FACE FACTS

Tim Noest *explains how facial recognition technology has finally come of age*

Picture credit: The Face Recognition Company

After several false dawns, facial recognition technology is finally ready for widespread, scalable deployment across a broad range of scenarios, including the challenges raised by COVID-19 face covering requirements.

While facial recognition may feel like a relatively recent development, it has actually been around for more than 50 years. Woodrow Bledsoe is credited as being the father of computer-based facial recognition in the sixties, when he classified faces by plotting horizontal and vertical coordinates of features, and then used a computer to find matches.

While Bledsoe's efforts were ultimately unsuccessful, the principles remained the same for many years: measuring distances between key facial features (eyes, nose, mouth, jaw) and converting those measurements into a unique data set, which can then be matched in a database.

Research in the field continued to advance the underlying methods over the next few decades, supported by parallel developments in camera technology, machine learning and data processing power.

Arguably, face recognition entered modern mainstream awareness in the early 2010s, when Facebook implemented facial-recognition-based photo tagging. At first it was very hit and miss, which only added to the public interest – it was funny to see our faces being matched to people who looked nothing like us. But then Facebook got serious about things and, through its DeepFace research group, developed a highly advanced neural facial recognition network. This deep-learning technology, combined with access to millions of face images from users, enabled Facebook to dramatically improve its face recognition capabilities.

In parallel with Facebook's efforts, other specialist face recognition companies were developing deep learning solutions, while independent academic research in deep-learning-based object recognition also accelerated.

Nick Pears has conducted and led computer vision research at the University of York for over two decades, and specialises in the analysis of human facial images, including face recognition technology.

Face recognition can be used to enhance security and provide alerts about individuals that pose a potential threat

"Over the last ten years, there have been four key technological factors that have been the driving force behind the emergence of high-performance face recognition technology" he explains. "First, there has been a remarkable increase in camera resolution and decrease in cost of digital imaging, predominantly driven by developments in smartphone camera technology; second, the performance-cost ratio of computational hardware has massively increased, perhaps driven by 3D gaming, cloud computing and cryptocurrency mining; third, there are now vast quantities of readily-available facial training data on social media and the web more generally – and, fourth, the deep learning revolution has yielded highly effective deep neural network architectures and associated training methods."

Suddenly, facial recognition began to be viewed as both a viable and useful technology, and was deemed robust enough for 'cooperative recognition' applications, where willing subjects posed for photos in controlled and well-lit environments, such as passport control gates in airports. However, its limitations in certain scenarios resulted in some high-profile failures that were both problematic for general market adoption and also damaging for the reputation of the technology.

"Under less constrained circumstances – lower fidelity images of people from different angles, taken from CCTV feeds and in less well-lit environments, for example – the technology was less successful," says Pears.

A particular challenge was achieving a consistent recognition performance across all population demographics. This is a crucial aspect of system development, both in terms of its ethical deployment and in terms of its public acceptability. The development of non-biased face recognition systems requires design considerations to be made over a number of components, including the raw image capture itself and the demographic balance of the training dataset.

Over time, systems have been developed that are broadly capable in a wide range of environmental and lighting conditions. This represents the current state-of-the-art methodology for facial recognition today.

So if face recognition is now robust and scalable enough for widespread adoption, how can it be used to benefit society? While there are a host of applications that are already in progress, from border checks and the boarding process at airports, to security processes for financial transactions and event registrations.

In the security field, facial recognition systems have historically been complex, bespoke installations focused on national security, policing and big transportation infrastructure, but this is changing. From a commercial security standpoint, systems are now available that bring the benefit of facial recognition to a much wider audience.

SAFETY BENEFITS HAVE TO BE WEIGHED UP AGAINST THE POTENTIAL VIOLATION OF PRIVACY IT MAY CAUSE

Today, a wide range of commercial environments, from retail outlets and hospitals to sports arenas and hotels, can use face recognition to enhance their security and receive alerts about individuals on a watchlist – suspected shoplifters, for example. Modern systems like these are optimised for ease-of-use by anyone from site managers to security staff, with all alerting and management features being delivered via a simple mobile app. In real-time, unwelcome visitors are detected by recognising faces that have been flagged previously, before alerting security or management via the app.

