When we talk about biometrics, most of us think of it as fingerprints recognition or iris scanning. However, there are other biometric techniques as well that are gaining popularity and being adopted worldwide. In this article, we will compare 5 common biometric techniques and consider their pros and cons.

1. **Fingerprint Identification**

A biometrics technique based on fingerprints looks for specific line patterns on the surface of your fingers. The ridge endings, bifurcations and islands making up the line pattern are then stored as an image. It is a very efficient and easy method of storing individual information and is the most common biometrics technique. It is also an easy to use and cheap technology.

The disadvantage of fingerprint identification is that since it is an external characteristic, its image can be copied and replicated – even if you store it in an encoded format. As an image, it can be compared and used to generate same code. Using technology that is relatively accessible, fingerprints can be spoofed. Moreover, another uncommon point that still needs consideration is that a fingerprint presented for recognition can be forced or does not essentially have to be attached to a body. Fingerprints also wear away in old age. Hence, some people may go through the trouble of being unable to register their prints.

1. **Iris Recognition**

Iris recognition uses a scanner to read the unique characteristics of the iris and then converts the information into an encrypted barcode. When performed with the help of infrared light, it is considered to be an excellent biometric security technique and is used in many [security applications](http://www.cardzgroup.com/ContactSmartCard.html).

One of the drawbacks of iris recognition is the resistance from users. Many people find it inconvenient to have their iris scanned, since it requires them to be in a certain position, causing them discomfort. It is also important to consider that even though iris scanning provides a high security level, it can come at the expense of speed.

1. **Facial Recognition**

Biometrics technique using facial recognition analyzes the position and shape of parts of a face to recognize a match. Features such as skin are also taken into account. Facial recognition is more commonly used as a security feature in identifying a face in complex images. The technology has rapidly developed over the years and is very helpful in remote recognition. Another advantage of this technology is that it helps in ‘negative identification’ – which means that it excludes faces from a crowd to narrow down suspects.

However, this technique usually works accurately if a person is looking straight at the camera. Although it is developing rapidly, it is still behind vein pattern or iris recognition in terms of accuracy.

1. **Vein Pattern Recognition**

In vein pattern recognition, the bifurcations and end points of veins in fingers or palms are captured as an image, digitized, and stored as an encrypted code. The technology is considered secure due to the fact that veins are beneath the surface of the skin rather than on it, and not easy to replicate.

However, an important fact to consider is that it is hard to recognize vein patterns of very cold fingers or ‘dead fingers’ (Raynaud’s Syndrome). The technology is also comparatively expensive and still relatively unknown to many.

1. **Voice Recognition**

Voice is another inherent individual feature like face and fingerprints. Voice recognition requires least effort from users and hence, is very convenient. This technology is used commonly in areas that require processing of user’s voice, such as call centers. It can also be used in security areas, such as forensic analysis, credit card verification, and teleconferencing, etc. For systems that require high level of security, voice recognition can be combined with another biometrics technique such as fingerprint recognition to provide two-factor authentication.

However, many users still may have privacy concerns about how their data is stored. Moreover, voice recognition may not work successfully in noisy places or in cases where an individual may have a respiratory illness.

**Final Thoughts**

There are many other physical and behavioral biometric authentication techniques out there in the market and each comes with its own advantages and shortcomings. However, one thing is for sure. Biometric methods are much safer than typical passwords due to their functionality based on unique human characteristics. With so many options now available to us, the future is definitely passwordless.