Can Big Brother identify your face from street-level CCTV surveillance and tell whether you’re happy, sad, or angry? Can that identification lead to your arrest on an outstanding warrant? What are the odds that the identification is incorrect, and really connects to someone else? Can you defeat the surveillance entirely using some trick?

On the flip side, can you get into a vault protected by a camera and facial identification software by holding up a print of an authorized person’s face? What if you put on a 3-D mask of an authorized person’s face?

Welcome to face recognition — and the spoofing of facial recognition.

**What is face recognition?**

Face recognition is a method for identifying an unknown person or authenticating the identity of a specific person from their face. It’s a branch of [computer vision](https://www.infoworld.com/article/3572553/what-is-computer-vision-ai-for-images-and-video.html), but face recognition is specialized and comes with social baggage for some applications, as well as some vulnerabilities to spoofing.

**How does face recognition work?**

The early facial recognition algorithms (which are still in use today in improved and more automated form) rely on biometrics (such as the distance between eyes) to turn the measured facial features from a two-dimensional image into a set of numbers (a feature vector or template) that describes the face. The recognition process then compares these vectors to a database of known faces which have been mapped to features in the same way. One complication in this process is adjusting the faces to a normalized view to account for head rotation and tilt before extracting the metrics. This class of algorithms is called *geometric*.

Another approach to face recognition is to normalize and compress 2-D facial images, and to compare these with a database of similarly normalized and compressed images. This class of algorithms is called *photometric*.

Three-dimensional face recognition uses 3-D sensors to capture the facial image, or reconstructs the 3-D image from three 2-D tracking cameras pointed at different angles. 3-D face recognition can be considerably more accurate than 2-D recognition.

Skin texture analysis maps the lines, patterns, and spots on a person’s face to another feature vector. Adding skin texture analysis to 2-D or 3-D face recognition can improve the recognition accuracy by 20 to 25 percent, especially in the cases of look-alikes and twins. You can also combine all the methods, and add in multi-spectral images (visible light and infrared), for even more accuracy.

Face recognition has been improving year over year since the field began in 1964. On average, the error rate has reduced by half every two years.

## Face recognition vendor tests

NIST, the US National Institute of Standards and Technology, has been performing tests of facial recognition algorithms, the [Face Recognition Vendor Test (FRVT)](https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf), since 2000. The image datasets used are mostly law enforcement mug shots, but also include in-the-wild still images, such as those found in [Wikimedia](https://commons.wikimedia.org/wiki/File:Sandra_Bullock_(9192364254).jpg), and low-resolution images from webcams.

The FRVT algorithms are mostly submitted by commercial vendors. The year-over-year comparisons show major gains in performance and accuracy; according to the vendors, this is primarily because of the use of [deep convolutional neural networks](https://www.infoworld.com/article/3397142/what-is-deep-learning-algorithms-that-mimic-the-human-brain.html).

Related NIST face recognition testing programs have studied demographic effects, detection of face morphing, identification of faces posted on social media, and identification of faces in video. A previous series of tests was conducted in the 1990s under a different moniker, Face Recognition Technology (FERET).

## Face recognition applications

Face recognition applications mostly fall into three major categories: security, health, and marketing/retail. Security includes law enforcement, and that class of facial recognition uses can be as benign as matching people to their passport photos faster and more accurately than humans can, and as creepy as the “[Person of Interest](https://en.wikipedia.org/wiki/Person_of_Interest_(TV_series))” scenario where people are tracked via CCTV and compared to collated photo databases. Non-law-enforcement security includes common applications such as face unlock for mobile phones and access control for laboratories and vaults.

Health applications of facial recognition include patient check-ins, real-time emotion detection, patient tracking within a facility, assessing pain levels in non-verbal patients, detecting certain diseases and conditions, staff identification, and facility security. Marketing and retail applications of face recognition include identification of loyalty program members, identification and tracking of known shoplifters, and recognizing people and their emotions for targeted product suggestions.

## Face recognition controversies, biases, and bans

To say that some of these applications are controversial would be an understatement. As a [2019 New York Times article](https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html) discusses, facial recognition has swirled in controversy, from its use for stadium surveillance to racist software.

Stadium surveillance? Face recognition was used at the 2001 Super Bowl: the software identified 19 people thought to be subjects of outstanding warrants, though none were arrested (not for lack of trying).

Racist software? There have been several issues, starting with the 2009 face tracking software that could track whites but not Blacks, and continuing with the 2015 MIT study that showed that the facial recognition software of the time worked much better on white male faces than female and/or Black faces.

These sorts of issues have led to outright bans of facial recognition software in specific places or for specific uses. In 2019, San Francisco became the first major American city to block police and other law enforcement agencies from using face recognition software; Microsoft called for federal regulations on facial recognition; and MIT showed that Amazon Rekognition had more trouble determining female gender than male gender from face images, as well as more trouble with Black female gender than white female gender.

In June 2020, Microsoft announced that it will not sell and has not sold its face recognition software to the police; Amazon banned police from using Rekognition for a year; and IBM abandoned its facial recognition technology. [Banning face recognition entirely will not be easy](https://www.vox.com/recode/2020/7/3/21307873/facial-recognition-ban-law-enforcement-apple-google-facebook), however, given its wide adoption in iPhones (Face ID) and other devices, software, and technologies.

