR, XS, and XS Max are all packing the second-generation of Face ID, which is an updated version of the biometric authentication system that is supposed to be faster than the version introduced with the iPhone X.

Canadian Government Use

Unlike the private sector, Government use cases for facial recognition applications are primarily related to security, specifically for identity verification and fraud prevention. For example, the Canada Border Services Agency (CBSA) has recently launched the Primary Inspection Kiosk (PIK) program where passengers entering the country from airports must check-in using self-serve kiosks.[i] These kiosks use facial recognition in order to clear passengers. The overall shift to un-maned kiosks has bolstered security while reducing congestion at airports and has been in development since 2015. Portuguese company Vision-Box has installed 130 Kiosks in the Toronto's Pearson International Airport. The Kiosks are designed to take biometric data in two phases - facial recognition and fingerprint biometrics. The kiosks will also be able to obtain iris data, a feature reserved for people travelling under the NEXUS program.

Facial recognition systems are also used in provincial casinos for identifying and locking out visitors with gambling addictions who have voluntarily entered themselves into self-exclusion lists.[ii] It is worth noting that the system was developed jointly with the Ontario Privacy Commissioner to ensure a privacy-by-default design. In real time, the system scans customers entering the casino and compares their images with gamblers on the self-exclusion list. If there is a match, the system notifies security and if not, the system deletes the image automatically. Access to the database is restricted and information about an individual is only accessible if the person in the picture is physically present.

Passport Canada has been using facial recognition software for the past decade to compare new passport photos against its database to prevent passport fraud. One to one (1:1) comparisons are done to confirm a person's identity, meaning that a recently taken image is compared to one already in the database that is associated with that person's identity. One to many (1:N) comparisons are done to compare an image against the entire database of passport photos to make sure there are no duplicate applicants or individuals with multiple identities.[iii] This initiative has been successfully used to catch individuals attempting to obtain multiple passports. This same concept is also used for driver's licences being issued at the provincial level.[iv]

Bill C-309, An Act to Amend the Criminal Code has made the concealment of identity (using masks or disguises) unlawful while participating in riots or unlawful assemblies.[v] Although the Privacy Act and PIPEDA (Personal Information Protection and Electronic Documents Act) state that consent must be obtained before private information is collected, Bill C-309 paves the way for law enforcement to scan large crowds using facial recognition software and uncover the identities of participants.

Implications for Shared Services Canada (SSC)

Value Proposition

SSC could leverage this technology by offering facial recognition as a service. SSC could utilise this technology to replace the current government employee security ID. A smart camera will instantly capture the biometric data of the individuals for local analysis and then open the gate to access the building. This service could reduce ongoing security costs associated with having a security team on site, but there probably will not be any savings in the short term due to the cost of developing the applications and installing the related equipment.

Facial recognition technology is a non-intrusive form of identity verification that cannot be lost by the individual. Within the SSC context, it would eliminate the need for employees to carry security passes. Additionally, this would help prevent unauthorized individuals from gaining access to secure facilities. Two-factor authentication with a user's face could also be used for accessing secure files with higher security classifications (such as secret documents).

There is a growing trend among smartphone manufacturers to create devices that can be unlocked with facial recognition technology. A market research firm based in Hong Kong estimates that nearly 64% (or 1 billion) of all smartphones shipped worldwide will have facial recognition capabilities in 2020.[vi] SSC can take advantage of this research and only issue phones with facial recognition capabilities to employees. This biometric information can be paired with any other type of authentication method to create a two-step verification process for all smartphones. SSC would not need to acquire any additional software licences, as these phones would already have the capacity for facial recognition. Since verification is done locally, (reference images are stored on the device outside of a cloud environment) this minimizes the security risks associated with facial recognition technology.

Although facial recognition requires a lot of computing power to process images in real time, Edge Computing can mitigate this concern. Image pre-processing tasks can be completed by the device that took the picture, or much closer to the device than the data center. The device would capture the image, scan it for faces, and then extract information like a faceprint from the image. Once the faceprint has been created, it is sent to the main server for authentication and the original image is discarded. Since pre-processing of the faceprint has been done outside of the server, the server can focus on verifying the recent faceprint against an internal match.

Challenges

The primary challenge with facial recognition technology is privacy. One way to mitigate the privacy concern is to leverage Edge Computing to store biometric data locally, which helps prevent data loss and inappropriate cross-linking of data across systems. The data is better stored as biometric features (a faceprint for example) rather than images of people's faces, which should be destroyed once the faceprint is collected; faceprint data should be stored, encrypted, and be made available through secured measures. In this way, it will inhibit the misuse of the image for unauthorized reasons.

