



Understanding Face Biometrics for Identity Verification and Authentication

February 2020

Identity Security in 2020

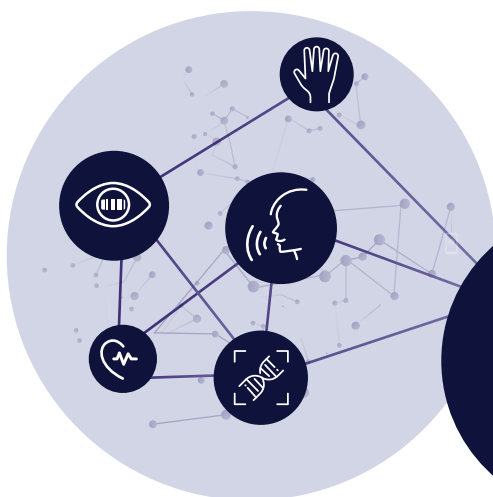
A person's face is the foundation of security and access control in the physical world. A face image is prominently found on most identity documents, be it an employee identity card, driver's license or passport. Face biometrics can bring the same, if not higher, level of security to the digital world of identity verification and authentication.



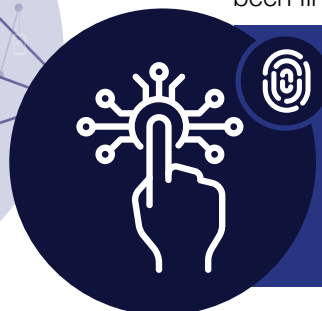
As we start a new decade in 2020, the dominant method for authentication is still a password - the weakest link in the entire security model. The legacy of passwords is that they are targeted by hackers as the simplest way to break into a company to disrupt – or even worse, hold ransom - the targeted victim. Whether exposed from inside or outside the organization, passwords are the Achilles-heel in the security wall. Why? Because passwords can be...



And they are invisible, and that allows a hacker or fraudster to take over an identity.



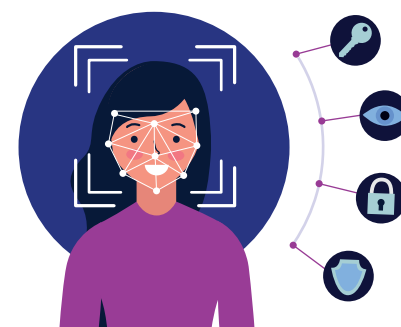
The biometric world offers a spectrum of options including iris, DNA, heartbeat, voice, gait, palm, and of course, fingerprint. However, these biometric options are not typically embedded in public identity documents, unless you happen to be a convicted felon and have been fingerprinted by the police.



Biometrics, like fingerprints and DNA, are commonly used for finding and capturing the “bad guys” which is an entirely different application. This report focuses on the use of face biometrics for identity verification and authentication with the intent of protecting “the good guys.”

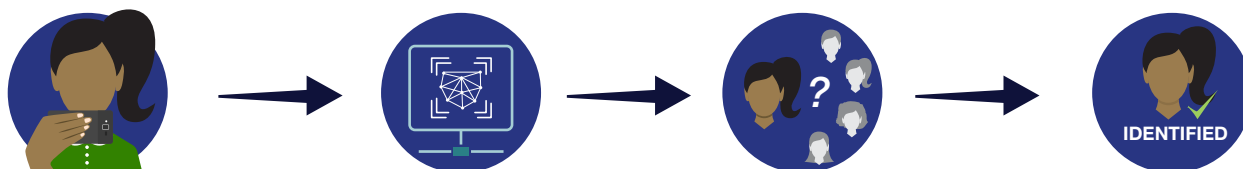
How Face Biometrics Work

Face biometrics work on the principle of translating the face captured by a camera into a digital value (face template) that uniquely represents a face. This face template can be used to verify and authenticate a person. This is an example of a face template. It is a mathematical value:



10F2450B369B545E8F77DD55E19D0D8FFE5C32AE6730C47914C4727264FA91B0F

Registering a face is like creating a password. A person simply takes a selfie which is then translated to a face template as described above. To authenticate, a person takes another “selfie” and, using the same translation method, a “challenge” template is created. The challenge template is compared to the registered face templates to determine a successful match. This is the way face recognition can augment or replace passwords.





