Title: Facial recognition system

URL: https://en.wikipedia.org/wiki/Facial_recognition_system

PageID: 602401

Categories: Category:Automatic identification and data capture, Category:Facial recognition, Category:Machine learning task, Category:Surveillance, Category:Video surveillance

-----

A facial recognition system [1] is a technology potentially capable of matching a human face from a digital image or a video frame against a database of faces. Such a system is typically employed to authenticate users through ID verification services , and works by pinpointing and measuring facial features from a given image. [2]

Development began on similar systems in the 1960s, beginning as a form of computer application . Since their inception, facial recognition systems have seen wider uses in recent times on smartphones and in other forms of technology, such as robotics . Because computerized facial recognition involves the measurement of a human's physiological characteristics, facial recognition systems are categorized as biometrics . Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition , fingerprint image acquisition , palm recognition or voice recognition , it is widely adopted due to its contactless process. [3] Facial recognition systems have been deployed in advanced human–computer interaction , video surveillance , law enforcement , passenger screening, decisions on employment and housing and automatic indexing of images. [4] [5]

Facial recognition systems are employed throughout the world today by governments and private companies. [6] Their effectiveness varies, and some systems have previously been scrapped because of their ineffectiveness. The use of facial recognition systems has also raised controversy, with claims that the systems violate citizens' privacy, commonly make incorrect identifications, encourage gender norms [7] [8] and racial profiling , [9] and do not protect important biometric data. The appearance of synthetic media such as deepfakes has also raised concerns about its security. [10] These claims have led to the ban of facial recognition systems in several cities in the United States . [11] Growing societal concerns led social networking company Meta Platforms to shut down its Facebook facial recognition system in 2021, deleting the face scan data of more than one billion users. [12] [13] The change represented one of the largest shifts in facial recognition usage in the technology's history. IBM also stopped offering facial recognition technology due to similar concerns. [14]

History of facial recognition technology

Automated facial recognition was pioneered in the 1960s by Woody Bledsoe , Helen Chan Wolf , and Charles Bisson, whose work focused on teaching computers to recognize human faces. [15] Their early facial recognition project was dubbed "man-machine" because a human first needed to establish the coordinates of facial features in a photograph before they could be used by a computer for recognition. Using a graphics tablet , a human would pinpoint facial features coordinates, such as the pupil centers, the inside and outside corners of eyes, and the widows peak in the hairline. The coordinates were used to calculate 20 individual distances, including the width of the mouth and of the eyes. A human could process about 40 pictures an hour, building a database of these computed distances. A computer would then automatically compare the distances for each photograph, calculate the difference between the distances, and return the closed records as a possible match. [15]

In 1970, Takeo Kanade publicly demonstrated a face-matching system that located anatomical features such as the chin and calculated the distance ratio between facial features without human intervention. Later tests revealed that the system could not always reliably identify facial features. Nonetheless, interest in the subject grew and in 1977 Kanade published the first detailed book on facial recognition technology. [16]

In 1993, the Defense Advanced Research Project Agency (DARPA) and the Army Research Laboratory (ARL) established the face recognition technology program FERET to develop "automatic face recognition capabilities" that could be employed in a productive real life environment "to assist security, intelligence, and law enforcement personnel in the performance of their duties." Face recognition systems that had been trialled in research labs were evaluated. The FERET tests found that while the performance of existing automated facial recognition systems varied, a handful of existing methods could viably be used to recognize faces in still images taken in a controlled environment. [17] The FERET tests spawned three US companies that sold automated facial recognition systems. Vision Corporation and Miros Inc were founded in 1994, by researchers who used the results of the FERET tests as a selling point. Viisage Technology was established by an identification card defense contractor in 1996 to commercially exploit the rights to the facial recognition algorithm developed by Alex Pentland at MIT . [18]

Following the 1993 FERET face-recognition vendor test, the Department of Motor Vehicles (DMV) offices in West Virginia and New Mexico became the first DMV offices to use automated facial recognition systems to prevent people from obtaining multiple driving licenses using different names. Driver's licenses in the United States were at that point a commonly accepted form of photo identification . DMV offices across the United States were undergoing a technological upgrade and were in the process of establishing databases of digital ID photographs. This enabled DMV offices to deploy the facial recognition systems on the market to search photographs for new driving licenses against the existing DMV database. [19] DMV offices became one of the first major markets for automated facial recognition technology and introduced US citizens to facial recognition as a standard method of identification. [20] The increase of the US prison population in the 1990s prompted U.S. states to established connected and automated identification systems that incorporated digital biometric databases, in some instances this included facial recognition. In 1999, Minnesota incorporated the facial recognition system FaceIT by Visionics into a mug shot booking system that allowed police, judges and court officers to track criminals across the state. [21]

Until the 1990s, facial recognition systems were developed primarily by using photographic portraits of human faces. Research on face recognition to reliably locate a face in an image that contains other objects gained traction in the early 1990s with the principal component analysis (PCA). The PCA method of face detection is also known as Eigenface and was developed by Matthew Turk and Alex Pentland. [22] Turk and Pentland combined the conceptual approach of the Karhunen–Loève theorem and factor analysis , to develop a linear model . Eigenfaces are determined based on global and orthogonal features in human faces. A human face is calculated as a weighted combination of a number of Eigenfaces. Because few Eigenfaces were used to encode human faces of a given population, Turk and Pentland's PCA face detection method greatly reduced the amount of data that had to be processed to detect a face. Pentland in 1994 defined Eigenface features, including eigen eyes, eigen mouths and eigen noses, to advance the use of PCA in facial recognition. In 1997, the PCA Eigenface method of face recognition [23] was improved upon using linear discriminant analysis (LDA) to produce Fisherfaces . [24] LDA Fisherfaces became dominantly used in PCA feature based face recognition. While Eigenfaces were also used for face reconstruction. In these approaches no global structure of the face is calculated which links the facial features or parts. [25]

Purely feature based approaches to facial recognition were overtaken in the late 1990s by the Bochum system, which used Gabor filter to record the face features and computed a grid of the face structure to link the features. [26] Christoph von der Malsburg and his research team at the University of Bochum developed Elastic Bunch Graph Matching in the mid-1990s to extract a face out of an image using skin segmentation. [22] By 1997, the face detection method developed by Malsburg outperformed most other facial detection systems on the market. The so-called "Bochum system" of face detection was sold commercially on the market as ZN-Face to operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hairstyles and glasses—even sunglasses". [27]

Real-time face detection in video footage became possible in 2001 with the Viola–Jones object detection framework for faces. [28] Paul Viola and Michael Jones combined their face detection method with the Haar-like feature approach to object recognition in digital images to launch

AdaBoost , the first real-time frontal-view face detector. [29] By 2015, the Viola–Jones algorithm had been implemented using small low power detectors on handheld devices and embedded systems . Therefore, the Viola–Jones algorithm has not only broadened the practical application of face recognition systems but has also been used to support new features in user interfaces and teleconferencing . [30]

Ukraine is using the US-based Clearview AI facial recognition software to identify dead Russian soldiers. Ukraine has conducted 8,600 searches and identified the families of 582 deceased Russian soldiers. The IT volunteer section of the Ukrainian army using the software is subsequently contacting the families of the deceased soldiers to raise awareness of Russian activities in Ukraine. The main goal is to destabilise the Russian government. It can be seen as a form of psychological warfare . About 340 Ukrainian government officials in five government ministries are using the technology. It is used to catch spies that might try to enter Ukraine. [31]

Clearview AI's facial recognition database is only available to government agencies who may only use the technology to assist in the course of law enforcement investigations or in connection with national security. [32]

The software was donated to Ukraine by Clearview AI. Russia is thought to be using it to find anti-war activists. Clearview AI was originally designed for US law enforcement. Using it in war raises new ethical concerns. One London based surveillance expert, Stephen Hare, is concerned it might make the Ukrainians appear inhuman: "Is it actually working? Or is it making [Russians] say: 'Look at these lawless, cruel Ukrainians, doing this to our boys'?" [33]

