IdentityX®

Biometrics Overview

Copyright

Disclaimer

The information in this document is subject to change without notice. Daon makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice.

Products sold or licensed by Daon are covered by the terms of its contractual agreements, license agreements and any warranties or guarantees therein. Daon reserves the right to discontinue production and change specifications and processes at any time without notice.

Validity of Information

Daon has made every effort to ensure that all statements and information contained herein are accurate. Daon does not warrant that this document is error free.

Trademark Acknowledgements

PUBLICATION ID: IDXBiomOvw.4.4.180320

Table of Contents

1 Why Biometrics?

The Internet has revolutionized many of our commercial interactions from banking to shopping. However, with the freedom to bank and shop at any time from our own homes, a new threat challenges the security of those password based authentication interactions. Time and again, systems have been hacked through spear phishing (masquerading emails seeking sensitive data) and social engineering (manipulating people online to divulge confidential information), highlighting the inherent failure of a system protected by passwords alone.

To counter the threats to password only systems, many organizations have chosen to introduce multi-factor authentication based on the use of SMS or hardware tokens from companies such as RSA or Vasco. These approaches certainly improve the security of the authentication process for the systems they protect, but they do so by adding friction to the user's interaction. This leads to the real cost of multi-factor authentication—inconvenience.

At a time when mobile devices from smartphones to tablets are enabling unheralded levels of access and convenience for their users by allowing them to interact not only at any time but also from any place, multi-factor authentication is often introducing *user friction* into the process, for example, requiring users to have specialist tokens, or to switch apps on the device, or to even access a different device. These additional requirements can often hamper the user's successful interaction with multi-factor authentication.

So what's the Solution?

Is there an authentication method available to increase a user's security while still maintaining the same level of convenience for the user as entering a password? The answer to this question is yes. This can be done but it requires an organization to embrace all authentication factors including passwords, tokens, and biometrics.

By using biometrics, users are enabled to authenticate themselves by touching a sensor, looking at a camera, typing on a keyboard, or simply speaking a phrase. With biometric authentication, the burden shifts from the user having to remember a password or a PIN or possessing a key fob or a smartcard, to the system recognizing the user from his or her inherent traits such as face, voice, iris, or fingerprint. Biometrics has the unique ability to identify the user thereby lowering the barrier for genuine users to be positively authenticated.

Biometrics which has for the longest time been the realm of government agencies can be effectively used as an authentication method by individuals using modern mobile computing devices. It can provide increased security while maintaining convenience for a user, but alone, it is not the silver bullet.

Role of Biometrics in this Solution

The purpose of this document is to provide a description of the current state-of-the-art for common biometric modalities and the challenges that need to be considered when using each of these biometric modes.

In the final analysis, no single authentication factor is perfect but combining multiple factors together can strengthen the security of systems. However simply combining different factors can lead to significant additional friction in the authentication process and while this may be warranted in some situations, in general it will lead to increasingly dissatisfied users. A more sensible approach would be to support multiple equivalent authentication methods based on the full range of authentication factors and allow the user to choose the most appropriate authentication method at that time on that device.

2 Introduction

2.1 What are biometrics?

Biometrics are measurable physiological and behavioral characteristics that uniquely identify a person. Examples include facial images, voice prints, fingerprints, and DNA. Biometric authentication is the process of recognizing someone from their biometric samples and is something we humans do every day. Every time we answer the phone to a friend we subconsciously compare the sound of the voice to our memory of our friend's voice. Even when we walk down the street, we compare the faces we see against our internal database of faces of people we know.

Computer based biometric authentication is performing this same process; gathering biometric samples and comparing them to stored records of samples and granting access to computer systems on the basis of positive authentication. One of the key benefits of biometric authentication is that the authentication process does not rely on the user doing anything more than being him/herself—no passwords to remember or tokens to carry.

Since a biometric is an authentication factor that is tied to an individual person, it cannot be shared or stolen—unlike other factors such as passwords and tokens. As a result, Biometric technology has proven itself to be very useful in preventing fraud where users may traditionally share passwords or tokens.

Biometrics Improve Security

Biometric technology is being used by countries around the world in systems such as voter registration and border control. India biometrically enrolled 1.2 billion identities at a rate of 1 million people per day.

Biometric sensors are becoming commonplace on consumer devices such as mobile phones, laptop computers, and home safes. Introduction of a fingerprint sensor on popular smartphones has resulted in many millions of people now using biometrics on a daily basis for personal authentication. Similarly, businesses use biometrics for everything from time and attendance systems to physical access control of facilities. Disneyworld has used biometrics to control admission to the park since 2005!

2.2 Authentication Factors

Authentication is the process of confirming the identity of a person. Traditionally the security industry divides the different methods used to authenticate people into three broad categories:

- What you know – examples of this would include passwords and PINs.
- What you have – examples of this would be smart cards or RSA SecurID tokens.
- What you are – measurable characteristics that make a person unique – biometrics!

Each factor has unique characteristics and combining these factors together can provide even stronger forms of authentication than what can be achieved by a single factor alone.

For the past decade, the de facto high security solution for most systems has been a combination of passwords and out-of-band tokens such as those based on SMS text messages or RSA SecurID tokens. However, even specialized tokens are not immune to attacks, as compromises for several popular solutions have been published.

More recently, interest has begun to focus on biometrics as a technique to enhance the security and convenience of systems without imposing increased burdens on the users of those systems.

2.3 Unique Advantages of biometrics

Using biometrics as part of an identity authentication solution can offer several important advantages:

- **Convenience:** With traditional password authentication, a user must remember and recall a complicated alpha-numeric character string, while if a token is used they must have that token in their possession every time they are authenticated. Biometrics are more convenient in that they do not need to be remembered and are always available. A user might simply glance at a camera, touch a sensor, or utter some words to use their biometrics for authentication. Biometrics can provide a quicker, more seamless and more usable experience during an authentication transaction. Furthermore, a user may be permitted to select those biometrics which are most convenient for their own particular scenario.
- **Fraud prevention:** Passwords and physical tokens can be shared amongst people, and they cannot guarantee that the original person who was issued the authentication factor is present during authentication. This type of identity fraud is difficult to prevent using traditional means. However, since biometrics are uniquely linked to a person, they provide far more assurance that the genuine user is present during a transaction.

- **Flexibility:** There are a number of different biometric types that may be selected for use in an authentication solution. For each type, different security and usability trade-offs may be made. In addition, multiple biometrics may be combined to further enhance security and usability. Biometrics provide a highly configurable authentication factor, with far more flexibility than a standard password or token.
- **Additional authentication factor:** The security level that is provided in any one solution will depend on the number of authentication factors required, the technology selected for each factor, and how that technology is configured. Security can be increased by using two or more different factors. Biometrics add an additional configurable security layer to an authentication solution.