Not all face recognition software suffers from the same biases. The [2019 NIST demographic effects study](https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects) followed up on the MIT work and showed that algorithmic demographic bias varies widely among developers of face recognition software. Yes, there are demographic effects on the false match rate and false non-match rate of facial identification algorithms, but they can vary by several orders of magnitude from vendor to vendor, and they have been decreasing over time.

## Hacking face recognition, and anti-spoofing techniques

Given the potential privacy threat from face recognition, and the attraction of getting access to high-value resources protected by face authentication, there have been many efforts to hack or spoof the technology. You can present a printed image of a face instead of a live face, or an image on a screen, or a 3-D printed mask, to pass authentication. For CCTV surveillance, you can play back a video. To avoid surveillance, you can try the “CV Dazzle” fabrics and make-up, and/or IR light emitters, to fool the software into not detecting your face.

Of course, there are efforts to develop anti-spoofing techniques for all these attacks. To detect printed images, vendors use a liveness test, such as waiting for the subject to blink, or perform motion analysis, or use infrared to distinguish a live face from a printed image. Another approach is to perform micro-texture analysis, since human skin is optically different from prints and mask materials. The latest anti-spoofing techniques are mostly based on deep convolutional neural networks.

This is an evolving field. There’s an arms war going on between attackers and anti-spoofing software, as well as academic research on the effectiveness of different attack and defense techniques.

## Face recognition vendors

[According to the Electronic Frontier Foundation](https://www.eff.org/pages/face-recognition), MorphoTrust, a subsidiary of [Idemia](https://www.morpho.com/en/media/ot-morpho-becomes-idemia-global-leader-trusted-identities-20170928) (formerly known as OT-Morpho or Safran), is one of the largest vendors of face recognition and other biometric identification technology in the United States. It has designed systems for state DMVs, federal and state law enforcement agencies, border control and airports (including TSA PreCheck), and the state department. Other common vendors include [3M](https://solutions.3m.com/wps/portal/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOJDDQx8LZwMHQ38fQPNDBwtHE0sAhwNDAPdTPWDU_PiQ4P1C7IdFQHlleBy/), [Cognitec](http://www.cognitec.com/applications-law-enforcement.html), [DataWorks Plus](http://www.dataworksplus.com/faceplus.html), [Dynamic Imaging Systems](http://www.dynamicimaging.com/solutions/facial-recognition/), [FaceFirst](https://www.facefirst.com/), and [NEC Global](http://www.nec.com/en/global/solutions/safety/Technology/index.html).

The [NIST Face Recognition Vendor Test](https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf) lists algorithms from many more vendors from all over the world. There are also several open source face recognition algorithms, of varying quality, and a few major cloud services that offer face recognition.

[Amazon Rekognition](https://aws.amazon.com/rekognition/) is an image and video analysis service that can identify objects, people, text, scenes, and activities, including facial analysis and custom labels. The [Google Cloud Vision API](https://cloud.google.com/vision) is a pretrained image analysis service that can detect objects and faces, read printed and handwritten text, and build metadata into your image catalog. Google AutoML Vision allows you to train custom image models.

The [Azure Face API](https://azure.microsoft.com/en-us/services/cognitive-services/face/) does face detection that perceives faces and attributes in an image, performs person identification that matches an individual in your private repository of up to 1 million people, and performs perceived emotion recognition. The Face API can run in the cloud or on the edge in containers.

## Face datasets for recognition training

There are [dozens of face datasets](https://www.face-rec.org/databases/) available for downloading that can be used for recognition training. Not all face datasets are equal: They tend to vary in image size, number of people represented, number of images per person, conditions of images, and lighting. Law enforcement also has access to non-public face datasets, such as current mugshots and driver’s license images.

Some of the larger face databases are [Labeled Faces in the Wild](http://vis-www.cs.umass.edu/lfw/), with ~13K unique people; [FERET](http://www.nist.gov/itl/iad/ig/colorferet.cfm), used for the early NIST tests; the [Mugshot](http://www.nist.gov/ts/msd/srd/nistsd18.cfm) database used in the ongoing NIST FRVT; the [SCFace](http://www.scface.org/) surveillance camera database, also available [with facial landmarks](http://atvs.ii.uam.es/atvs/scfacedb_landmarks.html); and [Labeled Wikipedia Faces](http://www.info.polymtl.ca/~mdhas/LWF/), with ~1.5K unique identities. Several of these databases contain multiple images per identity. [This list](http://web.mit.edu/emeyers/www/face_databases.html) from researcher Ethan Meyers offers some cogent advice on picking a face dataset for a specific purpose.

In summary, facial recognition is improving, and vendors are learning to detect most spoofing, but some applications of the technology are controversial. The error rate for face recognition is halving every two years, according to NIST. Vendors have improved their anti-spoofing techniques by incorporating convolutional neural networks.

Meanwhile, there are initiatives to ban the use of face recognition in surveillance, especially by police. Banning face recognition entirely would be difficult, however, given how widespread it has become.