Facial Recognition – Technology Between Support and Suppression

By Sophie-Charlotte Opitz and Jana Honegger
05.06.2020

Why is a picture of a face scanned by a machine and what is this then used for? How safe is this technology in terms of data transfer and identity theft? Facial recognition is a procedure that can help in the solving and prevention of crime. It can verify the identity of people in order to give them access to sensitive data and secured areas. Yet it can also be used in forms of surveillance that restrict human freedom of movement and action. An overview of the opportunities presented by digital facial recognition and the dangers that go with it.

Mathematical grid for facial recognition. Image: imago, CC by 2.0

WHAT IS FACIAL RECOGNITION BASED ON?

The ability to identify individuals and verify their identity using facial recognition relies on biometric technology. This technology encompasses processes in which the human body is measured in order to obtain knowledge about it. Alongside the fingers and veins, which supply prints and scans[1], the face is the part of the body most commonly used for this. The biometrics of the face – the position of its various features and the distances between them – can be measured when a camera takes a picture of it. This means that we cannot always control when data is collected. It can be recorded without our knowledge or permission.

Why is facial recognition used, and why do some people think it is dangerous?

HOW DOES FACIAL RECOGNITION WORK?

Facial recognition is based on either 2D or 3D scanning. For 2D procedures ordinary photographs are used. There are two methods:

1. Geometrical features of the face (the position of the nose, eyes, mouth, etc.) are drawn from the picture and analysed. For this purpose, a machine-made artificial network modelled on an individual's physiognomy is overlaid on the photo. Stored as numbers, this data is converted into a set of vectors. Other pictures from the database can then be compared with the set and aligned with other similar data.[2]
2. Template matching is also used for facial recognition. This procedure attempts to calculate

the similarities between an image of a face and a template modelled on a face. To do this, the system draws on images from a database and compares these with the templates. A vector ascertains the similarities by, for example, counting the 'empty' squares between the nose, mouth and eyes.[3]

These methods have been in a process of ongoing development since the early 1990s. Today, 2D facial recognition is also based on complex calculations such as wavelet analysis[4] or the Viola-Jones method[5]. The 2D methods are thus based on mathematical calculations using algorithms.

The disadvantage of 2D methods is that they cannot account for unusual angles, shadows or partial masking in their calculations. At this point 3D methods of facial recognition are a viable alternative. They do not decode the image into distances and values of brightness or colour but rather use information on depth recorded by laser scanners. This generates a netlike structure that recreates the face in virtual form. There are three common methods for using this grid to identify faces:[6]

1. Curves: the curves of the face are (re)traced, and these provide information about its physiognomy.
2. Form description: the size and shape of small portions of the grid that are essentially constant – areas on the bridge of the nose, the chin and the forehead, for example – are used for comparison.
3. Relationships: as in 2D procedures, here the distances between single points in a face are measured. As this takes place in 3D, the measurements differ from those used for 2D photos and include factors like the distance from the tip to the wing of the nose.
These 3D methods are based on artificial intelligence and algorithms. The software independently detects features like the locations of shadow and symmetries, and it can use these to recognise a face. This increases the reliability of facial recognition. However, the complexity generates a considerable volume of data, which makes it more difficult to compare large numbers of images from big databases.

The functionality of facial recognition is continually improving because more people are generating images of themselves and others and making these public – on social media, for example. These images can then be fed into databases. The availability of data capacity needed for processing this information is also constantly on the rise. These two factors mean that more precise models of recognition can be developed.

One reason for the major improvements in the reliability of recognition is deep learning technology.[7] This is a method that enables machines to process information, and artificial intelligence to learn from it. To achieve this, very large amounts of data are analysed and fed into a neuronal network that creates connections between the data. These connections are constantly developing, just like the human brain, and new connections are generated from them. The machine can then not only make predictions and decisions but also question and change them as necessary. As a rule, human intelligence does not interfere with the learning processes in deep learning. Deep learning is used in facial recognition because this method analyses large amounts of data based on parameters and models.

Sometimes different methods are combined. Combinations with other sensors, such as motion detectors or audio recorders, can then be used as aids to facilitate or initiate facial recognition. Motion sensors can, for example, activate the video surveillance needed for facial recognition.