2.4 What kinds of biometrics are there?

There are a number of different types of biometrics, known as modalities. These include both physical and behavioral types:

Physical Biometric Types:

- **Voice:** Refers to the unique audio signal when a person utters a phrase or set of digits. This is a combination of biological and behavioral characteristics. The behavioral aspect refers to something that has been learned and adopted by the user over time, such as their unique accent, dialect, and choice of words.
  Please read Chapter 3 – Voice Biometric for more details.
- **Face:** Refers to the unique appearance, geometry, and texture characteristics of a person's face which are captured in a digital photograph from which key facial characteristics are then extracted to produce an enrollment/verification template. Most systems use 2D recognition today, but the movement is toward using 3D which should increase accuracy. Facial recognition systems examine the structure and texture of a person's face and are not fooled by glasses, hats, changes in hair style/color, or other variations that can throw off a human observer.
  Please read Chapter 4 – Face Biometric for more details.
- **Fingerprint:** Refers to the pattern and details on the surface of the fingerprint**.** This has been used for the last 100 years for criminal forensics. During the past 20 years it has been used for civilian systems such as driver's license and passports. It is the most mature of all automated biometric technologies.
  Please read Chapter 5 – Fingerprint Biometric for more details.
- **Palm print:** Based on the pattern on the palm of the hand, this biometric is used in forensic/law enforcement applications as a supplement to fingerprints, with which it shares much of the same technology. A single palm print contains much more information than a single fingerprint due to the significantly larger image area.
- **Iris:** Refers to the pattern in the pigmented area around the pupil. Images of the iris need to be captured when the iris is illuminated with near infra-red light as the pattern of the iris for people with dark irises cannot be seen under visible white light. The iris should not be confused with the retina (see below).

- **Retina:** This biometric type is based on the unique pattern of blood vessels at the back of the pupil. It is this unique pattern that is captured and verified. It is not widely deployed because it is quite an intrusive technology—a user is required to look into a pair of binocular type devices and a light is shone into the back of the eye. In addition this technique could potentially leak medical information as certain diseases can be diagnosed, in part, based on information in the retinal image.
- **Vascular/vein:** This approach uses infrared sensors to detect heat patterns resulting from the flow of blood through veins and capillaries beneath the surface of the skin and can be applied to a person's finger, hand, palm, eye, or even face.
- **Hand geometry:** Based on the size and shape of the hand and the length of the fingers, this biometric has been in commercial use for around 20 years. It is not very accurate so it tends to be used in conjunction with an additional authentication factor such as a card. It is used in prisons in the UK for physical access.
- **Ear shape:** Algorithms have been created for smartphones that extract features from the shape of a person's outer ear from the points of the ear that are placed against the smartphone touchscreen. It has also been used in law enforcement where a latent ear print is discovered on a surface at a crime scene.
- **ECG:** Although not in widespread use, there is at least one vendor offering a proprietary wristband that measures the electrical currents generated by heart rhythm for authentication. However, with the advent of smart watches and wearables that measure heart rate and other bio signals, its popularity may increase.
- **DNA:** This is a very accurate biometric as it is based on the genetic makeup that is present in almost every cell in the body. It is mainly used in forensic applications. The process of acquiring and processing samples is time consuming and requires the use of a laboratory. Identical twins do share the same DNA so this biometric cannot be used to differentiate identical twins or triplets. However, fingerprints and irises are different between identical twins.

Behavioral Biometric Types:

Behavioral biometrics analyze the user's behavior to help verify their identity. Although accuracy is weaker than the physiological biometric traits such as finger, iris or face, behavioral traits, when used in conjunction with physical biometric types can ensure a required authentication confidence level is reached.

- **Behavioral keystroke:** This method is based on the typing technique of an individual which is a behavioral biometric. Typically it will examine the exact time that each key is pressed and released. On smartphones it may also incorporate device positioning by using information from the accelerometer and gyroscope sensors.
- **Hand writing:** The method by which a person signs his or her name is unique and is based on the stroke direction, pressure, speed, and shape of the signature.
- **Gait:** The manner in which a person walks, that is, their gait.

NOTE: For more details on the alternative biometrics mentioned above, see Chapter 6 – Alternative Biometrics

2.5 How biometric verification works

An authentication solution that uses biometrics will perform a once-off biometric enrollment process where biometric samples belonging to a specific user are registered. Later, that person's identity can be confirmed by verifying that a fresh biometric sample belongs to the enrolled individual.

Biometric verification (that is, biometric authentication) is the process of comparing data from a biometric sample captured from a person at the time of enrollment with another sample captured from the same person at the time of verification.

Biometric samples are generally converted into compact "templates" which are mathematical representations of the key features extracted from the raw samples. For example, in the case of fingerprints, the characteristics could be the co-ordinates and relative distances between the ridge endings in a fingerprint image.

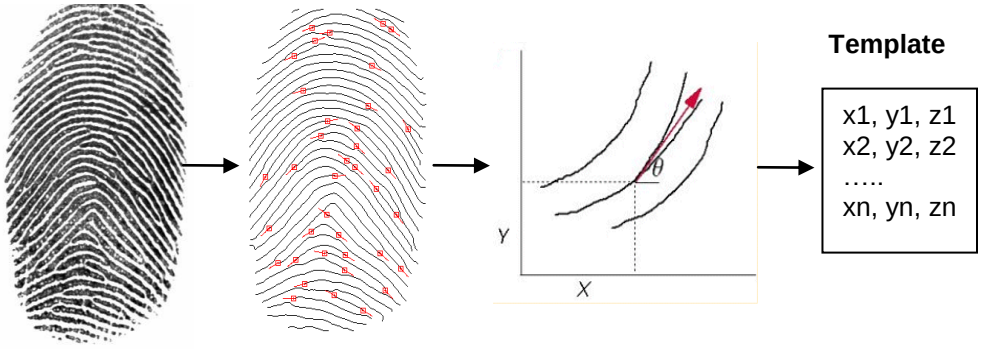

Figure 1 Fingerprint Template Conversion Process

Biometric matching is the process of comparing two templates to determine a similarity score, that is, how similar are the templates. The resulting score value can then be converted to a probability, a measure of how likely it is that the samples match, which is a key defining characteristic of biometric matching.

All biometric matching is probabilistic – unlike password matching which yields a binary decision, biometric matching results in a probability score. In other words, while you can be certain whether a password is correct, biometric verification returns a probability that the two biometric samples match, which is almost always less than 100%.

2.6 Measuring Biometric Accuracy

The biometric market is crowded with vendors supplying recognition and liveness detection algorithms with wide ranging claims and performance differences. All biometric systems are based on probability algorithms so accuracy errors are inevitable. These errors need to be measured and quantified in order to correctly configure a biometric deployment and to understand the expected error rates so that these exceptions can be handled appropriately.

Common Errors

In a biometric verification system, the most common errors are:

- **Failure to enroll (FTE)**

  When a person is repeatedly unable to register his or her biometrics for use in the system, an FTE error has occurred. Rejections occur because the biometric system determines that it is unable to acquire a reasonable sample of the biometric being enrolled.

  For example, in a voice biometric system if the person attempts to enroll with very loud background noise, the enrollment may fail. Similarly, if a user attempts to enroll their face in a dark room with little or no lighting, they may experience a face FTE. The probability of an FTE error occurring is called the FTE rate.

- **False match rate (FMR)**

  When a biometric algorithm incorrectly accepts the wrong person, an impostor, during a single authentication attempt, a false match error has occurred.

  For example, within a large population, a false match may be observed between two random people. While the biometric samples from these two people will not be identical, they may be similar enough under certain conditions for the matching algorithm to incorrectly decide that they originate from the same single person. The probability of a random false match error occurring is called the false match rate (FMR).

- **False non-match rate (FNMR)**

  When a biometric algorithm incorrectly rejects the correct person, a genuine user, during a single authentication attempt, a false non-match error has occurred.