Techniques for face recognition

While humans can recognize faces without much effort, [34] facial recognition is a challenging pattern recognition problem in computing . Facial recognition systems attempt to identify a human face, which is three-dimensional and changes in appearance with lighting and facial expression, based on its two-dimensional image. To accomplish this computational task, facial recognition systems perform four steps. First face detection is used to segment the face from the image background. In the second step the segmented face image is aligned to account for face pose , image size and photographic properties, such as illumination and grayscale . The purpose of the alignment process is to enable the accurate localization of facial features in the third step, the facial feature extraction. Features such as eyes, nose and mouth are pinpointed and measured in the image to represent the face. The so established feature vector of the face is then, in the fourth step, matched against a database of faces. [35]

Traditional

Some face recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. [36] These features are then used to search for other images with matching features. [37]

Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. [38] One of the earliest successful systems [39] is based on template matching techniques [40] applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches: geometric, which looks at distinguishing features, or photo-metric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances. Some classify these algorithms into two broad categories: holistic and feature-based models. The former attempts to recognize the face in its entirety while the feature-based subdivide into components such as according to features and analyze each as well as its spatial location with respect to other features. [41]

Popular recognition algorithms include principal component analysis using eigenfaces , linear discriminant analysis , elastic bunch graph matching using the Fisherface algorithm, the hidden Markov model , the multilinear subspace learning using tensor representation, and the neuronal motivated dynamic link matching . [citation needed] [42] Modern facial recognition systems make increasing use of machine learning techniques such as deep learning . [43]

Human identification at a distance (HID)

To enable human identification at a distance (HID) low-resolution images of faces are enhanced using face hallucination . In CCTV imagery faces are often very small. But because facial recognition algorithms that identify and plot facial features require high resolution images, resolution enhancement techniques have been developed to enable facial recognition systems to work with imagery that has been captured in environments with a high signal-to-noise ratio . Face hallucination algorithms that are applied to images prior to those images being submitted to the facial recognition system use example-based machine learning with pixel substitution or nearest neighbour distribution indexes that may also incorporate demographic and age related facial characteristics. Use of face hallucination techniques improves the performance of high resolution facial recognition algorithms and may be used to overcome the inherent limitations of super-resolution algorithms. Face hallucination techniques are also used to pre-treat imagery where faces are disguised. Here the disguise, such as sunglasses, is removed and the face hallucination algorithm is applied to the image. Such face hallucination algorithms need to be trained on similar face images with and without disguise. To fill in the area uncovered by removing the disguise, face hallucination algorithms need to correctly map the entire state of the face, which may be not possible due to the momentary facial expression captured in the low resolution image. [44]

3-dimensional recognition

Three-dimensional face recognition technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. [45] One advantage of 3D face recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. [45] [37] Three-dimensional data points from a face vastly improve the precision of face recognition. 3D-dimensional face recognition research is enabled by the development of sophisticated sensors that project structured light onto the face. [46] 3D matching technique are sensitive to expressions, therefore researchers at Technion applied tools from metric geometry to treat expressions as isometries . [47] A new method of capturing 3D images of faces uses three tracking cameras that point at different angles; one camera will be pointing at the front of the subject, second one to the side, and third one at an angle. All these cameras will work together so it can track a subject's face in real-time and be able to face detect and recognize. [48]

Thermal cameras

A different form of taking input data for face recognition is by using thermal cameras , by this procedure the cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or makeup. [49] Unlike conventional cameras, thermal cameras can capture facial imagery even in low-light and nighttime conditions without using a flash and exposing the position of the camera. [50] However, the databases for face recognition are limited. Efforts to build databases of thermal face images date back to 2004. [49] By 2016, several databases existed, including the IIITD-PSE and the Notre Dame thermal face database. [51] Current thermal face recognition systems are not able to reliably detect a face in a thermal image that has been taken of an outdoor environment. [52]

In 2018, researchers from the U.S. Army Research Laboratory (ARL) developed a technique that would allow them to match facial imagery obtained using a thermal camera with those in databases that were captured using a conventional camera. [53] Known as a cross-spectrum synthesis method due to how it bridges facial recognition from two different imaging modalities, this method synthesize a single image by analyzing multiple facial regions and details. [54] It consists of a non-linear regression model that maps a specific thermal image into a corresponding visible facial image and an optimization issue that projects the latent projection back into the image space. [50] ARL scientists have noted that the approach works by combining global information (i.e. features across the entire face) with local information (i.e. features regarding the eyes, nose, and mouth). [55] According to performance tests conducted at ARL, the multi-region cross-spectrum synthesis model demonstrated a performance improvement of about 30% over baseline methods and about 5% over state-of-the-art methods. [54]

Application

Social media

Founded in 2013, Looksery went on to raise money for its face modification app on Kickstarter. After successful crowdfunding, Looksery launched in October 2014. The application allows video chat with others through a special filter for faces that modifies the look of users. Image augmenting applications already on the market, such as Facetune and Perfect365, were limited to static images, whereas Looksery allowed augmented reality to live videos. In late 2015 SnapChat purchased Looksery, which would then become its landmark lenses function. [56] Snapchat filter applications use face detection technology and on the basis of the facial features identified in an image a 3D mesh mask is layered over the face. [57] A variety of technologies attempt to fool facial recognition software by the use of anti-facial recognition masks . [58]

DeepFace is a deep learning facial recognition system created by a research group at Facebook . It identifies human faces in digital images. It employs a nine-layer neural net with over 120 million connection weights, and was trained on four million images uploaded by Facebook users. [59] [60] The system is said to be 97% accurate, compared to 85% for the FBI's Next Generation Identification system. [61]

TikTok 's algorithm has been regarded as especially effective, but many were left to wonder at the exact programming that caused the app to be so effective in guessing the user's desired content. [62] In June 2020, TikTok released a statement regarding the "For You" page, and how they recommended videos to users, which did not include facial recognition. [63] In February 2021, however, TikTok agreed to a $92 million settlement to a US lawsuit which alleged that the app had used facial recognition in both user videos and its algorithm to identify age, gender and ethnicity. [64]

ID verification

The emerging use of facial recognition is in the use of ID verification services . Many companies and others are working in the market now to provide these services to banks, ICOs, and other e-businesses. [65] Face recognition has been leveraged as a form of biometric authentication for various computing platforms and devices; [37] Android 4.0 "Ice Cream Sandwich" added facial recognition using a smartphone 's front camera as a means of unlocking devices, [66] [67] while Microsoft introduced face recognition login to its Xbox 360 video game console through its Kinect accessory, [68] as well as Windows 10 via its "Windows Hello" platform (which requires an infrared-illuminated camera). [69] In 2017, Apple's iPhone X smartphone introduced facial recognition to the product line with its " Face ID " platform, which uses an infrared illumination system. [70]

Face ID

Apple introduced Face ID on the flagship iPhone X as a biometric authentication successor to the Touch ID , a fingerprint based system. Face ID has a facial recognition sensor that consists of two parts: a "Romeo" module that projects more than 30,000 infrared dots onto the user's face, and a "Juliet" module that reads the pattern. [71] The pattern is sent to a local "Secure Enclave" in the device's central processing unit (CPU) to confirm a match with the phone owner's face. [72]

The facial pattern is not accessible by Apple. The system will not work with eyes closed, in an effort to prevent unauthorized access. [72] The technology learns from changes in a user's appearance, and therefore works with hats, scarves, glasses, and many sunglasses, beard and makeup. [73] It also works in the dark. This is done by using a "Flood Illuminator", which is a dedicated infrared flash that throws out invisible infrared light onto the user's face to get a 2d picture in addition to the 30,000 facial points. [74]

Healthcare

Facial recognition algorithms can help in diagnosing some diseases using specific features on the nose, cheeks and other part of the human face . [75] Relying on developed data sets, machine learning has been used to identify genetic abnormalities just based on facial dimensions. [76] FRT has also been used to verify patients before surgery procedures.