WHO COLLECTS OUR DATA?

Perhaps the best-known and most criticised example of image-based data being collected and stored is the US firm Clearview.[8] Their database is said to contain more than three billion photographs of human faces. To acquire this data, a program searches publicly accessible sites on the internet, such as Facebook, YouTube and Instagram.[9] The pictures found there are automatically downloaded and the faces are scanned for their biometric

characteristics. When data correlates, the program supplies more photos and personal data. Clearview has hitherto been seen as the largest database, but there are other comparable systems. In addition to police data on demonstrators in places like Russia[10] and Hong Kong,[11] there are companies that make use of facial recognition. Apple collects facial data so that people can enable Face ID, which acts like a key that you can use to unlock your smartphone. Google is also presently suspected of deliberately collecting image data and of using unconventional methods:[12] In New York, Google is said to have employed people to offer passers-by vouchers if they provided their facial data – they were then photographed from different angles.

WHO IS INTERESTED IN OUR DATA?
There are many different people and organisations interested in our data – companies, governments and public authorities as well as criminal networks and individual actors. By buying in data sets from address brokers, companies acquire information about our purchasing behaviour and can control this by consciously deploying targeted advertising. Facial recognition is not needed for this, nor is it necessary to buy the data – just paying for something by direct debit may be enough for your buying habits to be tracked.[13]

Public authorities also pay for facial data. Six hundred US authorities have allegedly accepted offers from Clearview to assist them in solving sex crimes.[14]

Criminal organisations and individuals can exploit facial recognition to discover and misuse the identities of people. Examples here are stalking, buying illegal goods (drugs, child pornography, etc.) and using false identities.[15]

WHAT ARE THE BENEFITS OF FACIAL RECOGNITION?
The police and government security and law enforcement agencies can use facial recognition in the fight against crimes like human trafficking and sex offences as a means to analyse video material and ascertain people's identities. This technology can also help to uncover identity thieves.[16]

Companies like Migrolino[17] and Valora[18] in Switzerland are experimenting with facial recognition to simplify payment when shopping or to check the age of customers when they wish to buy age-restricted products.

Internet sites like Pornhub use facial recognition software to identify and 'tag' performers in videos so that the videos can be indexed with their names as keywords.[19]

Facial recognition is also used to connect people – e.g. in photo albums on Facebook – and so to create new contacts

... AND THE DRAWBACKS?
The alleged benefits of facial recognition and the different ways in which it can simplify day-to-day processes also have a serious downside. Facial recognition is a risk to privacy and it affects our basic rights.

In some parts of the world, for example, facial recognition is used by police to identify demonstrators. In 2019 this was done during protests in Hong Kong.[20] The danger with this is that protestors then have to worry that their identities will be registered with the authorities and stored, and that they will face criminal prosecution as a result. This could then lead to a change in behaviour, with people no longer taking part in demonstrations. In the case of the protests in Hong Kong, demonstrators fought back by using laser pointers that disrupted the recognition system.[21] They also used the same technologies against the state's surveillance system, applying facial recognition to identify police officers and enabling legal action to be taken against the police if necessary. This data could be verified in part with the help of a private database. The authorities in Hong Kong reacted swiftly, implementing strict data protection controls to regulate the private use of facial recognition.[22]

This picture of the demonstration of 7 August 2019 with laser pointers used to disrupt facial recognition became a symbol of the Hong Kong pro-democracy protests.
Photo: Studio Incendo, CC by 2.0