  For example, if a genuine user positions an enrolled finger very differently on a small finger sensor compared to when s/he first enrolled, the captured sample might be rejected. Similarly, some environmental conditions such as poor lighting conditions and background noise can cause false non-matches for face and voice modalities. The probability of such an error occurring is called the false non-match rate (FNMR).

- **Equal error rate (EER)**

  A biometric matching algorithm can be configured to operate at different matching thresholds. The higher the threshold is set, the lower the likelihood of a false match (accepting the wrong person), but the greater the likelihood of a false non match (rejecting the correct person). Different thresholds will result in different FMR and FNMR errors. There will be one particular threshold that will result in both the FMR and FNMR to being the same value, and this error rate at that configuration is called the equal error rate (EER). At the EER, the FMR and FNMR are equal.

Standard methods are defined for measuring biometric error rates including FTE, FMR, FNMR, and EER. The ISO 19795 "Biometric performance testing and reporting" series of standards describe these methods in detail. Specialized software, which conforms to these test methods, is used to perform the biometric benchmarking.

Attackers may attempt to circumvent a biometric verification system by presenting an attack instrument instead of a live genuine biometric. For example, a photograph of a face might be presented instead of the genuine user. Biometric liveness and anti-spoofing algorithms attempt to detect these attacks, but they also have probabilistic outcomes with errors. In a system using biometric anti-spoofing algorithms, the most common errors are:

- **Attack presentation classification error rate (APCER):**

  Proportion of attack presentations incorrectly classified as bona fide (normal) presentations at the presentation attack detection (PAD) subsystem in a specific scenario.

- **Bona fide presentation classification error rate (BPCER)**

  Proportion of bona fide (normal) presentations incorrectly classified as presentation attacks at the presentation attack detection (PAD) subsystem in a specific scenario.

The ISO 30107 "Biometric presentation attack detection" series of standards describe these errors and how to measure and test them in detail.

In a biometric technology test, one of the first steps is to gather a representative dataset of biometric samples that can be used for testing purposes. The dataset should be large enough, and contain samples from a sufficient number of different people, to later yield statistical confidence in the measured error rates.

The test dataset is divided into enrollment and verification data. Every enrollment is passed to the biometric enrollment algorithm and the number of resulting failures establishes the FTE rate. Matching is performed by comparing every verification sample against every enrollment sample for the entire dataset. Typically many millions of matches are performed and each comparison score is recorded. These scores are then statistically analyzed to produce the FMR and FNMR.

This quantitative benchmarking approach allows solutions to be directly compared for accuracy, speed, functionality, compliance, and quality. The findings are used not only to select the most appropriate suppliers for a given project but also to derive the optimal algorithm configuration for a given environment. For example, knowing the biometric error rates, the algorithm decision thresholds might be configured to yield a specific FMR for security purposes.

2.7 Greatest challenge faced by biometrics

Biometrics works well when the system gathering the biometric data is supervised such as in a police station or at a border crossing kiosk. However, should the capturing of the biometric data be unsupervised, then there is an opportunity for an imposter to replay the biometrics of the genuine user or use a fake biometric.

The question then becomes how a biometric system knows the samples are from the genuine live user and are not being replayed by an imposter. This is generally called “the biometric liveness” question.

As each of the three main biometric types is being described in this document (Voice, Face, and Fingerprint), the currently available techniques to address this *liveness detection* question will be discussed.

3 Voice Biometric

3.1 Voice Verification Techniques

Voice is a combinational biometric being based on both behavioral and physiological characteristics.

Voice verification splits into two categories:

- **Text dependent matching**

  This is a verification process which requires the user to speak the same phrase at verification as he/she spoke at enrollment.

- **Text independent matching**

  This is a verification process which requires the user to record some free text during the enrollment process and then to speak a random phrase during the verification process. The verification accuracy can be improved by having the user speak longer phrases during the verification process.

Text dependent matching generally has higher accuracy than text independent matching and it is considered to be less of a burden during enrollment as most text independent systems require at least 15 to 30 seconds of speech during the enrollment process.

In general, voice biometrics work with the use of a trained “background model”. There are typically two types of background models:

- **“Universal”**

  The “universal” background model represents the general characteristics of speech for a *given language.*

- **“Specific”**

  The “specific” background model represents the characteristics of a *particular phrase*.

Both are created from collections of voice samples. In general, the “specific” background models may be used to provide more accurate voice verification results.

3.2 How Voice Verification Works

To perform voice verification, a system will require an “enrollment” and a “verification” template. The enrollment process will require the user to speak a phrase or phrases which are then compared to the background model. How the user’s speech varies from the background model, becomes part of the enrollment template.

During the verification process, the user is again asked to speak a phrase. This utterance is then compared against both the enrollment template and the background model to produce a score. This score value is an indication of how likely the verification

and enrollment utterances were spoken by the same person. Typically, the same voice background model is used for both enrollment and verification processes.

Where this process can break down is in a situation where the background model is not representative of the enrolled user and an imposter. This is most often the case when "specific" background models are used and the enrolled user is not representative of the people with whom the background model was created.

For example, the "specific" background model might be created from US English speakers and a French person then enrolls speaking English. If that French person has a very strong French accent, then that accent provides some of the difference characteristics between the enrolled utterances and the "specific" background model created in English. If another French person attempts to verify as an imposter in place of the enrolled person, and assuming they have similar accents, then the imposter's verification template will also contain many of the same difference characteristics as the enrolled user. This may result in higher than expected scores in the matching process.

This is a flaw of the "specific" background model process. Background models produce more accurate verifications provided that the enrolled users are represented by the background model being used.

Voice verification checks that the verification utterance originates from the same person who uttered the enrollment utterance. The highest text-dependent verification scores will be obtained when the exact same phrase is uttered at both verification and enrollment. However, a specialized speech recognition algorithm may also be used to confirm that the correct expected phrase words were uttered, either at enrollment or verification.

Speech recognition refers to the process of recognizing the words spoken in an utterance instead of recognizing the person (speaker recognition).

A **text-validation algorithm** performs this efficient form of speech recognition to ensure that the correct requested phrase was uttered. The text validation algorithm is informed of what phrase to expect and then attempts to check that this phrase was indeed uttered. This is an easier problem than speech recognition which has no prior knowledge of the words or phrase that should be present.

While both verification and liveness must ensure that the spoken phrases originated from the correct person, there is also a need to confirm that the words uttered in the phrases are the correct words that have been requested. This is to prevent an attacker replaying another phrase, with the incorrect words, but recorded from the correct person.

- Text-validation is applied to the liveness challenge phrase. See next section on Voice Liveness.
- Text-validation may also be applied to the phrase uttered at enrollment to ensure that the user spoke the requested words.

3.3 Voice Liveness

An attacker may obtain recordings of a user's voice and attempt to replay them into a voice authentication system in order to be incorrectly authenticated as that user for fraudulent purposes. A number of techniques can be used to help prevent the replay of the enrolled utterances:

- **Replay detection**

  This technique focuses on examining the audio to determine if the artifacts of a *recording of a recording* can be found within the stream. If this technique is successful, it could provide a strong liveness detection method assuming that the attacker is unable to bypass the audio capture capability and feed the replay directly into the system as if it were coming directly from the microphone.

- **Random challenge phrase**

  This technique is based on using text independent matching and automatic speech recognition. At the time of verification, the user is asked to speak a random phrase, preferably one that s/he has not spoken or is unlikely to have spoken before. The system then performs a text independent verification for that user and also uses text validation to ensure that the user has spoken the phrase s/he was asked to speak. Both results are combined to produce a liveness result. Generally this technique does not provide high accuracy as compared with text dependent matching. As a result, it is most often combined with text dependent matching to improve the accuracy of the overall voice matching.