Face templates can also be generated from a photo scanned on an identity document to verify a person during an on-boarding or enrollment session. Depending on the security level, and how alike the templates are, the matching algorithm will generate a positive or negative result. The relying party would use the authentication result to make a decision. That decision could range from...



Granting physical access



Signing a document

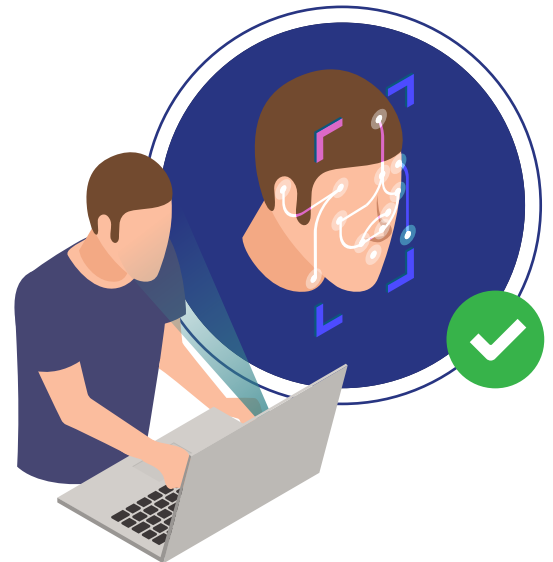


Completing a transaction

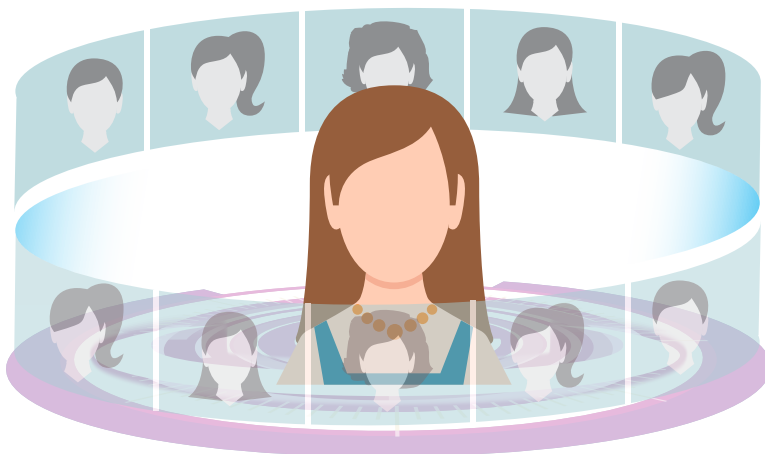
A key aspect of the face template approach is that it is statistically impossible to have an exact match. If an exact match occurs, we know that this is a “man in the middle” replay attack! This capability enables a higher level of protection against hackers compared to password and other inferior authentication methods.

Another aspect of the selfie verification session is the ability to **prove that a live person is in front of the camera.**

“Anti-spoofing” techniques eliminate the ability for someone to spoof the selfie with a static image or pre-recorded video. Anti-spoofing with a 2D camera requires the user to perform a random head movement – and by closely measuring the movement the software can differentiate between a real and a fake image. Anti-spoofing with a 3D camera is easier because the camera sensor returns depth information that can be used to differentiate between a real and a fake image.



Privacy Advantages of Face Biometrics



A key privacy feature is that face templates cannot be reverse engineered to recreate the original face image. Even with access to the template generation algorithm, and the ability to generate millions of templates from a huge face-image library, one cannot regenerate the original face input. Individuals can rest assured that using face templates means less privacy exposure.



Unique identifiers

Face templates are like password “hashes” in that they are one-way. They are different in that every face template is unique, because every input image is slightly different.



Replay attack protection

This protects a system from a replay attack – since a face template should never be seen again in normal operation.



Single pixel differentiation

A single pixel difference between input images will result in a different face template. Whereas the same password generates the same hash.