In March, 2022 according to a publication by Forbes, FDNA, an AI development company claimed that in the space of 10 years, they have worked with geneticists to develop a database of about 5,000 diseases and 1500 of them can be detected with facial recognition algorithms. [77]

Deployment of FRT for availing government services

India

In an interview, the National Health Authority chief Dr. R.S. Sharma said that facial recognition technology would be used in conjunction with Aadhaar to authenticate the identity of people seeking vaccines. [78] Ten human rights and digital rights organizations and more than 150 individuals signed a statement by the Internet Freedom Foundation that raised alarm against the deployment of facial recognition technology in the central government's vaccination drive process. [79] Implementation of an error-prone system without adequate legislation containing mandatory safeguards, would deprive citizens of essential services and linking this untested technology to the vaccination roll-out in India will only exclude persons from the vaccine delivery system. [80]

In July, 2021, a press release by the Government of Meghalaya stated that facial recognition technology (FRT) would be used to verify the identity of pensioners to issue a Digital Life Certificate using "Pensioner's Life Certification Verification" mobile application. [81] The notice, according to the press release, purports to offer pensioners "a secure, easy and hassle-free interface for verifying their liveness to the Pension Disbursing Authorities from the comfort of their homes using smart phones". Mr. Jade Jeremiah Lyngdoh, a law student, sent a legal notice to the relevant authorities highlighting that "The application has been rolled out without any anchoring legislation which governs the processing of personal data and thus, lacks lawfulness and the Government is not empowered to process data." [82]

Deployment in security services

Commonwealth

The Australian Border Force and New Zealand Customs Service have set up an automated border processing system called SmartGate that uses face recognition, which compares the face of the traveller with the data in the e-passport microchip. [83] [84] All Canadian international airports use facial recognition as part of the Primary Inspection Kiosk program that compares a traveler face to their photo stored on the ePassport . This program first came to Vancouver International Airport in early 2017 and was rolled up to all remaining international airports in 2018–2019. [85]

Police forces in the United Kingdom have been trialing live facial recognition technology at public events since 2015. [86] In May 2017, a man was arrested using an automatic facial recognition (AFR) system mounted on a van operated by the South Wales Police. Ars Technica reported that "this appears to be the first time [AFR] has led to an arrest". [87] However, a 2018 report by Big Brother Watch found that these systems were up to 98% inaccurate. [86] The report also revealed that two UK police forces, South Wales Police and the Metropolitan Police , were using live facial recognition at public events and in public spaces. [88] In September 2019, South Wales Police use of facial recognition was ruled lawful. [88] Live facial recognition has been trialled since 2016 in the streets of London and will be used on a regular basis from Metropolitan Police from beginning of 2020. [89] In August 2020 the Court of Appeal ruled that the way the facial recognition system had been used by the South Wales Police in 2017 and 2018 violated human rights. [90]

However, by 2024 the Metropolitan Police were using the technique with a database of 16,000 suspects, leading to over 360 arrests, including rapists and someone wanted for grievous bodily harm for 8 years. They claim a false positive rate of only 1 in 6,000. The photos of those not identified by the system are deleted immediately. [91]

United States

The U.S. Department of State operates one of the largest face recognition systems in the world with a database of 117 million American adults, with photos typically drawn from driver's license photos. [92] Although it is still far from completion, it is being put to use in certain cities to give clues as to who was in the photo. The FBI uses the photos as an investigative tool, not for positive identification. [93] As of 2016, [update] facial recognition was being used to identify people in photos taken by police in San Diego and Los Angeles (not on real-time video, and only against booking photos) [94] and use was planned in West Virginia and Dallas . [95]

In recent years Maryland has used face recognition by comparing people's faces to their driver's license photos. The system drew controversy when it was used in Baltimore to arrest unruly protesters after the death of Freddie Gray in police custody. [96] Many other states are using or developing a similar system however some states have laws prohibiting its use.

The FBI has also instituted its Next Generation Identification program to include face recognition, as well as more traditional biometrics like fingerprints and iris scans , which can pull from both criminal and civil databases. [97] The federal Government Accountability Office criticized the FBI for not addressing various concerns related to privacy and accuracy. [98]

Starting in 2018, U.S. Customs and Border Protection deployed "biometric face scanners" at U.S. airports. Passengers taking outbound international flights can complete the check-in, security and the boarding process after getting facial images captured and verified by matching their ID photos stored on CBP's database. Images captured for travelers with U.S. citizenship will be deleted within up to 12-hours. The Transportation Security Administration (TSA) had expressed its intention to adopt a similar program for domestic air travel during the security check process in the future. The American Civil Liberties Union is one of the organizations against the program, concerning that the program will be used for surveillance purposes. [99]

In 2019, researchers reported that Immigration and Customs Enforcement (ICE) uses facial recognition software against state driver's license databases, including for some states that provide licenses to undocumented immigrants. [98]

In December 2022, 16 major domestic airports in the US started testing facial-recognition tech where kiosks with cameras are checking the photos on travelers' IDs to make sure that passengers are not impostors. [100] In 2025, it was revealed that the New Orleans Police Department had rolled out what the ACLU's Freed Wessler called "the first known widespread effort by police in a major US city to use AI to identify people in live camera feeds for the purpose of making immediate arrests." in defiance of a 2022 city ordinance limiting the use of the technology. [101]

China

In 2006, the "Skynet" (■■■)Project was initiated by the Chinese government to implement CCTV surveillance nationwide and as of 2018, [update] there have been 20 million cameras, many of which are capable of real-time facial recognition, deployed across the country for this project. [102] Some official claim that the current Skynet system can scan the entire Chinese population in one second and the world population in two seconds. [103]

In 2017, the Qingdao police was able to identify twenty-five wanted suspects using facial recognition equipment at the Qingdao International Beer Festival, one of which had been on the run for 10 years. [104] The equipment works by recording a 15-second video clip and taking multiple snapshots of the subject. That data is compared and analyzed with images from the police department's database and within 20 minutes, the subject can be identified with a 98.1% accuracy. [105]

In 2018, Chinese police in Zhengzhou and Beijing were using smart glasses to take photos which are compared against a government database using facial recognition to identify suspects, retrieve an address, and track people moving beyond their home areas. [106] [107]

As of late 2017, [update] China has deployed facial recognition and artificial intelligence technology in Xinjiang . Reporters visiting the region found surveillance cameras installed every hundred meters or so in several cities, as well as facial recognition checkpoints at areas like gas stations, shopping centers, and mosque entrances. [108] [109] In May 2019, Human Rights Watch reported finding Face++ code in the Integrated Joint Operations Platform (IJOP), a police surveillance app used to collect data on, and track the Uighur community in Xinjiang . [110] Human Rights Watch released a correction to its report in June 2019 stating that the Chinese company Megvii did not appear to have collaborated on IJOP, and that the Face++ code in the app was inoperable. [111] In February 2020, following the Coronavirus outbreak , Megvii applied for a bank loan to optimize the body temperature screening system it had launched to help identify people with symptoms of a Coronavirus infection in crowds. In the loan application Megvii stated that it needed to improve the accuracy of identifying masked individuals. [112]

Many public places in China are implemented with facial recognition equipment, including railway stations, airports, tourist attractions, expos, and office buildings. In October 2019, a professor at Zhejiang Sci-Tech University sued the Hangzhou Safari Park for abusing private biometric information of customers. The safari park uses facial recognition technology to verify the identities of its Year Card holders. An estimated 300 tourist sites in China have installed facial recognition systems and use them to admit visitors. This case is reported to be the first on the use of facial recognition systems in China. [113] In August 2020, Radio Free Asia reported that in 2019 Geng Guanjun, a citizen of Taiyuan City who had used the WeChat app by Tencent to forward a video to a friend in the United States was subsequently convicted on the charge of the crime "picking quarrels and provoking troubles". The Court documents showed that the Chinese police used a facial recognition system to identify Geng Guanjun as an "overseas democracy activist" and that China's network management and propaganda departments directly monitor WeChat users. [114]

In 2019, Protestors in Hong Kong destroyed smart lampposts amid concerns they could contain cameras and facial recognition system used for surveillance by Chinese authorities. [115] Human rights groups have criticized the Chinese government for using artificial intelligence facial recognition technology in its suppression against Uyghurs, [116] Christians [117] and Falun Gong practitioners. [118] [119]

India

Even though facial recognition technology (FRT) is not fully accurate, [120] it is being increasingly deployed for identification purposes by the police in India. FRT systems generate a probability match score, or a confidence score between the suspect who is to be identified and the database of identified criminals that is available with the police. The National Automated Facial Recognition System (AFRS) [121] is already being developed by the National Crime Records Bureau (NCRB), a body constituted under the Ministry of Home Affairs. The project seeks to develop and deploy a national database of photographs which would comport with a facial recognition technology system by the central and state security agencies. The Internet Freedom Foundation has flagged concerns regarding the project. [122] The NGO has highlighted that the accuracy of FRT systems are "routinely exaggerated and the real numbers leave much to be desired. [122] The implementation of such faulty FRT systems would lead to high rates of false positives and false negatives in this recognition process."