All of these techniques have merit, and as is the case in many biometric systems, a better approach could be based on applying multiple techniques at the same time – such as using a replay detection technique with a random challenge phrase technique.

3.4 Voice Accuracy

The accuracy of voice verification is impacted by:

- **Capture Device**

  This refers to the microphone used to capture the voice samples. There is a plethora of such devices now available as all cell phones, tablets, and laptops now come with integrated microphones. In addition, many users choose to add external microphones through webcams to their desktop and laptop computers. All these different types of microphones and associated sound cards have unique characteristics which may impact on the quality of the audio data being captured and as a result will impact on the matching accuracy.

- **Transmission channel**

  Traditionally audio from a phone is transmitted either over the traditional telephone (POTS) network or over the mobile network. More recently, with the introduction of VoIP systems, audio data can now be transmitted over IP networks. These channels connecting the callers generally compress the audio data to reduce the

bandwidth required to send the data. However, this compression is lossy, leading to degradation in the quality of the audio data being received. This degradation in quality is particularly difficult for voice verification systems. For example, if a user enrolls on a device such as a landline connected through one channel to the voice verification system, and subsequently verifies on a device connected through a different channel such as a mobile network to the system, the quality of the audio data being captured may be quite different and as a result will impact on the matching accuracy.

- **Background noise**

  Noise is a significant issue for voice systems as the capture devices tend to pick up background noise in the environment of the speaker. This makes it more difficult for the voice verification system to extract the pure speech audio of the speaker from the extraneous audio in the background.

The best matching accuracy is achieved when the user:

- Uses the same device to enroll and to verify.
- Uses the same channel to connect to the voice biometric system to enroll and to verify, where ideally, little or no lossy compression should be applied to the audio data.
- The user enrolls and verifies in an environment with the minimum of background noise.

Accuracy for voice verification and voice liveness algorithms are presented in the table below. The methods used to measure these error rates and their meanings are explained in Section 2.6. The tested capture environment used smartphones, tablets, and PCs.

Modality	Function	FMR	FNMR	EER
Voice	Text-dependent Verification	0.1%	1.8%	0.6%
Voice	Text-independent	2.00%	7.5%	5.00%

Table 1: Voice accuracy for verification (Daon measured rates)

These accuracy statistics were obtained using voice data collected from hundreds of volunteers using a mixture of smart device and PC microphones over three sessions. Each session ranged from a day to weeks apart. The voice data was processed offline, using Daon analytical tools (DaonAnalytics), to calculate the accuracy statistics.

Since the audio is captured directly on a smartphone or PC, it is recorded at a sample frequency rate of 16Khz. If the audio is captured in a call centre from a caller over the traditional telephone system, it would be at the lower sample rate of 8Khz, and this would degrade accuracy somewhat as less audio information would be present.

The accuracy for the two different voice liveness approaches is shown in the table below. The replay attack detection operates passively on the same utterance as used for

verification. The random challenge phrase requires an extra second phrase to be uttered by the user as part of the liveness challenge.

Modality	Function	APCER	BPCER	
Voice	Replay attack detection	1.6%	1.0%	
Voice	Random challenge phrase	4.6%	1.2%	

Table 2: Accuracy for voice liveness detection (Daon measured rates)

4 Face Biometric

Face is a physiological biometric that is based on the appearance of the face. People use faces to recognize each other. However, accurate machine algorithms are also available to perform face authentication. Since 2007, it has been shown that face verification algorithms can now outperform untrained humans. Only “super-recognizers”, which appear to be an elite group of face forensic examiners, can outperform algorithms and in challenging situations only.

4.1 Face Verification Techniques

There are a number of techniques used in face matching, which include:

- **Geometry of the face:** A shape-based technique using models based on the relative position of and distance between key features of the face such as the eyes, the nose and the chin.
- **Appearance-based:** A global representation of the face is derived based on measuring pixel value statistics, such as pixel intensities within the face image. The algorithm is trained to differentiate between the appearance measurements from different faces.
- **Skin texture:** This is a specialized texture-based technique which focuses on the finer details of the skin of the face, such as lines, spots, and other patterns. It requires high resolution images in order to detect and differentiate between these finer features. Skin texture approaches can potentially differentiate between faces of identical twins.
- **3D face:** This technology improves upon the single 2D image geometric methods by being able to construct a 3D model of the face geometry. Specialized illuminators and cameras, such as those using structured infrared light in the iPhoneX, may be used to capture the required data. This technique is more tolerant to the user moving, changing expression, or changing the orientation of the head. It also deals better with changes in hair style, the growth or loss of facial hair, glasses, etc.

4.2 How Face Verification Works

To perform face verification, a system will require an enrollment and a verification template. The enrollment process will require one or more photographs of the user from which key facial characteristics are extracted to produce an enrollment template.

During the verification process, one or more facial images of the user are captured from which the key characteristics are extracted to produce the verification template. The enrollment and the verification templates are then compared, using a face matching algorithm to determine the level of similarity between the two. A comparison score is produced which represents the level of similarity between the face captured at enrollment and the face captured at verification. An authentication decision can be made based on the value of the comparison score, or the error rates (FMR, FNMR) that correspond to the comparison.

4.3 Face Liveness

Face is a biometric which is very susceptible to compromise, since it is often publicly available from photographs or videos. Without countermeasures, most face verification systems with unsupervised capture can be compromised by an imposter using a photograph of the genuine user. Given the ubiquity of cameras, screenshots, and the sheer number of photographs posted to social networking sites, locating and placing a photograph of a genuine user in front of a camera is not complicated.

The three main presentation attacks against a face verification system use:

- **Static photo:** An attacker obtains and presents a photo of the genuine user to the capture camera.
- **Replayed video:** An attacker obtains and replays a video of the genuine user to the capture camera.
- **3D Mask:** An attacker constructs a 3D mask of the genuine user's face, and wears it while presenting to the capture camera. Such masks can be constructed from only two photos of the genuine user, providing a frontal and side view.

Face liveness detection algorithms are each designed to prevent one or more of these attacks. The methods used to help detect each form of attack are introduced below:

- **Static photo detection:** Active liveness methods look for movements within the face, such as eye-blink, eye-movements, and mouth movements. Some passive liveness algorithms examine the texture of the presented face to detect whether it is printed paper or a live face.
- **Replayed video detection:** An active challenge-response method may be used to request the user to dynamically perform some action which is not expected to be present in a random recorded video. For example, the user might be asked to turn their head in a certain direction, or to perform a specific facial expression such as smiling.

  A face-voice synchrony algorithm might challenge the user to utter a specific phrase and then check that the face mouth movements correspond to the vocal words uttered.

  Illumination-based challenge algorithms might shine different wavelengths or patterns of light on the user's face and expect to observe certain reflectance or non-reflectance responses.

  Additionally, some algorithms will attempt to detect the texture or artifacts introduced by the display medium. Two or more capture cameras, setup to allow stereo vision, can detect that a flat display medium is being used.
- **3D Mask detection.** A 3D mask, with a live attacker showing eyes and mouth, can overcome many of the earlier liveness detection methods. Detecting variations in face temperature with thermal sensors and detecting blood flow through face veins using infrared are both options requiring additional hardware. Current research suggests that it is possible to detect the texture and rigidness of a mask compared to a live face using only images from a regular camera.