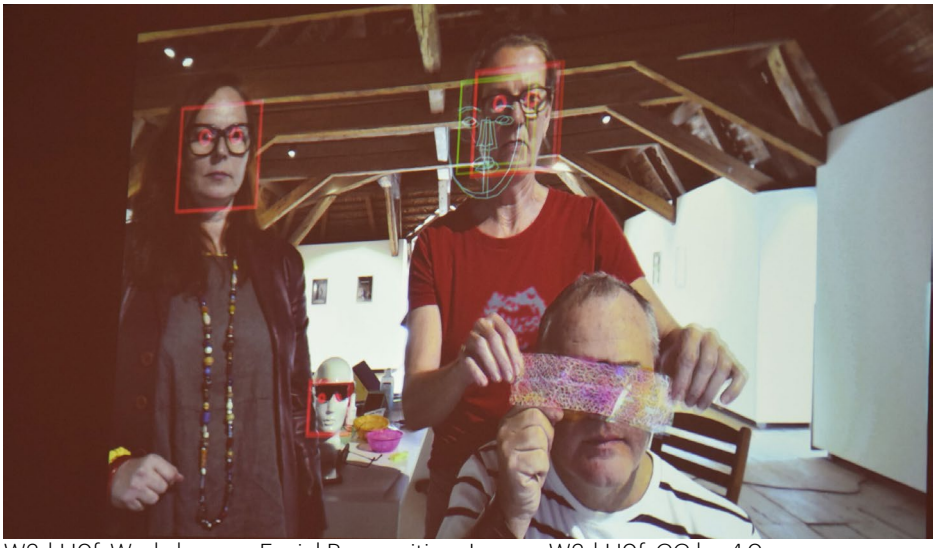
The example of the internet site Pornhub is also double-edged, as facial recognition software does not distinguish between professional performers and amateurs. This means that it can be used to ascertain the identities of people who would have not authorised the collecting of this information.[23]

Another politically controversial example, where basic rights and privacy might be violated, is the establishment of a social credit system in China, which was instituted in 2017.[24] Facial recognition systems equipped with cameras monitor people as they go about their everyday lives. Behaviour that the Chinese government deems 'positive' is rewarded by giving people points in an account, while 'negative' behaviour is sanctioned with a points deduction,[25] which can lead to a loss of social security benefits or to travel restrictions.[26] It is not only everyday behaviour in public spaces that is taken into account here but also purchasing power[27] and political attitudes,[28] among other things. The social credit system is currently in a test phase and is not used all over China.

The way the data used for facial recognition is sourced is also problematic. Clearview, for example, downloads its data from platforms like Facebook and Instagram, although this contravenes the conditions of use on these social media platforms.[29] Public authorities also put sensitive data, such as the identities of suspected criminals, into the hands of providers. No absolute reassurances can be given that this data is safe from hacking attacks and data theft.

Many of the technologies are based on standardised faces and have an algorithmic bias that corresponds with existing forms of discrimination and influences the data sets. The norms that are established by this hinder the recognition of the faces of Blacks and People of Colour, women, the elderly, trans people, and people with disabilities. As a result, a large section of society is prevented from fully benefiting from the positive aspects of the technologies.[30]

For these reasons, in a public workshop in 2019, the Swiss non-profit association *W3rkH0f* attempted to outwit facial recognition.[31] They installed two of the programs most commonly used for facial recognition – OpenCV and Vision Framework (Apple facial recognition). Participants were asked to trick these by using make-up, glasses and items of clothing. One finding was that simply wearing a pair of sunglasses is not sufficient to circumvent the recognition process.


W3rkH0f, Workshop on Facial Recognition. Image: W3rkH0f, CC by 4.0

Ultimately, it is almost impossible to regulate facial recognition in public and digital space. All the faces that are registered are scanned at the same time. Whether there is a good reason for this or not is irrelevant.

WHAT OTHER CONSIDERATIONS ARE THERE?
The debates on facial recognition are heated, and different views come up against each other. Where some people see the benefits for stronger internal security or easier authentication for various services, others protest against the violations of privacy and basic rights that the technology can entail.[32] The right to anonymity in public space could be infringed to the extent that people end up simply conforming with what the state demands. Absolute, repressive surveillance seems to be close at hand in this scenario.

In these debates, two different uses of facial recognition are often confused: the verification of faces and their identification. Facial recognition is used for verification in order to confirm someone's identity. However, the technology is also used for identification purposes to ascertain someone's identity. The latter is open to abuse, as biometric data is linked to individuals. Whereas this data may not legally be processed in the EU,[33] in Switzerland things are somewhat different, as data processing is in principle permissible.[34] It only requires special justification if the basic principles governing its processing are violated – these include, for example, the obligation to inform people that their facial data is being stored. At present an EU commission is considering whether the technology of artificial intelligence violates basic rights (e.g. the right to privacy).[35] The first White Paper on this is now ready and is being discussed in the European Parliament.[36]

Even if the technology of facial recognition is not yet perfect and there are collisions with basic rights, privacy and other legal provisions, this issue must be discussed on all levels (political, social and legal). One of the most important principles that must be stipulated when states, organisations and companies implement facial recognition is transparency on all the procedures used. Which faces are recorded? Can I object to facial recognition? Where, for how long, and in what ways is data stored? Who uses this data? What is the data used for?

