Facial recognition has a long history dating back to the 1800s. To track down criminals, such as infamous bandits Jesse Woodson James and Billy the Kid, law enforcement would place “Wanted Alive or Dead” posters advertising bounties and soliciting public cooperation to help locate and even apprehend the alleged criminals. In addition to the bounty, these posters would include a photo and brief description of the crime, which would then be circulated to law enforcement agencies around the country and displayed in every US Post Office to speed up apprehension.

Facial Recognition

Advancements in artificial intelligence and biometric technology have led to the widespread use of computerised facial recognition.
Today, technology such as social media, television and other more specialized communication networks play a more influential role in the recognition process. Advancements in artificial intelligence and biometric technology, including the development of Machine Learning capabilities, have led to increased accuracy, accessibility and the widespread use of computerized facial recognition. The significance of this means that facial recognition can occur on an even larger scale and in more challenging environments.

This article will explore key milestones and technological advances that have resulted in the modern incarnation of facial recognition, before discussing the capabilities of cutting-edge “one-to-many” technology which is increasingly being used by counter-terror defense, police and security forces around the world.

Technology Inception And Developments

The technology was able to match 40 faces an hour, which was considered very impressive at the time.

The 1960s marked the start of computerized facial recognition, when Woodrow Wilson (Woody) Bledsoe developed a way to classify faces using gridlines. Bledsoe’s facial recognition still required a large amount of human involvement because a person had to extract the co-ordinates of the face’s features from a photograph and enter this information into a computer. The technology was able to match 40 faces an hour (each face took approximately 90 seconds to be matched) which was considered very impressive at the time.

By the end of the 1960s, facial recognition had seen further development at the Stanford Research Institute where the technology proved to outperform humans in terms of accuracy of recognition (humans are notoriously bad at recognizing people they don’t know). By the end of the century, the leading player in the field was a solution that came out of the University of Bochum in Germany – and the accuracy of this technology was such that it was even sold on to bank and airport customers.

From this stage on, the facial recognition market began to blossom, with error rates of automatic
facial recognition systems decreasing by a factor of 272 from 1993 to 2010 according to US Government-sponsored evaluations.

**Modern Usage Of Facial Recognition**

Fast-forward to the modern day and facial recognition has become a familiar technology when using applications such as the iPhone X’s Face ID capability or MasterCard Identity Check, passport e-gates at airports and other security and access control points. These solutions implement a consensual form of identity verification, as the user has a vested interest in being identified.

This is a “one-to-one” facial recognition event, one person in front of the camera being compared to one identity either on a passport or the app. In these scenarios, the hardware is specifically developed for the application at hand, therefore technically much easier to accomplish.

Facial recognition can now be used in a variety of governmental and commercial environments

The safety and security world brings a much more complex problem to solve – how to pick out a face in a moving and changing environment and compare it to several faces of interest. “One-to-many” facial recognition is a much harder problem to solve.

It’s even more challenging when the aim is to achieve successful and accurate recognition on commonly available hardware like live CCTV feeds and standard computing hardware. And unlike in the 1960’s where identifying a face every 90 seconds was acceptable; the safety and security market requires near instant feedback on who a person matched against a watchlist is.

**Security And Safety Applications**

The idea behind all facial recognition technologies is broadly the same: you start with an image of a person’s face (ideally a high quality one, although machine learning means that to a point we can now even use video without reducing accuracy). A fully front facing image is best, think a passport photo, but machine learning and new software has made this more flexible.
An algorithm converts this image into a numeric template, which cannot be converted back to an image and so represents a secure one way system. Every numeric template is different, even if it started out as an image of the same person, although templates from the same person are more similar than templates from different people.

The accuracy of facial recognition continues to increase alongside deployments in more challenging and complex environments

What happens next sounds simple although the technology is extremely complex: templates of people's faces are taken in real time and compared to those in the database. The technology identifies individuals by matching the numeric template of their face with all the templates saved in a database in a matter of seconds or milliseconds. To put this into perspective, imagine you are at the turnstiles of a busy train station looking for a person on the run.

Today's facial recognition technology would be able to identify that person should they pass in view of a CCTV camera, as well as notify the police of any additional persons of interest, whether they are a known terrorist or missing vulnerable person on an entirely separate watch list.

Because of technical progression, facial recognition can now be used in a variety of governmental and commercial environments, from identifying barred hooligans attempting entry at a football stadium or helping self-excluded gamblers at casino to overcome addiction.

Real-Time Assessments

The latest evolution of facial recognition pits the technology against an even more challenging application – directly matching individuals from body worn cameras for real time recognition for police officers on the beat. This capability equips first responders with the ability to detect a person from a photo and verify their identity with assurance.

The broader implication for this means that every interaction, such as stop and search or arrest, can be supported by real-time facial recognition which will see cases of mistaken identity driven down on the streets. First responders can now for the first time be deployed and furnished with
the ability to identify wider groups of people of interest with a degree of accuracy that previously relied only on the fallible human memory.

As the accuracy of the technology continues to increase alongside deployments in more challenging and complex environments, its ability to support government initiatives and law enforcement means the debate about the lawful and appropriate use of facial recognition must be addressed. Facial recognition should not be everywhere looking for everyone, but when used properly it has the potential to improve public safety and we should make the most of its potential.

Author Profile

Fernande van Schelle
Facial Recognition Technology To Enhance Travel And Banking In 2018

2018 will start to see facial recognition and other biometrics used in a combination of ways, but I’d like to look even further into t...

Surveillance Data And Artificial Intelligence To Drive Video Analytics...

The security industry remains interested in capturing actionable data from video analytics and this year we saw increasing interest from non...