4.4 Face Accuracy

Face verification accuracy can be impacted by several factors:

- **Illumination:** Poor quality lighting, reflections, and shadows on the face can cause significant issues. Ensure adequate lighting that is uniformly distributed over the face with no shadows or reflections.
- **Positioning:** The distance to the camera will impact the captured face resolution. If part of the face is missing from the captured image, the algorithm may have difficulty correctly matching it. The face should be at arm's length from the capture device and the full head should be visible on the capture screen.
- **Facial expression:** A different expression between enrollment and verification can negatively impact accuracy. Always use a neutral facial expression for optimal accuracy.
- **Pose:** The head angle will impact accuracy, and should be full frontal for best results.
- **Background:** A complex background, especially one containing other faces, can hamper face detection. Ensure no other faces or moving objects are present in the background.
- **Camera lens:** The camera lens should be kept clean to avoid any impact from dirt or smears.
- **Head clothing:** Hats, scarves, and earrings can obscure parts of the face. These should be removed for enrollment, and may need to be removed during verification.
- **Spectacles:** Glasses and sunglasses can partially obscure the face and eyes. Sunglasses should be removed for enrollment and verification.
- **User habituation:** Frequent users tend to be more familiar with the system and are more likely to position themselves correctly, yielding better accuracy.
- **Cosmetics:** Liberal use of cosmetics can temporarily alter face appearance.
- **Facial hair:** Face hair that covers large parts of the face can degrade accuracy if that hair is later removed or significantly changed.
- **Aging:** Faces age over time and if many years have elapsed between enrollment and verification, accuracy can be reduced. Update enrollments every few years as instructed by the system.
- **Surgery:** Some types of facial surgeries can permanently alter the appearance of a person's face, making it less likely to match an older enrolled image. Re-enrollment is recommended where this has occurred.
- **Injury:** Significant injuries to the face, which permanently alter the appearance, may reduce verification rates. As with surgery, re-enrollment is recommended.

Accuracy for face verification and face liveness algorithms are presented in the tables below. The methods used to measure these error rates and their meanings are explained in Section 2.6.

Modality	Function	FMR	FNMR	EER
Face	Verification	0.02%	6.3%	1.2%

Table 3: Face accuracy for Verification and Liveness (Daon measured rates)

These accuracy statistics were obtained using face data collected from hundreds of volunteers in challenging environments (including in cars, in poorly lit homes, etc.) using smart devices over multiple sessions. For the verification data, there was at least a day between each session.

The table below shows three different face liveness detection algorithms, the attacks they prevent, attacks that may sometimes succeed, and the BPCER (genuine reject) error rate.

Modality	Liveness technique	BPCER	Attacks prevented	Attacks that may succeed
Face	Eye-blink detection	6.0%	Photograph, printout, or screen image, where eyes not blinking.	Video recording of the person blinking Photo of the user with cut-out eyes or 3D mask.
Face	Head movement detection	2.0%	Photograph, printout, screen image, or basic mask (with or without cut-out eyes)	CVideo recording of the correct person performing the requested head shake or head nod, Advanced 3D mask
Face	Passive liveness	5.0%	Prevents many photographs, printouts, screen images, video recordings, basic masks, and 3D masks.	Limited number of higher resolution videos, basic masks, and 3D masks.

Table 4: Face anti-spoofing accuracy (Daon measured rates)

The strongest liveness solution will be obtained by combining two or more of these individual liveness detection techniques. For example, passive liveness can be used in conjunction with head movement, and this prevents more attacks than any single

method alone. The table below estimates the security and convenience of each technique and when the techniques are combined.

Face liveness technique	Security	Convenience
Eye blink	Low	High
Head movement (shake or nod)	Low-medium	High
Passive	Low-medium	High
Eye blink + Passive	Medium	Medium – High
Head movement (shake or nod) + Passive	High	Medium
Random combination of shake, nod and blink	High	Low
Passive with a random combination of, shake, nod and blink	Highest	Low

Table 5: Security & convenience of different face liveness techniques

5 Finger Biometric

Finger is a physiological biometric based on the pattern and details on the surface of the fingerprint. It is one of the most established biometrics, especially for government and law enforcement applications.

5.1 Finger Verification Techniques

There are a number of techniques used in finger matching, which include:

- **Minutiae:** The lines on a fingerprint, called ridges, will come to an end or split into two lines at specific location points on that finger. These ridge endings and bifurcation feature points are termed minutiae.

  A finger minutiae-matching algorithm compares the location of these points between two fingerprints. Additional information, relating to the minutiae, such as the number of ridge lines between a pair of points and their relative distances may also be used during comparison.

- **Pattern:** The flow of ridge lines forms unique patterns on a fingerprint. A finger matching algorithm can compare these patterns between two fingerprints. Some algorithms will subdivide the fingerprint into smaller square cells and compare the patterns in each cell. These pattern-based algorithms can be better suited to smaller low resolution sensors where minutiae details are not fully visible.

- **Ridge details:** With high resolution images, the intricate details that are present on a single ridge line, such as sweat pores and individual ridge contours, can be measured and compared. Image resolutions of 1000 DPI are preferred for algorithms that rely on comparing these fine ridge details.

5.2 How Finger Verification Works

During registration a finger enrollment template is created using features extracted from one or more captured images of a single finger. In a system where multiple fingers can be used, an enrollment template is created for each unique finger.

During the verification process, one or more images of the selected finger are captured, and the unique features are extracted to produce a verification template. The enrollment and the verification templates are then compared using a finger matching algorithm to determine the level of similarity between the two. A comparison score is produced which represents the level of similarity between the finger captured at enrollment and the finger captured at verification. An authentication decision can be made based on the value of the comparison score, or the error rates (FMR, FNMR) that correspond to the comparison.

5.3 Finger Liveness

A fingerprint system can be attacked by presenting a fake finger to the sensor. The two main presentation attacks against a finger verification system use:

- **Artificial fingerprint**

  An attacker obtains a copy of the genuine fingerprint, and then creates a fake finger with the same fingerprint features. Some materials which are used to create fake fingers include gelatin, silicone, latex, glue, and modelling clay.

- **Cadaver finger**

  An attacker obtains a severed dead finger from a genuine user and presents it to the sensor. Optical-based finger sensors are more susceptible to this, and the longer the finger has been severed, the more difficult it will become to capture ridge-pattern details of sufficient quality.

A number of liveness detection algorithms have been designed to prevent these attacks and include the following methods:

- **Electrical properties:** The electrical properties of the finger, such as its impedance or resistance to an electrical current will differ between live fingers and fake materials. Transparent electrodes can be embedded within the finger sensor surface to obtain these measurements.
- **Pulse:** Specialized hardware can also be used to measure pulse, blood pressure, pulse oximetry, and electrocardiogram signals to confirm that a live finger is present. Pulse oximetry measures the oxygen content of the blood in the finger. Electrocardiogram measures electrical signals from the heart, using two electrodes each of which must be touched by a finger from a different hand.
- **Multi-spectral light illumination:** Using a specialized multispectral sensor, the reflection of multiple wavelengths of light and different polarizations can be used to detect the presence of fake finger material.
- **Perspiration:** Sweat pores are present on the ridge lines of a fingerprint and a live finger continually perspires through these. By monitoring the moisture pattern from these sweat pores over a short time period during finger capture, the liveness of the finger can be confirmed.
- **Temporary skin deformation:** The skin on a fingerprint is stretched (or temporarily deformed) when it is pressed down on a capture sensor. A fake finger is more rigid and will often be stretched less, which can be used to detect the attack.
- **Ultrasound:** A fingerprint image can be captured using ultrasound technology; and it has been shown that information from the ultrasound echo measurements can be used to differentiate a live finger from a fake one.
- **Other finger characteristics:** The temperature and odor of a finger can be measured to help determine that it is a genuine live sample.