Under the Supreme Court of India's decision in Justice K.S. Puttaswamy vs Union of India (22017 10 SCC 1), any justifiable intrusion by the State into people's right to privacy, which is protected as a fundamental right under Article 21 of the Constitution, must confirm to certain thresholds, namely: legality, necessity, proportionality and procedural safeguards. [123] As per the Internet Freedom Foundation, the National Automated Facial Recognition System (AFRS) proposal fails to meet any of these thresholds, citing "absence of legality," "manifest arbitrariness," and "absence of safeguards and accountability." [124]

While the national level AFRS project is still in the works, police departments in various states in India are already deploying facial recognition technology systems, such as: TSCOP + CCTNS in Telangana, [125] Punjab Artificial Intelligence System (PAIS) in Punjab, [126] Trinetra in Uttar Pradesh, [127] Police Artificial Intelligence System in Uttarakhand, [128] AFRS in Delhi, Automated Multimodal Biometric Identification System (AMBIS) in Maharashtra, FaceTagr in Tamil Nadu. The Crime and Criminal Tracking Network and Systems (CCTNS), which is a Mission Mode Project under the National e-Governance Plan (NeGP), [129] is viewed as a system which would connect police stations across India, and help them "talk" [130] to each other. The project's objective is to digitize all FIR-related information, including FIRs registered, as well as cases investigated, charge sheets filed, and suspects and wanted persons in all police stations. This shall constitute a national database of crime and criminals in India. CCTNS is being implemented without a data protection law in place. CCTNS is proposed to be integrated with the AFRS, a repository of all crime and criminal related facial data which can be deployed to purportedly identify or verify a person from a variety of inputs ranging from images to videos. [131] This has raised privacy concerns from civil society organizations and privacy experts. Both the projects have been censured as instruments of " mass surveillance " at the hands of the state. [132] In Rajasthan, 'RajCop,' a police app has been recently integrated with a facial recognition module which can match the face of a suspect against a database of known persons in real-time. Rajasthan police is in currently working to widen the ambit of this module by making it mandatory to upload photographs of all arrested persons in CCTNS database, which will "help develop a rich database of known offenders." [133]

Helmets fixed with camera have been designed and being used by Rajasthan police in law and order situations to capture police action and activities of "the miscreants, which can later serve as evidence during the investigation of such cases." [133] PAIS (Punjab Artificial Intelligence System), App employs deep learning, machine learning, and face recognition for the identification of criminals to assist police personnel. [133] The state of Telangana has installed 8 lakh CCTV cameras, [133] with its capital city Hyderabad slowly turning into a surveillance capital. [134]

A false positive happens when facial recognition technology misidentifies a person to be someone they are not, that is, it yields an incorrect positive result. They often results in discrimination and strengthening of existing biases. For example, in 2018, Delhi Police reported that its FRT system had an accuracy rate of 2%, which sank to 1% in 2019. The FRT system even failed to distinguish accurately between different sexes. [135]

The government of Delhi in collaboration with Indian Space Research Organisation (ISRO) is developing a new technology called Crime Mapping Analytics and Predictive System (CMAPS). The project aims to deploy space technology for "controlling crime and maintaining law and order." [133] The system will be connected to a database containing data of criminals. [133] The technology is envisaged to be deployed to collect real-time data at the crime scene. [133]

In a reply dated November 25, 2020 to a Right to Information request filed by the Internet Freedom Foundation seeking information about the facial recognition system being used by the Delhi Police (with reference number DEPOL/R/E/20/07128), [136] the Office of the Deputy Commissioner of Police cum Public Information Officer: Crime stated that they cannot provide the information under section 8(d) of the Right to Information Act, 2005. [137] A Right to Information (RTI) request dated July 30, 2020 was filed with the Office of the Commissioner, Kolkata Police, seeking information about the facial recognition technology that the department was using. [138] The information sought was denied [139] stating that the department was exempted from disclosure under section 24(4) of the RTI Act.

Latin America

In the 2000 Mexican presidential election , the Mexican government employed face recognition software to prevent voter fraud . Some individuals had been registering to vote under several different names, in an attempt to place multiple votes. By comparing new face images to those already in the voter database, authorities were able to reduce duplicate registrations. [140]

In Colombia public transport busses are fitted with a facial recognition system by FaceFirst Inc to identify passengers that are sought by the National Police of Colombia . FaceFirst Inc also built the facial recognition system for Tocumen International Airport in Panama. The face recognition system is deployed to identify individuals among the travellers that are sought by the Panamanian National Police or Interpol . [141] Tocumen International Airport operates an airport-wide surveillance system using hundreds of live face recognition cameras to identify wanted individuals passing through the airport. The face recognition system was initially installed as part of a US$11 million contract and included a computer cluster of sixty computers, a fiber-optic cable network for the airport buildings, as well as the installation of 150 surveillance cameras in the airport terminal and at about 30 airport gates . [142]

At the 2014 FIFA World Cup in Brazil the Federal Police of Brazil used face recognition goggles . Face recognition systems "made in China" were also deployed at the 2016 Summer Olympics in Rio de Janeiro. [141] Nuctech Company provided 145 inspection terminals for Maracanã Stadium and 55 terminals for the Deodoro Olympic Park . [143]

European Union

Police forces in at least 21 countries of the European Union use, or plan to use, facial recognition systems, either for administrative or criminal purposes. [144]

Greek police passed a contract with Intracom-Telecom for the provision of at least 1,000 devices equipped with live facial recognition system. The delivery is expected before the summer 2021. The total value of the contract is over 4 million euros, paid for in large part by the Internal Security Fund of the European Commission . [145]

Italian police acquired a face recognition system in 2017, Sistema Automatico Riconoscimento Immagini (SARI). In November 2020, the Interior ministry announced plans to use it in real-time to identify people suspected of seeking asylum. [146]

The Netherlands has deployed facial recognition and artificial intelligence technology since 2016. [147] The database of the Dutch police currently contains over 2.2 million pictures of 1.3 million Dutch citizens. This accounts for about 8% of the population. In The Netherlands, face recognition is not used by the police on municipal CCTV. [148]

South Africa

In South Africa, in 2016, the city of Johannesburg announced it was rolling out smart CCTV cameras complete with automatic number plate recognition and facial recognition. [149]

Deployment in retail stores

The US firm 3VR, now Identiv , is an example of a vendor which began offering facial recognition systems and services to retailers as early as 2007. [150] In 2012, the company advertised benefits such as "dwell and queue line analytics to decrease customer wait times", "facial surveillance analytic[s] to facilitate personalized customer greetings by employees " and the ability to "[c]reate loyalty programs by combining Point of sale (POS) data with facial recognition". [151]

United States

In 2018, the National Retail Federation Loss Prevention Research Council called facial recognition technology "a promising new tool" worth evaluating. [152]