If this technology were to be used to authenticate identities in multiple areas, there may be large amounts of hardware required for computing power. If facial recognition technology, with millions of scanned faceprints were to be adopted by one or multiple departments, the computing capacity being used to process the requirements and match the image information with the faceprint records in the database would be extensive. From this perspective, if SSC were to support such a project, the demanded computing power to support this technology could be provided either in the form of a private or public cloud to meet the computing demands.

There are also certain factors that can limit the accuracy of facial recognition systems. If the photo was taken in profile or if the image quality is too low, there may not be enough information available for the system to extract and generate a match. Haircuts, skin color, makeup, glasses, and face coverings such as surgical masks can also lower recognition accuracy. Considering that these systems are based on Artificial Intelligence (AI), there is also the possibility of improperly “training” them.

An AI for a facial recognition system should be manually supervised to “reward” correct matches, but if the training set only consists of a very specific demographic of people it will have difficulty with detecting other types of faces. The lack of a diverse training set creates recognition biases in the programs, which makes them better at detecting and correctly identifying individuals with specific attributes over others.

In a study conducted by Joy Buolamwini where three different facial recognition systems were tested for accuracy in determining genders, they had error rates between 21% and 35% for women with darker skin tones whereas the error rate for light-skinned males was less than 1%.[vii] This brings into question the reliability of these systems. To avoid discrimination against specific minority groups, they must be developed and tested to make sure they don’t have any recognition biases.

These systems also have fuzzy accuracy rates, meaning that matches are never 100% accurate when doing searches, for example, in a database of images. There is the real possibility of false positives, where matches are found but they aren’t for the right person, and of false negatives, where the real match exists within the database but the system is unable to create a match. This accuracy gap means that the systems should only be used by trained individuals who understand how the technology works and specific guidelines should be followed when matches are generated by the system.

A good example in the field is how the Toronto police force is using the system: only six FBI-trained Toronto Police officers can use the system and it can only generate a list of candidates. They do not use the system as a sole basis for arrests but in tandem with other traditional evidence gathering methods.[viii] AI systems, if they are to help inform important decisions should never be solely trusted and should be used as tools to inform decisions, not guide them.

To deal with the issue of bad lighting or faces at unrecognizable angles, some systems are altering images so that they are more “readable”. Panasonic has developed facial recognition software that analyses movement, speed and lighting present in videos to automatically correct still images that would otherwise be blurry.[ix] Since the software adjusts the image before being analysed, it creates a new concern that additional false positives will be created. If an image has been touched up and edited before it was “plugged-in” to a facial recognition system, this can alter the faceprint being analysed and the search results may be biased or incorrect.

Another limitation of these systems is that it can only recognize individuals whose images are already contained within its database. Systems must also be able to perform “liveness” testing, or in other words, they must be able to determine if the subject in question is actually there in person since faces are not secret, in the same sense that passwords are secret, and faces cannot be hidden. Facial recognition systems rely on the difficulty of impersonating a real person to keep the system secure. Given this fact, the system needs to be able to determine the “liveness” of the image it’s analysing and determine if the person it just photographed is real or if it’s a picture.

Facial recognition system technology has not yet been regulated in Canada and organizations that currently use it must operate within a specific legal framework. Under the Canadian Privacy Act, federal government institutions can only use personal information for the specific purpose for which it was collected and consent of the individual must be obtained before that information can be used for another purpose. Under PIPEDA, an organization must inform individuals and receive consent to any use of their personal information.[x] This is a potential legal barrier to any organization planning to conduct live analysis of public crowds since each individual would need to consent to the collection and use of their faces (private information). These regulations ensure that databases containing personal information belonging to different GC departments cannot be shared between departments for purposes other than the specific use for which consent was obtained.

Considerations

Any wide-scale use case developed by SSC will need to be reported to the Office of the Privacy Commissioner (OPC) for assessment. They would also need to comply with the Privacy Act and PIPEDA. Use cases must also be justified with regards to possible privacy intrusions and the OPC has suggested a four-part test to determine this:[xi]

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Would the loss of privacy be proportionate to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?

Additionally, use cases that are to be deployed on a wide scale within SSC, such as facial recognition systems to enter secured buildings, would rely on the consent of all participants. High quality images with neutral facial expressions would also need to be collected, or compiled from existing databases (i.e. building passes). These new centralized repositories of staff pictures could also be new targets of cybersecurity attacks. They would need to have the utmost protections afforded to them. Smaller scale use cases, such as unlocking a device with a face capture, would pose smaller risks since the information is stored locally.