5.4 Finger Accuracy

Finger verification accuracy can be impacted by several factors:

- **Sensor:** The sensor size and captured image resolution will significantly impact finger accuracy. Large optical sensors, producing images at 500 DPI and above, have been shown to yield the best accuracy, while small capacitive sensors will yield less accurate results. The sensor should be kept clean and free from scratches and dirt.
- **Finger quality:** The clarity and strength of the pattern on the fingerprint will impact accuracy. Dry, cracked, and damp fingers typically result in poor quality finger images. Some professions and sports can degrade finger quality. Examples include manual workers, and those who regularly rock-climb and play the guitar with their bare fingers.
- **Positioning:** The way the finger is placed on the sensor will impact accuracy. If a different part of the finger is placed on the sensor at verification compared to enrollment, as can happen with a small sensor, then this may cause a false non-match. The length of fingernails and cosmetic fingernails can impact positioning. The finger should always be placed in the same position on the sensor.
- **Age:** Older people tend to have poorer quality fingerprints. In addition, minor damage to an older person's finger tends to take longer to heal. Both of these factors can contribute to higher false non-matches for this segment of the population.
- **User habituation:** Frequent users tend to be more familiar with the system and are more likely to position themselves correctly, yielding better accuracy.

Summary accuracy for leading finger verification algorithms, as benchmarked by the US National Institute of Standards and Technology (NIST), are presented in the table below. The methods used to measure these error rates and their meanings are explained in Section 2.6. The tested capture environment was optical sensors connected to desktop computers.

Modality	Function	FMR	FNMR	EER	Supplier
Finger	Verification – desktop	0.01%	0.50%	<0.50%	Multiple – optical sensors

Table 6: Finger accuracy for verification (NIST results)

These accuracy statistics were obtained from the NIST Fingerprint Vendor Technology Evaluation (FpVTE) 2012, published as NIST IR 8034. The evaluation datasets were based on US government operational datasets using large optical area fingerprint sensors. The results above apply for single finger verification using either the right or left index finger.

Traditionally, fingerprint capture has taken place using finger devices with optical sensors connected to fixed workstations. The US National Institute of Standards and Technology (NIST) have extensively tested fingerprint algorithms with images from such optical finger sensors. The accuracy rates shown in the table above for “Verification – desktop” are taken from these NIST results.

Use of fingerprint sensors on mobile consumer devices such as smartphones is a much more recent development. The majority of flagship smartphones now have an embedded fingerprint sensor and these are expected to become ubiquitous in smartphones within the next five years. This is bringing biometric technology to a widespread market. These consumer-grade sensors are small silicon sensors and do not capture the quality or size of images available from certified optical readers.

Based on our own quantitative testing with small silicon sensors, Daon estimates that the false non-match rate, where a genuine user is incorrectly rejected, will be higher on these smaller consumer sensors.

6 Alternative Biometrics

There are a number of alternative biometric modalities that rely on measuring other unique physiological or behavioral characteristics of an individual. Some of these are already widely deployed in government or law enforcement projects. Most of them are not yet widely deployed in smartphones or tablet scenarios, especially for consumer authentication. These alternative modalities are introduced below and their strengths and weaknesses examined.

6.1 Behavioral Keystroke Dynamics

Measuring the unique timing information while a user types on a keyboard or a touchscreen keypad provides another behavioral biometric trait. A keyboard dynamic algorithm will measure the timing information obtained from when a user presses a key, releases a key, presses the next key, and so on.

While an attacker may know the phrase to be typed, they will be less likely to be able to reproduce the correct timing of pressing the necessary keys. Accuracy is weaker than physiological biometric traits, such as finger, iris, face, or voice, but will be highest when the user is always asked to type the same phrase.

For example, Daon testing has shown that if the same keyboard is always used for typing the user's e-mail address, an EER of 2% (98% of genuine user attempts are recognized) is achievable. When a different keyboard is used between enrollment and verification sessions, the EER increases to 5%.

Keyboard dynamics can be used on shared PCs to ensure that the correct user is present and to limit access to content. With touchscreen smartphones keypad dynamics are sometimes used as part of a continuous authentication process that monitors the user activity and builds up an authentication confidence over time that the correct user is present.

6.2 Iris

The iris is the colored circular structure at the front of the eye which controls the diameter and size of the eye pupil. The texture pattern of the iris is highly unique and is fixed before birth, although the iris color can change in the first year of life. While most people in the world have brown eyes, it is not the color but the detailed pattern of the iris that is used for recognition purposes. With darker iris colors, the details of this pattern cannot be seen using only visible light, and so during capture of an iris image, the eye is illuminated with near-infrared light which shows the pattern details. One or more near-infrared illuminators are required to produce this light during capture.

Specialized iris capture cameras have been in use in government and enterprise applications for many years. For example, some national identity projects use iris to help ensure that each citizen can only obtain a single identity number. In some airports, iris is used both to authenticate travellers and to search against a ‘watch list’ of known suspects.

Iris has not yet been widely deployed on smartphones, partly due to the requirement for an additional near-infrared illuminator and a camera sensor that can be used for both infrared iris capture and visible light photos. Sunlight also contains significant amounts of near-infrared light and this can interfere with the iris capture in some outdoor settings. Nevertheless a small number of iris enabled smartphones have recently become available, and the number is expected to increase in the coming years.

Since the iris is captured with near-infrared light, a video or screen image will not be captured correctly using normal visible light, and so cannot be easily replayed to spoof the system. However, there are a number of additional iris liveness techniques that can be implemented in conjunction with existing specialized iris cameras. Some look for changes in pupil size in reaction to light; others look for continuous micro variations in the pupil size; others look for reflections from the eye surface; others look for reflections from the retina at the back of the eye; while some examine the texture of the eye to detect printed contact lenses. Some of these techniques will not be suitable for implementation with smartphones due to the expected movement of a handheld device and the less constrained environment.

Iris biometrics can offer a very low false match rate (FMR), especially if images are captured from both eyes. A single iris image contains more usable unique information than a single full fingerprint, that is a FMR of better than one in a million (0.0001%) is achievable with only one eye. Since both irises of the same person are independently unique, using two eyes will give significantly even more accuracy. The genuine reject rate, the FNMR, is similar to that of fingerprint and will be quite dependent on the iris capture device used. Handheld binocular shaped devices that are placed over a person’s eyes to block out all outside light will give better accuracy than a smartphone camera held at varying distances from the eyes. Iris biometrics is expected to become more popular in personal smartphone devices, but due to the limited number of current devices that provide iris capture, the deployment accuracy has not been well studied.

6.3 Retina

The retina is the internal layer at the back of the eyeball that contains a unique pattern of blood vessels that can be used as a biometric. With sufficient lighting, the retina is visible through the pupil of the eye. Opticians now regularly capture images of the retina as part of a routine examination to check the health of the eyes. As with the devices used by opticians, a user must place their eyes close to a binocular retina capture camera, often resting their head or chin against part of the device. This capture is more intrusive than other biometrics and so is not suitable for use with current smartphone and tablet models.