But such systems are not designed to be a replacement for existing security infrastructure and processes such as CCTV or guards. It is designed to augment security operations to run more effectively and efficiently. Over reliance on technology has the potential to lead to humans subconsciously deferring responsibility to a machine – which can cause problems. The right approach is for technology systems to assist humans who should be the final gatekeeper and never defer the ultimate responsibility of decision.

In any discussion around facial recognition, the ethical questions surrounding its use must also be taken into consideration. Potential safety benefits have to be weighed up against the potential violation of privacy that it may cause.

With regards to data protection considerations, Will Richmond-Coggan, nationally recognised data protection specialist at Freeths LLP, says: "The challenge with most forms of facial recognition technology is that they involve the processing of biometric data for the purposes of identification, which brings that processing into the realms of special category data processing, which is governed by data protection law such as the EU's General Data Protection Regulation. This imposes an additional range of criteria to be satisfied before the processing can be lawfully carried out, in addition to the standard range of lawful bases for processing (contract, legitimate interests, consent), which also have to be established."

Sometimes the facial recognition technology will be used to automate an identification process, such as access control to restricted areas, or to enable functionality in a vehicle or device.

DATA PROTECTION

"Where such processing amounts to automated decision-making this imposes additional challenges, including the risk that users will object and force an alternative process to be adopted," says Richmond-Coggan. "In any case, the processing is likely to be regarded as sufficiently high impact that both the developer of the technology and any controller looking to deploy it will be expected to have completed a formal data protection impact assessment, such as those identified in Article 35 of the GDPR."

The Coronavirus pandemic has changed the world dramatically, and face coverings are expected to be part of normal day-to-day life for a long time to come. Even when mandatory restrictions are lifted it is likely that mask-wearing will continue voluntarily for some time and even permanently for many. This is not a short-term issue; a long-term solution is critical.

Although we are in the early stages of a vaccine, the speed of implementation will see ongoing resistance to vaccines from some sectors and the continuation of mask wearing. It is difficult to imagine a post-COVID era where face coverings are not a significant part of normal life. In February of 2020, someone inside a high-street store with their face covered would have been noted as behaving suspiciously. Today, the reverse is true.

The requirement for citizens to wear face coverings in stores, commercial premises, in public sector buildings and on public transport, presents a unique set of challenges for facial recognition – a premise built entirely upon the ability to see a face. It also potentially presents criminal opportunity – for individuals to conceal their identity with a view to entering premises or carrying out acts without identification. This represents a potential threat to retailers, commercial organisations, transport hubs and beyond.

The Face Recognition Company has enhanced the capacity of its systems to process partial information – taking visible information and other data from partially obscured features to recognise individuals of interest whether they are masked or unmasked with virtually the same level of accuracy as the current unmasked model. This means that the effect of masking is negligible in system-response terms. The strength of this technology lies in the model training, utilising large and extreme datasets from real-world examples that facilitate machine-learning, giving high accuracy in real-world use.

One wonders what Woodrow Bledsoe might think, were he able to see the progress made since his first efforts to identify faces using a computer. Similarly, we might also consider what the next 50 years will hold. Not only the immediacy of partially obscured facial recognition, but also the ongoing societal changes that will see permanent behavioural changes in the population. Facial coverings will become more sophisticated, incorporating patterns and element designs which will seek to obfuscate recognition systems. It is vital that recognition technology remains ahead of potential future threats, seeking to anticipate and respond to such ahead of these threats becoming a reality ●

Tim Noest is the CEO of The Face Recognition Company, which is on a mission to harness the power of machine learning to provide solutions in digital safety and customer metric analytics for the physical environment.

Partially obscured features do not stop the technology from identifying individuals of interest

Picture credit: The Face Recognition Company