If SSC were to adopt or develop facial recognition software, the software would need to be tested for recognition biases. Meaning, that it should have uniform recognition performance across all genders, skin types, and ages. If there are any biases present, the software would need to undergo more development and could garner more associated costs. Facial recognition applications purchased from a vendor would need to be closely scrutinized and evaluated since SSC would not know exactly how the application was trained and developed. Additionally, there are no industry standards for facial recognition products, meaning that there is no benchmarked performance level that needs to be achieved before a product goes to market. If SSC were to develop the software itself, it would have complete control and knowledge over the performance of the system.

Lastly, it is important to consider the legal context of any facial recognition systems deployed within SSC. Presently, the technology is not regulated and performance standards have not been set for developers. The legal landscape could change by the time SSC is ready to adopt the technology. An ongoing privacy assessment of current service offerings may help provide a better understanding of the impact that facial recognition technology would have.

References

https://en.wikipedia.org/wiki/Facial_recognition_system

https://www.gartner.com/doc/341020/face-recognition-software-antiterrorism-tool

https://www.upwork.com/hiring/for-clients/pros-cons-facial-recognition-technology-business/

https://disruptionhub.com/5-applications-facial-recognition-technology/

https://findbiometrics.com/solutions/facial-recognition/

https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition2.htm

https://www.kairos.com/blog/5-companies-using-facial-recognition-to-change-the-world

https://www.techemergence.com/facial-recognition-applications/

https://www.priv.gc.ca/media/1765/fr_201303_e.pdf

http://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344

https://www.biometricupdate.com/201606/canadian-government-used-facial-recognition-to-detect-passport-fraudsters

https://www.upwork.com/hiring/for-clients/pros-cons-facial-recognition-technology-business/

https://www.apple.com/ca/business-docs/FaceID_Security_Guide.pdf

[*], http://www.ex-sight.com/technology.htm

[i] Braga, Matthew. (March 2nd, 2017). *Facial Recognition Technology is coming to Canadian Airports this spring.* Canadian Broadcasting Corporation. Retrieved 17-05-2019 from: https://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344

[ii] Elash, Anita, and Luk, Vivian. (July 25th, 2011). *Canadian Casinos, Banks, Police use Facial-Recognition Technology.* The Globe and Mail. Toronto, Ontario. Retrieved 21-05-2019 from:

https://www.theglobeandmail.com/news/national/time-to-lead/canadian-casinos-banks-police-use-facial-recognition-technology/article590998/

[iii] Mackrael, Kim, and Ha, Tu Thanh. (May 15th, 2014) *Facial Recognition Program Allows RCMP to Identify Alleged Passport Fraud.* The Globe and Mail. Toronto, Ontario. Retrieved 27-05-2019 from: https://www.theglobeandmail.com/news/national/facial-recognition-program-allows-rcmp-to-nab-alleged-passport-fraudster/article18703608/

[iv] Office of the Privacy Commissioner of Canada. (March 2013). *Automated Facial Recognition in the Public and Private Sectors.* Government of Canada. Retrieved 23-05-2019 from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/

[v] Parliament of Canada. (June 19th, 2013). *Bill C-309 An Act to Amend the Criminal Code (concealment of identity).* Government of Canada. Retrieved 03-06-2019 from: https://www.parl.ca/LegisInfo/BillDetails.aspx?Bill=C309&Language=E&Mode=1&Parl=41&Ses=1

[vi] Naiya, Pavel. (February 7th, 2018) *More than one billion smartphones to feature facial recognition in 2020.* Counterpoint technology Market Research. Hong Kong, China. Retrieved 27-05-2019 from: https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/

[vii] Lohr, Steve. (February 9th,2018). *Facial Recognition is Accurate, if You're a White Guy.* New York Times. New York, USA. Retrieved 29-05-2019 from: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[viii] Burt, Chris. (May 28th, 2019). *Toronto police using facial recognition as Canadian government ponders rules.* Biometrics Research Group Inc. Retrieved 29-05-2019 from: https://www.biometricupdate.com/201905/toronto-police-using-facial-recognition-as-canadian-government-ponders-rules

[ix] Panasonic. (February 20th, 2018) *Panasonic to Launch Face Recognition Server Software Using Deep Learning Technology.* Panasonic Corporation. Kadoma, Japan. Retrieved 15-05-2019 from: https://security.panasonic.com/news/archives/686

[x] Office of the Privacy Commissioner of Canada. (March 2013). *Automated Facial Recognition in the Public and Private Sectors.* Government of Canada. Retrieved 23-05-2019 from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/

[xi] Office of the Privacy Commissioner of Canada. (March 2013). *Automated Facial Recognition in the Public and Private Sectors.* Government of Canada. Retrieved 23-05-2019 from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/