Retina biometrics, like iris biometrics, can be very accurate, but have limited deployments due to the specialized devices and inconvenience during capture compared with other modalities. Retina biometrics have been used in physical access control devices for high security installations. The failure to enrol and failure to capture rates are also higher than iris. Some users may also have privacy concerns, in that the retina image can reveal some personal (although limited) health information.

There are no known uses of retina capture on smartphones or tablets today, and we do not expect that to change in the near future.

6.4 Eye-vein

The visible blood vessels in the white sclera of the front of an eye can be used as a physiological biometric. While some of these blood vessels are visible when a person is looking frontal at a capture camera, additional vein information can be captured if the person looks left or right, thereby exposing more of the white sclera.

In cases where it is not desirable to have the person look away from the camera, other facial biometric information, such as the periocular features around the eyes, can also be matched to supplement the eye-vein matching.

Eye-vein and periocular biometrics have been deployed in smartphones for authentication purposes. The use of eye-vein biometrics is controlled by patents held by a single algorithm vendor, which is a similar situation that existed for iris biometrics fifteen years previously.

There has been limited independent large-scale testing of the accuracy of frontal eye-vein with periocular on smartphones, but it appears to be comparable to other biometrics such as a single finger or face. Efforts have also been made to prevent a variety of replay spoofing attacks but some parties claim to have been able to overcome these with a single image.

6.5 Other Vascular Patterns

Other parts of the human body, in addition to the retina, exhibit unique patterns of blood vessels that can be used as biometrics. Biometric devices have been developed to capture and analyze the vascular patterns in a finger, in the palm, on the back of the hand, and from the wrist. Some of these capture devices are contactless, so that the area being imaged does not need to physically touch a sensor surface. The devices use near-infrared light to obtain an image that shows the blood vessels, as these are often not visible under normal visible light. The matching algorithms use pattern matching techniques to verify identity.

While it is intrinsically more difficult to spoof patterns of blood vessels that appear beneath the skin, vein biometrics are not immune to spoofing attacks. Some academics have demonstrated how to successfully spoof popular palm and finger vein devices.

False rejects may also occur with vein biometrics due to changes in temperature which cause the blood vessels to expand or contract, the interference of external lighting with the infrared capture similar to iris capture, and obstructions such as hair on the back of the hand diminishing the image quality.

Vascular patterns are not suitable for collection by current smartphone and tablet devices.

6.6 Palm

Palmprint biometrics use the unique ridge lines and creases on the surface of the palm of the hand, similar to approaches used for fingerprint biometrics. Palmprint biometrics are used in law enforcement applications, including matching against latent palmprints present at crime scenes. Since the palm area is much bigger than a fingerprint, it contains more unique information and can provide greater accuracy than one or two fingers alone. In law enforcement applications, a large optical platen sensor is used to capture the palmprint from a live individual, usually at the same time that fingerprints are captured.

Recently commercial contactless palmprint algorithms have emerged for use with smartphones. The front or back smartphone camera is used to capture one or more images of the palm and match it against an enrollment palm image captured from the same device. Matching smartphone palm photos is considerably more difficult, and less accurate, than when using traditional optical sensors on which the palm is placed. The correct positioning of the hand and keeping it outstretched and parallel to the smartphone can be challenging. The impact of lighting and shadows on the palm also have an impact, as they do with face biometrics. Segmenting the palm from the background, especially where that background shares similar colors to the palm, further adds to the challenge. Liveness detection challenges will also exist as the palmprint is being captured at a similar distance as a photo or video.

6.7 Hand geometry

Hand geometry measures the shape of a person’s hand, including the length, width, and height of the fingers, and the distances across portions of the palm. Hand geometry has been in use for decades in physical access control devices, especially for secure facilities such as prisons or data centers. In these scenarios the hand is placed on the flat surface of a special device, with pegs used to guide the placement, while one or more cameras capture images of the hand.

Images of the hand can also be captured using a smartphone, and hand geometry measurements extracted. The user will hold their hand outstretched while the back camera takes a photo. The correct positioning of the hand is a challenge as there is no flat surface or pegs to help ensure optimal placement. Instead, the scheme relies on the user’s becoming habituated and learning how to correctly position their hand parallel to the smartphone and to keep it outstretched.

Hand geometry, and especially when using a smartphone for capture, is less accurate than other smartphone biometrics including finger, face, and voice. However, it could be

used in conjunction with other information captured contactlessly from the hand such as palmprint or even fingerprint. Since an image of the biometric is being captured without contact using the smartphone camera, the same liveness challenges as with capturing a face will exist.

Hand or finger geometry are not commercially deployed in smartphones, but research work has been investigated in this area along with contactless palmprint.

6.8 Signature

The way a person uniquely signs their signature with a pen or a finger can be used as a behavioral biometric. Where a tablet or smartphone screen is used, the signature can be created with a finger, rather than a stylus, although this is less accurate. Signature biometrics are not restricted to a person's personal signature but can be applied to any words, phrase, or figures that the owner can repeatably generate.

The signature biometric algorithm will examine the location co-ordinates of the signature as it is written on a screen with a stylus or finger and the speed of the writing along the signature lines. Where a specialized signature tablet is being used, the pressure exerted by the stylus on the screen during the signature is also measured. Measuring the speed and pressure elements provide some degree of liveness detection, in that an attacker who has a copy of a person's signature and can accurately write that signature will not know the speed that the different signature components are written at or the pressure applied.

While signature biometrics have been used by financial institutions using specialized signature capture tablets, they have not yet been widely deployed to smartphones. There are a number of research projects and commercial offerings that use finger pattern signatures as one of several behavioral biometrics that are combined together to reach a required authentication confidence level.

6.9 Gait

The manner in which a person walks, or their gait, can be used as a behavioral biometric. With traditional gait biometrics, cameras are used to observe a person at a distance and measure their walking speed, step length and width, and movement of hips, knees, legs and ankles.

Some indirect gait analysis can also be performed by a smartphone, where the accelerometers and gyroscope sensors are used to take measurements while the person is walking or moving. These sensor readings can be used to build a unique gait profile for the person, although the accuracy is not as good as the main physiological biometrics used on smartphones. Due to the weaker accuracy, these smartphone gait measurements may be used as part of a continuous authentication scheme where multiple biometrics are used to build up and maintain a confidence that the correct user is in possession of the smartphone device.

Under some circumstances, such as with "rooted" devices where operating system administrator privileges have been obtained, it may be possible to spoof the device

sensor readings and allow incorrect measurements to be passed to the authentication algorithm. Software checks can be made to reduce these risks.

6.10 Ear Shape

The shape of a person's outer ear and the features on it have been used in law enforcement applications to help match a person against a latent ear print left on a glass surface at a crime scene. Algorithms have also been created for smartphones that extract ear shape features from a video of the ear or from the points of the ear that are placed against the smartphone touchscreen. Ear shape could be considered convenient as it might be captured when answering a telephone call and placing the smartphone against the ear.

No large independent studies of ear shape accuracy for smartphones exist, but extracted ear information is less unique than other biometrics such as finger or face. The same liveness challenges that are present for face, will exist for ear shape.

6.11 Electrocardiography (ECG)

The electrical activity of the heart, or electrocardiography, can be used as a unique biometric trait. A popular method to measure this involves the user touching a conductive material with one finger from both hands, while a verification measurement is taken for a few seconds. Alternatively, the sensing device might be incorporated into a wrist band worn on one arm while a finger from the other hand must touch it to complete the circuit and allow an electrical measurement to be made.