In July 2020, the Reuters news agency reported that during the 2010s the pharmacy chain Rite Aid had deployed facial recognition video surveillance systems and components from FaceFirst, DeepCam LLC, and other vendors at some retail locations in the United States. [152] Cathy Langley, Rite Aid's vice president of asset protection, used the phrase "feature matching" to refer to the systems and said that usage of the systems resulted in less violence and organized crime in the company's stores, while former vice president of asset protection Bob Oberosler emphasized improved safety for staff and a reduced need for the involvement of law enforcement organizations . [152] In a 2020 statement to Reuters in response to the reporting, Rite Aid said that it had ceased using the facial recognition software and switched off the cameras. [152]

According to director Read Hayes of the National Retail Federation Loss Prevention Research Council, Rite Aid's surveillance program was either the largest or one of the largest programs in retail. [152] The Home Depot , Menards , Walmart , and 7-Eleven are among other US retailers also engaged in large-scale pilot programs or deployments of facial recognition technology. [152]

Of the Rite Aid stores examined by Reuters in 2020, those in communities where people of color made up the largest racial or ethnic group were three times as likely to have the technology installed, [152] raising concerns related to the substantial history of racial segregation and racial profiling in the United States . Rite Aid said that the selection of locations was "data-driven", based on the theft histories of individual stores, local and national crime data , and site infrastructure. [152]

Australia

In 2019, facial recognition to prevent theft was in use at Sydney's Star Casino and was also deployed at gaming venues in New Zealand. [153]

In June 2022, consumer group CHOICE reported facial recognition was in use in Australia at Kmart, Bunnings, and The Good Guys. The Good Guys subsequently suspended the technology pending a legal challenge by CHOICE to the Office of the Australian Information Commissioner, while Bunnings kept the technology in use and Kmart maintained its trial of the technology. [154]

Additional uses

At the American football championship game Super Bowl XXXV in January 2001, police in Tampa Bay, Florida used Viisage face recognition software to search for potential criminals and terrorists in attendance at the event. 19 people with minor criminal records were potentially identified. [155] [156]

Face recognition systems have also been used by photo management software to identify the subjects of photographs, enabling features such as searching images by person, as well as suggesting photos to be shared with a specific contact if their presence were detected in a photo. [157] [158] By 2008 facial recognition systems were typically used as access control in security systems . [159]

The United States' popular music and country music celebrity Taylor Swift surreptitiously employed facial recognition technology at a concert in 2018. The camera was embedded in a kiosk near a ticket booth and scanned concert-goers as they entered the facility for known stalkers . [160]

On August 18, 2019, The Times reported that the UAE-owned Manchester City hired a Texas-based firm, Blink Identity, to deploy facial recognition systems in a driver program. The club has planned a single super-fast lane for the supporters at the Etihad stadium . [161] However, civil rights groups cautioned the club against the introduction of this technology, saying that it would risk "normalising a mass surveillance tool". The policy and campaigns officer at Liberty , Hannah Couchman said that Man City's move is alarming, since the fans will be obliged to share deeply sensitive personal information with a private company, where they could be tracked and monitored in their everyday lives. [162]

In 2019, casinos in Australia and New Zealand rolled out facial recognition to prevent theft, and a representative of Sydney's Star Casino said they would also provide 'customer service' like welcoming a patron back to a bar. [153]

In August 2020, amid the COVID-19 pandemic in the United States , American football stadiums of New York and Los Angeles announced the installation of facial recognition for upcoming matches. The purpose is to make the entry process as touchless as possible. [163] Disney's Magic Kingdom , near Orlando, Florida , likewise announced a test of facial recognition technology to create a touchless experience during the pandemic; the test was originally slated to take place between March 23 and April 23, 2021, but the limited timeframe had been removed as of late April 2021. [update] [164]

Media companies have begun using face recognition technology to streamline their tracking, organizing, and archiving pictures and videos. [165]

Advantages and disadvantages

Compared to other biometric systems

In 2006, the performance of the latest face recognition algorithms was evaluated in the Face Recognition Grand Challenge (FRGC) . High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins. [45] [166]

One key advantage of a facial recognition system that it is able to perform mass identification as it does not require the cooperation of the test subject to work. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd, without passers-by even being aware of the system. [167] However, as compared to other biometric techniques, face recognition may not be most reliable and efficient. Quality measures are very important in facial recognition systems as large degrees of variations are possible in face images.

Factors such as illumination, expression, pose and noise during face capture can affect the performance of facial recognition systems. [167] Among all biometric systems, facial recognition has the highest false acceptance and rejection rates, [167] thus questions have been raised on the effectiveness of or bias of face recognition software in cases of railway and airport security, law enforcement and housing and employment decisions. [168] [5]

Weaknesses

Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute in 2008, describes one obstacle related to the viewing angle of the face: "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems." [45] Besides the pose variations, low-resolution face images are also very hard to recognize. This is one of the main obstacles of face recognition in surveillance systems. [169] It has also been suggested that camera settings can favour sharper imagery of white skin than of other skin tones. [5]

Face recognition is less effective if facial expressions vary. A big smile can render the system less effective. For instance: Canada, in 2009, allowed only neutral facial expressions in passport photos. [170]

There is also inconstancy in the datasets used by researchers. Researchers may use anywhere from several subjects to scores of subjects and a few hundred images to thousands of images. Data sets may be diverse and inclusive or mainly contain images of white males. It is important for researchers to make available the datasets they used to each other, or have at least a standard or representative dataset. [171]

Although high degrees of accuracy have been claimed for some facial recognition systems, these outcomes are not universal. The consistently worst accuracy rate is for those who are 18 to 30 years old, Black and female. [5]

Racial bias and skin tone

Studies have shown that facial recognition algorithms tend to perform better on individuals with lighter skin tones compared to those with darker skin tones. This disparity arises primarily because training datasets often overrepresent lighter-skinned individuals, leading to higher error rates for darker-skinned people. For example, a 2018 study found that leading commercial gender classification models, which are facial recognition models, have an error rate up to 7 times higher for those with darker skin tones compared to those with lighter skin tones. [172]

Common image compression methods, such as JPEG chroma subsampling, have been found to disproportionately degrade performance for darker-skinned individuals. These methods inadequately represent color information, which adversely affects the ability of algorithms to recognize darker-skinned individuals accurately. [173]

Cross-race effect bias

Facial recognition systems often demonstrate lower accuracy when identifying individuals with non-Eurocentric facial features. Known as the Cross-race effect , this bias occurs when systems perform better on racial or ethnic groups that are overrepresented in their training data, resulting in reduced accuracy for underrepresented groups. [174] The overrepresented group is generally the more populous group in the location that the model is being developed. For example, models developed in Asian cultures generally perform better on Asian facial features than Eurocentric facial features due to overrepresentation in the developers training dataset. The opposite is observed in models developed in Eurocentric cultures. [175]

The systems used for facial recognition often lack the sufficient training needed to fully recognize those features not of Eurocentric descent. When the training and databases for these Machine Learning (ML) models do not contain a diverse representation, the models fail to identify the missed population, adding to their racial biases. [7]

The cross-race effect is not exclusive to machines; humans also experience difficulty recognizing faces from racial or ethnic groups different from their own. This is an example of inherent human biases being perpetuated in training datasets. [176]

Challenges for individuals with disabilities

Facial recognition technologies encounter significant challenges when identifying individuals with disabilities. For instance, systems have been shown to perform worse when recognizing individuals with Down syndrome , often leading to increased false match rates. This is due to distinct facial structures associated with the condition that are not adequately represented in training datasets. [177]

More broadly, facial recognition systems tend to overlook diverse physical characteristics related to disabilities. The lack of representative data for individuals with varying disabilities further emphasizes the need for inclusive algorithmic designs to mitigate bias and improve accuracy. [178]

Additionally, facial expression recognition technologies often fail to accurately interpret the emotional states of individuals with intellectual disabilities. This shortcoming can hinder effective communication and interaction, underscoring the necessity for systems trained on diverse datasets that include individuals with intellectual disabilities. [179]

Furthermore, biases in facial recognition algorithms can lead to discriminatory outcomes for people with disabilities. For example, certain facial features or asymmetries may result in misidentification or exclusion, highlighting the importance of developing accessible and fair biometric systems. [180]

Advancements in fairness and mitigation strategies

Efforts to address these biases include designing algorithms specifically for fairness. A notable study introduced a method to learn fair face representations by using a progressive cross-transformer model. [181] This approach highlights the importance of balancing accuracy across demographic groups while avoiding performance drops in specific populations.