Increased Security

Even if a database containing a list of users and their associated face templates was hacked and shared publicly, the face templates cannot be used to spoof a person – unlike password hashes.



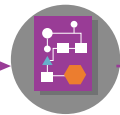
As mentioned earlier, and it bears repeating: faces cannot be forgotten, written down, lost, shared, sold, and/or stolen. Faces are also visible to the naked eye and easily recognized by a normal person, and this enables additional security measures that are not possible with other biometric methods, and certainly not passwords.



For example, to protect access to a personal computer, face authentication software can be installed to either augment or replace login passwords.



This software features face login – delivering two or three factor authentication –



and if you choose it can provide a visual audit trail of all login activity.



If a failed login attempt occurs, then the event can trigger an alert to IT administrators.

Applying that same face authentication method to a banking app would provide a visible record showing the person who performed any activity with that app and protect against family and friend fraud. These methods detect and deter fraudulent activities and mitigate the impact of such activities if they occur.



Current Market Uses of Face Biometrics

Recognizing the need for better security, companies like Apple, Microsoft, and Samsung have started offering biometrics for protecting access to smart phones and computers. These device access methods provide a layer of security, but the original intent was for user convenience and time-savings. From a security perspective, they are not ideal because user identity is not linked to a verified person. Identity for the Apple iPhone, as an example, is only linked to the current person with access to the phone. And there is no visual audit trail. Furthermore, these providers do not allow access to the biometric templates, and so they cannot be used for on-boarding or identity document verification. They are also proprietary implementations which means there is no one single biometric solution that works across all computers and phones. This makes it virtually impossible to use these devices for identity verification and authentication.



A key element of establishing trust with any authentication method is a secure enrollment process. This can be as simple as an IT department provisioning a username and password for new employees, or a more robust process for setting up a new bank account. In all cases the applicant's identity must be verified. In the digital world, enrollment leverages identity documents such as an employee identity card, driver's license, or passport. By comparing the face template harvested from the identity document, with the template from the selfie, and optionally against a pre-registered face template, the software can authenticate a person using a mobile phone and establish a trusted identity for the relying party.

Debunking Face Biometrics Myths

Some common misunderstandings exist in the industry and those include:



Lack of revocability of biometrics

Some people argue that if a biometric is stolen it can never be used again. This article has shown if a biometric value is used again, it represents an error or replay attack, and can be stopped.



A fraudster may obtain a copy of a user's face signature and construct a replica of their face

As described above, the face image to face template algorithm is a one-way transformation similar to a password hash. The original image cannot be retrieved.



Face images are easy to steal via Facebook or other methods

This is true, but we have demonstrated that to take a selfie, the real user must be present to satisfy the "liveness" and anti-spoofing test.



A biometric template does not constitute a secret

Biometric values are in fact a secret and have interesting characteristics that make them better than passwords.



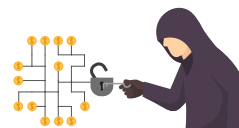
One-Time-Password (OTP) and SMS-based authentication methods are secure

The fact is that older authentication methods are proving to be less secure and the FBI is warning against their use. Here are some examples:



RSA one-time-password (OTP) tokens are being cracked in real time.

- [Chinese hacker group caught bypassing 2FA](#)



FBI - vulnerabilities tied to token and phone-based multi-factor authentication

- [FBI urges businesses to use authentication systems involving biometrics](#)

In summary, face biometrics for identity and authentication allows applications to provide higher levels of privacy and security that have not been attainable in the past.

Now is the time to have these discussions about the many emerging verification methods such as biometrics, and the impact they will have on our society.

DIACC is the community where collaboration occurs, and where members work together to solve the real-world identity challenges of today.



JOIN


the DIACC to participate in the conversation about Canada's digital future.

Contact

The Digital ID and Authentication Council of Canada

 diacc.ca

 [@mydiacc](https://twitter.com/mydiacc)

 [/company/mydiacc](https://www.linkedin.com/company/mydiacc)

 [/mydiacc](https://www.facebook.com/mydiacc)