There are limited independent studies of the accuracy, especially over the longer term, of heart rhythm based biometrics, and measurements may be affected by the current state and wellness of a person. ECG biometrics are not in widespread use although there is at least one vendor offering a proprietary wristband that measures the heart rhythm for authentication. However, with the advent of smart watches and wearables that measure heart rate and other bio signals, its popularity may increase.

6.12 DNA

DeoxyriboNucleic Acid (DNA) is a long molecule, present in human cells, that contains a person's unique genetic code. DNA is an extremely unique identifier of a person that does not change throughout their life. However, it cannot yet be used to differentiate between genetically identical twins although some research is underway that might allow DNA mutations to be used for this task.

The current challenges with DNA are that it is both expensive and slow to extract. It can still cost several hundred dollars to extract the unique DNA biometric markers for a person, and the fastest current devices still take about ninety minutes to perform this. In addition, other genetic and medical information could be extracted from the DNA, which raises privacy concerns. DNA is not suitable for use with current smartphones and tablets.

7 Multi-Biometric Fusion

Multi-biometric fusion refers to combining information from two or more biometrics within a system. Data from multiple biometrics is combined or fused to improve the accuracy, security, and/or usability of the system.

7.1 How Multi-biometric Fusion Works

A generic multi-biometric fusion process where two biometrics are combined is shown in the figure below. Biometric capture and verification matching are performed with each sample separately as in a single biometric system.

For example, Sample 1 might be a face image which is captured and matched against the enrolled face to obtain a face matching score. Sample 2 might be a voice sample which is also captured, matched against a voice enrollment, and a voice matching score generated.

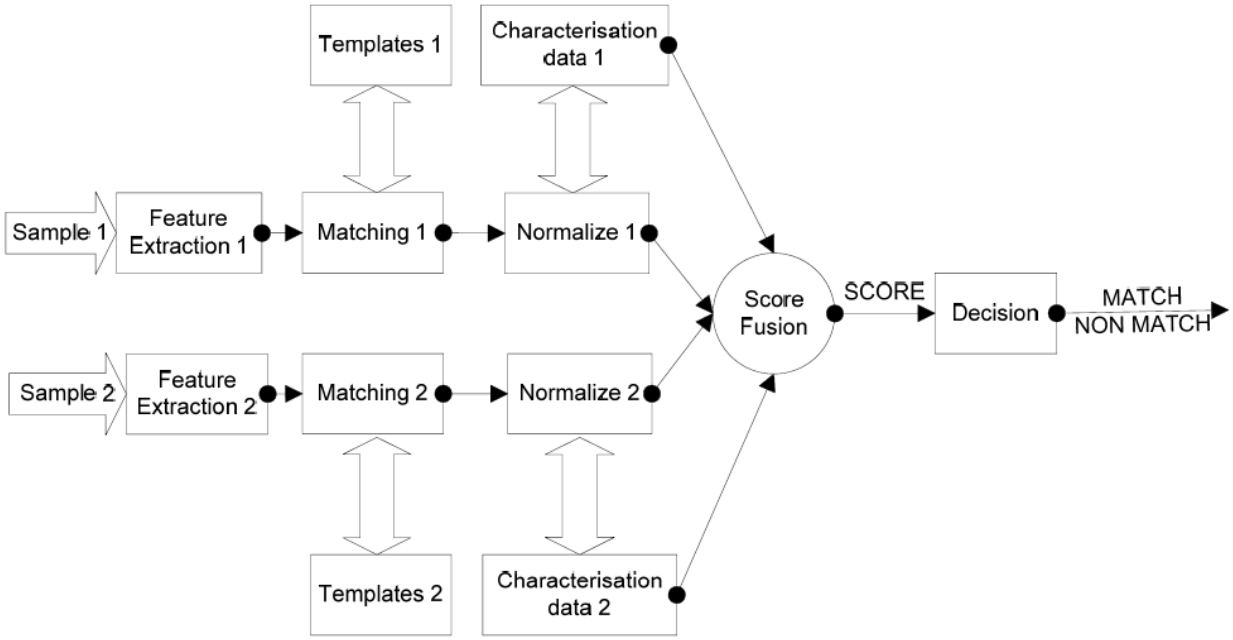

Figure 2: Multi-biometric Fusion Process (ISO/IEC TR 24722 Technical Report)

In order to fuse the two scores, Sample 1 and Sample 2 must first be normalized which is the process of converting the value to the same scale. Once the scores are normalized, they can be fused or combined to give an overall score value which is used as the basis for the decision.

7.2 Fusion and Liveness

Multi-biometric fusion can be applied both to traditional verification algorithms and to liveness algorithms. For example, liveness scores from multiple liveness detection algorithms may be combined to generate an overall fused liveness score. Furthermore, a verification score may be combined with a liveness score to produce a final authentication result.

In practice, minimum thresholds are often set for both verification and liveness algorithms that are fused in order to ensure that the fusion algorithm contributes some confidence to the overall authentication result.

For example, in order for an authentication to succeed, it may be necessary to perform well enough in both voice verification and voice liveness tests.

7.3 Fusion Accuracy

More verification data is usually better, and if a fusion process is configured correctly, it should always improve or at least equal the non-fused accuracy. Fusion accuracy will be impacted by the normalization and fusion techniques applied, and the amount of training data available.

Since greater accuracy is obtained when using fusion, the thresholds and error rates required for each modality alone in the process can usually be relaxed. That is, a lower confidence in face or voice can be allowed, because when combined the security is far better than either alone.

The table below shows the verification error rates at the selected minimum thresholds for each modality when performing fusion. These fusion settings have lower FNMR but higher FMR for face and voice alone than earlier default thresholds when not using fusion. However, the combined fused security (FMR) is much better than either alone.

Modality	Function	FMR	FNMR
Face	Verification	0.1%	3.7%
Voice	Verification	0.3%	1.0%
Face-voice	Fused verification	0.0003%	4.7%

Table 7 Fusion Accuracy for Face–Voice Verification (Daon measured and derived rates)

The fused accuracy statistics were derived by fusing the individual face and voice scores, using FMR product fusion. Score fusion is more suitable than decision fusion, as the many different scores that occur can be taken into account to improve achieved accuracy while with decision fusion there are only two possible scores (pass/fail).

8 Summary

Several different biometric modalities, including face, voice, finger, iris, and behavioral keystroke have been described above. Each modality has its own strengths and weaknesses and some will be more suitable for certain scenarios than others. For example, face and voice can be captured with existing standard cameras and microphones such as found on many consumer devices, while fingerprints still require specialized sensors and iris requires special illumination.

Because a probability of error occurs with all biometrics, the different accuracy rates were reported across modalities, showing the potential trade-offs. Providing a choice of biometric modalities increases inclusion (more people can use the system) and enhances user experience.

Biometric-based systems can be attacked using fake or copied samples, and attack methods were described. However, the liveness mechanisms to detect such attacks are advancing, although they will not be required in all scenarios. Combining multiple biometric samples will increase both accuracy and security, providing further resilience.

The growing trend towards ubiquitous use of biometrics on consumer devices is soaring. As an authentication factor, biometrics offer a level of convenience and flexibility to users that other factors cannot, while at the same time helping to increase user security and reduce fraud.