Additionally, targeted dataset collection has been shown to improve racial equity in facial recognition systems. By prioritizing diverse data inputs, researchers demonstrated measurable reductions in performance disparities between racial groups. [177]

Ineffectiveness

Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, [update] never recognized a single criminal, despite several criminals in the system's database living in the Borough and the system has been running for several years. "Not once, as far as the police know, has Newham's automatic face recognition system spotted a live target." [156] [182] This information seems to conflict with claims that the system was credited with a 34% reduction in crime (hence why it was rolled out to Birmingham also). [183]

An experiment in 2002 by the local police department in Tampa , Florida, had similarly disappointing results. [156] A system at Boston's Logan Airport was shut down in 2003 after failing to make any matches during a two-year test period. [184]

In 2014, Facebook stated that in a standardized two-option facial recognition test, its online system scored 97.25% accuracy, compared to the human benchmark of 97.5%. [185]

Systems are often advertised as having accuracy near 100%; this is misleading as the outcomes are not universal. [5] The studies often use samples that are smaller and less diverse than would be necessary for large scale applications. Because facial recognition is not completely accurate, it creates a list of potential matches. A human operator must then look through these potential matches and studies show the operators pick the correct match out of the list only about half the time. This causes the issue of targeting the wrong suspect. [93] [186]

Controversies

Privacy violations

Civil rights organizations and privacy campaigners such as the Electronic Frontier Foundation , Big Brother Watch and the ACLU express concern that privacy is being compromised by the use of surveillance technologies . [187] [86] [188] Face recognition can be used not just to identify an individual, but also to unearth other personal data associated with an individual – such as other photos featuring the individual, blog posts, social media profiles, Internet behavior, and travel patterns. [189] Concerns have been raised over who would have access to the knowledge of one's whereabouts and people with them at any given time. [190] Moreover, individuals have limited ability to avoid or thwart face recognition tracking unless they hide their faces. This fundamentally changes the dynamic of day-to-day privacy by enabling any marketer, government agency, or random stranger to secretly collect the identities and associated personal information of any individual captured by the face recognition system. [189] Consumers may not understand or be aware of what their data is being used for, which denies them the ability to consent to how their personal information gets shared. [190]

In July 2015, the United States Government Accountability Office conducted a Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate. The report discussed facial recognition technology's commercial uses, privacy issues, and the applicable federal law. It states that previously, issues concerning facial recognition technology were discussed and represent the need for updating the privacy laws of the United States so that federal law continually matches the impact of advanced technologies. The report noted that some industry, government, and private organizations were in the process of developing, or have developed, "voluntary privacy guidelines". These guidelines varied between the stakeholders , but their overall aim was to gain consent and inform citizens of the intended use of facial recognition technology. According to the report the voluntary privacy guidelines helped to counteract the privacy concerns that arise when citizens are unaware of how their personal data gets put to use. [190]

In 2016, Russian company NtechLab caused a privacy scandal in the international media when it launched the FindFace face recognition system with the promise that Russian users could take photos of strangers in the street and link them to a social media profile on the social media platform Vkontakte (VK). [191] In December 2017, Facebook rolled out a new feature that notifies a user when someone uploads a photo that includes what Facebook thinks is their face, even if they are not tagged. Facebook has attempted to frame the new functionality in a positive light, amidst prior backlashes. [192] Facebook's head of privacy, Rob Sherman, addressed this new feature as one that gives people more control over their photos online. "We've thought about this as a really empowering feature," he says. "There may be photos that exist that you don't know about." [193] Facebook's DeepFace has become the subject of several class action lawsuits under the Biometric Information Privacy Act, with claims alleging that Facebook is collecting and storing face recognition data of its users without obtaining informed consent, in direct violation of the 2008 Biometric Information Privacy Act (BIPA). [194] The most recent case was dismissed in January 2016 because the court lacked jurisdiction. [195] In the US, surveillance companies such as Clearview AI are relying on the First Amendment to the United States Constitution to data scrape user accounts on social media platforms for data that can be used in the development of facial recognition systems. [196]

In 2019, the Financial Times first reported that facial recognition software was in use in the King's Cross area of London. [197] The development around London's King's Cross mainline station includes shops, offices, Google's UK HQ and part of St Martin's College. According to the UK Information Commissioner's Office : "Scanning people's faces as they lawfully go about their daily lives, in order to identify them, is a potential threat to privacy that should concern us all." [198] [199] The UK Information Commissioner Elizabeth Denham launched an investigation into the use of the King's Cross facial recognition system, operated by the company Argent. In September 2019 it was announced by Argent that facial recognition software would no longer be used at King's Cross . Argent claimed that the software had been deployed between May 2016 and March 2018 on two cameras covering a pedestrian street running through the centre of the development. [200] In October 2019, a report by the deputy London mayor Sophie Linden revealed that in a secret deal the Metropolitan Police had passed photos of seven people to Argent for use in their King's cross facial recognition system. [201]

Automated Facial Recognition was trialled by the South Wales Police on multiple occasions between 2017 and 2019. The use of the technology was challenged in court by a private individual, Edward Bridges, with support from the charity Liberty (case known as R (Bridges) v Chief

Constable South Wales Police). The case was heard in the Court of Appeal and a judgement was given in August 2020. [202] The case argued that the use of Facial Recognition was a privacy violation on the basis that there was insufficient legal framework or proportionality in the use of Facial Recognition and that its use was in violation of the Data Protection Acts 1998 and 2018 . The case was decided in favour of Bridges and did not award damages. The case was settled via a declaration of wrongdoing. [202] In response to the case, the British Government has repeatedly attempted to pass a Bill regulating the use of Facial Recognition in public spaces. The proposed Bills have attempted to appoint a Commissioner with the ability to regulate Facial Recognition use by Government Services in a similar manner to the Commissioner for CCTV . Such a Bill has yet to come into force [correct as of September 2021 [update]]. [126]

In January 2023, New York Attorney General Letitia James asked for more information on the use of facial recognition technology from Madison Square Garden Entertainment following reports that the firm used it to block lawyers involved in litigation against the company from entering Madison Square Garden . She noted such a move would could go against federal, state, and local human rights laws. [203]

Imperfect technology in law enforcement

As of 2018, [update] it is still contested as to whether or not facial recognition technology works less accurately on people of color. [204] One study by Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research) found that the error rate for gender recognition for women of color within three commercial facial recognition systems ranged from 23.8% to 36%, whereas for lighter-skinned men it was between 0.0 and 1.6%. Overall accuracy rates for identifying men (91.9%) were higher than for women (79.4%), and none of the systems accommodated a non-binary understanding of gender. [205] It also showed that the datasets used to train commercial facial recognition models were unrepresentative of the broader population and skewed toward lighter-skinned males. However, another study showed that several commercial facial recognition software sold to law enforcement offices around the country had a lower false non-match rate for black people than for white people. [206]

Experts fear that face recognition systems may actually be hurting citizens the police claims they are trying to protect. [207] It is considered an imperfect biometric, and in a study conducted by Georgetown University researcher Clare Garvie, she concluded that "there's no consensus in the scientific community that it provides a positive identification of somebody." [208] It is believed that with such large margins of error in this technology, both legal advocates and facial recognition software companies say that the technology should only supply a portion of the case – no evidence that can lead to an arrest of an individual. [208] The lack of regulations holding facial recognition technology companies to requirements of racially biased testing can be a significant flaw in the adoption of use in law enforcement. CyberExtruder, a company that markets itself to law enforcement said that they had not performed testing or research on bias in their software. CyberExtruder did note that some skin colors are more difficult for the software to recognize with current limitations of the technology. "Just as individuals with very dark skin are hard to identify with high significance via facial recognition, individuals with very pale skin are the same," said Blake Senftner, a senior software engineer at CyberExtruder. [208]