As these questions are often not answered transparently, it is all the more necessary to critically challenge facial recognition.

References
(accessed 25 May 2020)

[1] Li Xueyan und Guo Shuxu, The Fourth Biometric – Vein Recognition, 2008.
[2] Simon Hurtz, Warum automatisierte Gesichtserkennung so gefährlich ist, 2020.
[3] Carsten Wächter und Stefan Römer, Gesichts-Erkennung I, 2001. (last accessed 25.05.2020)

[4] Clemens Valens, A really friendly guide to wavelets, 2010.
[5] Anmol Parande, Understanding and Implementing the Viola-Jones Image Classification Algorithm, 2019.
[6] Benjamin Kees, Gesichtserkennung, 2012.
[7] Nico Litzel und Stefan Luber, Was ist Deep Learning?, 2017.
[8] WELT-Redaktion/dpa, US-Firma sammelt drei Milliarden Bilder von Menschen aus dem Internet, 2020.
[9] Jannis Brühl und Simon Hurtz, Eine Software schockiert Amerika, 2020.
[10] Julian Hans, Wie Russland Demonstranten identifiziert, 2017.
[11] Manuel Escher, Gesichtserkennung gegen Polizei, Demos am Airport: Kreative Proteste in Hongkong, 2019.
[12] Chris Matyszczyk, Google bought my friend's face for $5, 2019.
[13] Maike Brzoska und Clemens Schömann-Finck, 50 Cent für eine Adresse, 2010.
[14] Jannis Brühl und Simon Hurtz, Eine Software schockiert Amerika, 2020.
[15] Simon Hurtz, Warum automatisierte Gesichtserkennung so gefährlich ist, 2020.
[16] Holger Suhl, Wie Gesichtserkennung unser Leben verändert, 2016.
[17] Michael Bolzli, Gesichtserkennung für den Alkohol-Verkauf, 2019.
[18] Benjamin Weinmann, Ist das die Zukunft des Shoppings? Valora will die Gesichter der Kunden scannen, 2019.
[19] SZ-Redaktion, Pornhub identifiziert Darstellerinnen mit Gesichtserkennung, 2017.
[20] Manuel Escher, Gesichtserkennung gegen Polizei, Demos am Airport: Kreative Proteste in Hongkong, 2019.
[21] Florian Rötzer, Hongkong: Demonstranten versuchen Überwachung auszuschalten, 2019.
[22] Paul Mozur In Hong Kong Protests, Faces Become Weapons, 2019.
[23] SZ-Redaktion, Pornhub identifiziert Darstellerinnen mit Gesichtserkennung, 2017.
[24] Toni Prug, "The" Social Credit System – Why It's Both Better and Worse Than We can Imagine, 2018.
[25] Louise Matsakis, How the West Got China's Social Credit System Wrong, 2019.
[26] Chris Baynes, China blocks 17.5 million plane tickets for people without enough 'social credit', 2019.
[27] Anna L. Ahlers, Kommunalpolitik in China – Warum wir chinesische Politik erst verstehen, wenn wir auch die lokale Ebene in den Blick nehmen, 2014.
[28] Andreas Sträter, Wie China seine Bürgerinnen und Bürger mit einem Punktesystem kontrollieren will, 2020.
[29] Simon Hurtz, Warum automatisierte Gesichtserkennung so gefährlich ist, 2020.
[30] Cade Metz und Natasha Singer, Many Facial-Recognition Systems Are Biased, Says U.S. Study, 2019.
[31] W3rkH0f, Gesichtserkennung, 2019.
[32] Holger Suhl, Wie Gesichtserkennung unser Leben verändert, 2016.
[33] BDSG (neu), 2018.
[34] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Datenschutz. (last accessed 25.05.2020)
[35] Alexander Fanta, EU erwägt Verbot von Gesichtserkennung, 2020.
[36] Europäische Kommission, Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, 2020. (last accessed 25.05.2020)