The United States' National Institute of Standards and Technology (NIST) carried out extensive testing of FRT system 1:1 verification [209] and 1:many identification. [209] It also tested for the differing accuracy of FRT across different demographic groups. The independent study concluded at present, no FRT system has 100% accuracy. [210]

Data protection

In 2010, Peru passed the Law for Personal Data Protection, which defines biometric information that can be used to identify an individual as sensitive data. In 2012, Colombia passed a comprehensive Data Protection Law which defines biometric data as senstivite information. [141] According to Article 9(1) of the EU's 2016 General Data Protection Regulation (GDPR) the processing of biometric data for the purpose of "uniquely identifying a natural person" is sensitive and the facial recognition data processed in this way becomes sensitive personal data. In response to the GDPR passing into the law of EU member states , EU based researchers voiced concern that if they were required under the GDPR to obtain individual's consent for the processing of their facial recognition data, a face database on the scale of MegaFace could never be established again. [211] In September 2019 the Swedish Data Protection Authority (DPA) issued its first ever financial penalty for a violation of the EU's General Data Protection Regulation (GDPR) against a school that was using the technology to replace time-consuming roll calls during class. The DPA found that the school illegally obtained the biometric data of its students without completing an impact assessment. In addition the school did not make the DPA aware of the pilot scheme. A 200,000 SEK fine (€19,000/$21,000) was issued. [citation needed]

In the United States of America several U.S. states have passed laws to protect the privacy of biometric data. Examples include the Illinois Biometric Information Privacy Act (BIPA) and the California Consumer Privacy Act (CCPA). [212] In March 2020 California residents filed a class action against Clearview AI , alleging that the company had illegally collected biometric data online and with the help of face recognition technology built up a database of biometric data which was sold to companies and police forces. At the time Clearview AI already faced two lawsuits under BIPA [213] and an investigation by the Privacy Commissioner of Canada for compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA). [214]

Bans on the use of facial recognition technology

United States of America

In May 2019, San Francisco, California became the first major United States city to ban the use of facial recognition software for police and other local government agencies' usage. [215] San Francisco Supervisor, Aaron Peskin , introduced regulations that will require agencies to gain approval from the San Francisco Board of Supervisors to purchase surveillance technology. [216] The regulations also require that agencies publicly disclose the intended use for new surveillance technology. [216] In June 2019, Somerville , Massachusetts became the first city on the East Coast to ban face surveillance software for government use, [217] specifically in police investigations and municipal surveillance. [218] In July 2019, Oakland, California banned the usage of facial recognition technology by city departments. [219]

The American Civil Liberties Union ("ACLU") has campaigned across the United States for transparency in surveillance technology [218] and has supported both San Francisco and Somerville's ban on facial recognition software. The ACLU works to challenge the secrecy and surveillance with this technology. [citation needed] [220]

During the George Floyd protests , use of facial recognition by city government was banned in Boston , Massachusetts. [221] As of June 10, 2020, [update] municipal use has been banned in: [11]

Berkeley, California

Oakland, California

Boston , Massachusetts – June 30, 2020 [222]

Brookline, Massachusetts

Cambridge, Massachusetts

Northampton, Massachusetts

Springfield, Massachusetts

Somerville, Massachusetts

Portland, Oregon – September 2020 [223]

The West Lafayette, Indiana City Council passed an ordinance banning facial recognition surveillance technology. [224]

On October 27, 2020, 22 human rights groups called upon the University of Miami to ban facial recognition technology. This came after the students accused the school of using the software to identify student protesters. The allegations were, however, denied by the university. [225]

A state police reform law in Massachusetts will take effect in July 2021; a ban passed by the legislature was rejected by governor Charlie Baker . [226] Instead, the law requires a judicial warrant, limit the personnel who can perform the search, record data about how the technology is used, and create a commission to make recommendations about future regulations. [227]

Reports in 2024 revealed that some police departments, including San Francisco Police Department , had skirted bans on facial recognition technology that had been enacted in their respective cities. [228]

European Union

In January 2020, the European Union suggested, but then quickly scrapped, a proposed moratorium on facial recognition in public spaces. [229] [230]

The European " Reclaim Your Face " coalition launched in October 2020. The coalition calls for a ban on facial recognition and launched a European Citizens' Initiative in February 2021. More than 60 organizations call on the European Commission to strictly regulate the use of biometric surveillance technologies. [231]

Emotion recognition

In the 18th and 19th century, the belief that facial expressions revealed the moral worth or true inner state of a human was widespread and physiognomy was a respected science in the Western world. From the early 19th century onwards photography was used in the physiognomic analysis of facial features and facial expression to detect insanity and dementia . [232] In the 1960s and 1970s the study of human emotions and its expressions was reinvented by psychologists , who tried to define a normal range of emotional responses to events. [233] The research on automated emotion recognition has since the 1970s focused on facial expressions and speech , which are regarded as the two most important ways in which humans communicate emotions to other humans. In the 1970s the Facial Action Coding System (FACS) categorization for the physical expression of emotions was established. [234] Its developer Paul Ekman maintains that there are six emotions that are universal to all human beings and that these can be coded in facial expressions. [235] Research into automatic emotion specific expression recognition has in the past decades focused on frontal view images of human faces. [236] Facial thermography can be considered as a promising tool of emotion recognition. [237] [238]

In 2016, facial feature emotion recognition algorithms were among the new technologies, alongside high-definition CCTV , high resolution 3D face recognition and iris recognition , that found their way out of university research labs. [citation needed] In 2016, Facebook acquired FacioMetrics, a facial feature emotion recognition corporate spin-off by Carnegie Mellon University . In the same year Apple Inc. acquired the facial feature emotion recognition start-up Emotient. [239] By the end of 2016, commercial vendors of facial recognition systems offered to integrate and deploy emotion recognition algorithms for facial features. [citation needed] The MIT's Media Lab spin-off Affectiva [240] by late 2019 offered a facial expression emotion detection product that can recognize emotions in humans while driving . [239]

Anti-facial recognition systems

The development of anti-facial recognition technology is effectively an arms race between privacy researchers and big data companies. Big data companies increasingly use convolutional AI technology to create ever more advanced facial recognition models. Solutions to block facial recognition may not work on newer software, or on different types of facial recognition models. One popular cited example of facial-recognition blocking is the CVDazzle makeup and haircut system, but the creators note on their website that it has been outdated for quite some time as it was designed to combat a particular facial recognition algorithm and may not work. [241] Another example is the emergence of facial recognition that can identify people wearing facemasks and sunglasses, especially after the COVID-19 pandemic. [242]

Given that big data companies have much more funding than privacy researchers, it is very difficult for anti-facial recognition systems to keep up. There is also no guarantee that obfuscation techniques that were used for images taken in the past and stored, such as masks or software obfuscation, would protect users from facial-recognition analysis of those images by future technology. [243]

In January 2013, Japanese researchers from the National Institute of Informatics created 'privacy visor' glasses that use nearly infrared light to make the face underneath it unrecognizable to face recognition software that use infrared. [244] The latest version uses a titanium frame, light-reflective material and a mask which uses angles and patterns to disrupt facial recognition technology through both absorbing and bouncing back light sources. [245] [246] [247] [248] However, these methods are used to prevent infrared facial recognition and would not work on AI facial recognition of plain images. Some projects use adversarial machine learning to come up with new printed patterns that confuse existing face recognition software. [249]

One method that may work to protect from facial recognition systems are specific haircuts and make-up patterns that prevent the used algorithms to detect a face, known as computer vision dazzle . [241] Incidentally, the makeup styles popular with Juggalos may also protect against facial recognition. [250]

Facial masks that are worn to protect from contagious viruses can reduce the accuracy of facial recognition systems. A 2020 NIST study, tested popular one-to-one matching systems and found a failure rate between five and fifty percent on masked individuals. The Verge speculated that the accuracy rate of mass surveillance systems, which were not included in the study, would be even less accurate than the accuracy of one-to-one matching systems. [251] The facial recognition of Apple Pay can work through many barriers, including heavy makeup, thick beards and even sunglasses, but fails with masks. [252] However, facial recognition of masked faces is increasingly getting more reliable.

Another solution is the application of obfuscation to images that may fool facial recognition systems while still appearing normal to a human user. These could be used for when images are posted online or on social media. However, as it is hard to remove images once they are on the internet, the obfuscation on these images may be defeated and the face of the user identified by future advances in technology. Two examples of this technique, developed in 2020, are the ANU 's 'Camera Adversaria' camera app, and the University of Chicago 's Fawkes image cloaking software algorithm which applies obfuscation to already taken photos. [243] However, by 2021 the Fawkes obfuscation algorithm had already been specifically targeted by Microsoft Azure which changed its algorithm to lower Fawkes' effectiveness. [253]

See also

AI effect

Amazon Rekognition

Applications of artificial intelligence

Artificial intelligence for video surveillance

Automatic number plate recognition

Biometric technology in access control

Coke Zero Facial Profiler

Computer processing of body language

Computer vision

DeepFace

FaceNet

Face perception

Face Recognition Grand Challenge

FindFace

Glasgow Face Matching Test

ISO/IEC 19794-5

MALINTENT

National biometric id card

Multimedia information retrieval

Multilinear subspace learning

Pattern recognition , analogy and case-based reasoning

Retinal scan

SenseTime

Super recognisers

Template matching

Three-dimensional face recognition

Vein matching

Gait analysis

Fawkes (image cloaking software)

List of computer vision topics

List of emerging technologies

Outline of artificial intelligence

References

Further reading

Farokhi, Sajad; Shamsuddin, Siti Mariyam; Flusser, Jan; Sheikh, U.U; Khansari, Mohammad; Jafari-Khouzani, Kourosh (2014). "Near infrared face recognition by combining Zernike moments and undecimated discrete wavelet transform". Digital Signal Processing . 31 (1): 13– 27. Bibcode : 2014DSP....31...13F . doi : 10.1016/j.dsp.2014.04.008 .

"The Face Detection Algorithm Set to Revolutionize Image Search" (Feb. 2015), MIT Technology Review

Garvie, Clare; Bedoya, Alvaro; Frankle, Jonathan (October 18, 2016). Perpetual Line Up: Unregulated Police Face Recognition in America . Center on Privacy & Technology at Georgetown Law . Retrieved October 22, 2016 . "Facial Recognition Software 'Sounds Like Science Fiction,' but May Affect Half of Americans" . As It Happens . Canadian Broadcasting Corporation . October 20, 2016 . Retrieved October 22, 2016 . Interview with Alvaro Bedoya, executive director of the Center on Privacy & Technology at Georgetown Law and co-author of Perpetual Line Up: Unregulated Police Face Recognition in America .

"Facial Recognition Software 'Sounds Like Science Fiction,' but May Affect Half of Americans" . As It Happens . Canadian Broadcasting Corporation . October 20, 2016 . Retrieved October 22, 2016 . Interview with Alvaro Bedoya, executive director of the Center on Privacy & Technology at Georgetown Law and co-author of Perpetual Line Up: Unregulated Police Face Recognition in America .

Press, Eyal , "In Front of Their Faces: Does facial-recognition technology lead police to ignore contradictory evidence?", The New Yorker , 20 November 2023, pp. 20–26.

External links

Media related to Facial recognition system at Wikimedia Commons

A Photometric Stereo Approach to Face Recognition (master's thesis). The University of the West of England, Bristol .

v

t

e

History timeline

timeline

Companies

Projects

Parameter Hyperparameter

Hyperparameter

Loss functions

Regression Bias–variance tradeoff Double descent Overfitting

Bias–variance tradeoff

Double descent

Overfitting

Clustering

Gradient descent SGD Quasi-Newton method Conjugate gradient method

SGD

Quasi-Newton method

Conjugate gradient method

Backpropagation

Attention

Convolution

Normalization Batchnorm

Batchnorm

Activation Softmax Sigmoid Rectifier

Softmax

Sigmoid

Rectifier

Gating

Weight initialization

Regularization

Datasets Augmentation

Augmentation

Prompt engineering

Reinforcement learning Q-learning SARSA Imitation Policy gradient

Q-learning

SARSA

Imitation

Policy gradient

Diffusion

Latent diffusion model

Autoregression

Adversary

RAG

Uncanny valley

RLHF

Self-supervised learning

Reflection

Recursive self-improvement

Hallucination

Word embedding

Vibe coding

Machine learning In-context learning

In-context learning

Artificial neural network Deep learning

Deep learning

Language model Large language model NMT

Large language model

NMT

Reasoning language model

Model Context Protocol

Intelligent agent

Artificial human companion

Humanity's Last Exam

Artificial general intelligence (AGI)

AlexNet

WaveNet

Human image synthesis

HWR

OCR

Computer vision

Speech synthesis 15.ai ElevenLabs

15.ai

ElevenLabs

Speech recognition Whisper

Whisper

Facial recognition

AlphaFold

Text-to-image models Aurora DALL-E Firefly Flux Ideogram Imagen Midjourney Recraft Stable Diffusion

Aurora

DALL-E

Firefly

Flux

Ideogram

Imagen

Midjourney

Recraft

Stable Diffusion

Text-to-video models Dream Machine Runway Gen Hailuo AI Kling Sora Veo

Dream Machine

Runway Gen

Hailuo AI

Kling

Sora

Veo

Music generation Riffusion Suno AI Udio

Riffusion

Suno AI

Udio

Word2vec

Seq2seq

GloVe

BERT

T5

Llama

Chinchilla AI

PaLM

GPT 1 2 3 J ChatGPT 4 4o o1 o3 4.5 4.1 o4-mini 5

1

2

3

J

ChatGPT

4

4o

o1

o3

4.5

4.1

o4-mini

5

Claude

Gemini Gemini (language model) Gemma

Gemini (language model)

Gemma

Grok

LaMDA

BLOOM

DBRX

Project Debater

IBM Watson

IBM Watsonx

Granite

PanGu-Σ

DeepSeek

Qwen

AlphaGo

AlphaZero

OpenAI Five

Self-driving car

MuZero

Action selection AutoGPT

AutoGPT

Robot control

Alan Turing

Warren Sturgis McCulloch

Walter Pitts

John von Neumann

Claude Shannon

Shun'ichi Amari

Kunihiko Fukushima

Takeo Kanade

Marvin Minsky

John McCarthy

Nathaniel Rochester

Allen Newell

Cliff Shaw

Herbert A. Simon

Oliver Selfridge

Frank Rosenblatt

Bernard Widrow

Joseph Weizenbaum

Seymour Papert

Seppo Linnainmaa

Paul Werbos

Geoffrey Hinton

John Hopfield

Jürgen Schmidhuber

Yann LeCun

Yoshua Bengio

Lotfi A. Zadeh

Stephen Grossberg

Alex Graves

James Goodnight

Andrew Ng

Fei-Fei Li

Alex Krizhevsky

Ilya Sutskever

Oriol Vinyals

Quoc V. Le

Ian Goodfellow

Demis Hassabis

David Silver

Andrej Karpathy

Ashish Vaswani

Noam Shazeer

Aidan Gomez

John Schulman

Mustafa Suleyman

Jan Leike

Daniel Kokotajlo

François Chollet

Neural Turing machine

Differentiable neural computer

Transformer Vision transformer (ViT)

Vision transformer (ViT)

Recurrent neural network (RNN)

Long short-term memory (LSTM)

Gated recurrent unit (GRU)

Echo state network

Multilayer perceptron (MLP)

Convolutional neural network (CNN)

Residual neural network (RNN)

Highway network

Mamba

Autoencoder

Variational autoencoder (VAE)

Generative adversarial network (GAN)

Graph neural network (GNN)

Category

United States

Israel

Yale LUX