The Ethics of Facial Recognition Technology

A face analyzer is software that identifies or confirms a person's identity using their face. It works by identifying and measuring facial features in an image. Facial recognition can identify human faces in images or videos, determine if the face in two images belongs to the same person, or search for a face among a large collection of existing images. Biometric security systems use facial recognition to uniquely identify individuals during user onboarding or logins as well as strengthen user authentication activity. Mobile and personal devices also commonly use face analyzer technology for device security.

A Look at the Benefits:

Some benefits of face recognition systems are as follows:

Efficient Security:

Facial recognition is a quick and efficient verification system. It is faster and more convenient compared to other biometric technologies like fingerprints or retina scans. There are also fewer touchpoints in facial recognition compared to entering passwords or PINs. It supports multifactor authentication for additional security verification.

Improved Accuracy:

Facial recognition is a more accurate way to identify individuals than simply using a mobile number, email address, mailing address, or IP address. For example, most exchange services, from stocks to cryptos, now rely on facial recognition to protect customers and their assets.

Easier Integration:

Face recognition technology is compatible and integrates easily with most security software. For example, smartphones with front-facing cameras have built-in support for facial recognition algorithms or software code.

What are the use cases of facial recognition systems?

The following are some practical applications of a face recognition system:

Fraud Detection:

Companies use facial recognition to uniquely identify users creating a new account on an online platform. After this is done, facial recognition can be used to verify the identity of the actual person using the account in case of risky or suspicious account activity.

Cyber Security:

Companies use facial recognition technology instead of passwords to strengthen cybersecurity measures. It is challenging to gain unauthorized access into facial recognition systems, as nothing can be changed about your face. Face recognition software is also a convenient and highly accurate security tool for unlocking smartphones and other personal devices.

Airport and Border Control:

Many airports use biometric data as passports, allowing travellers to skip long lines and walk through an automated terminal to reach their gate faster. Face recognition technology in the form of e-Passports reduces wait times and improves security.

Banking:

Individuals authenticate transactions by simply looking at their phone or computer instead of using one-time passwords or two-step verification. Facial recognition is safer as there are no passwords for hackers to compromise. Similarly, some ATM cash withdrawals and checkout registers can use facial recognition for approving payments.

HealthCare:

Facial recognition can be used to gain access to patient records. It can streamline the patient registration process in a healthcare facility and autodetect pain and emotion in patients.

How does facial recognition work?

Facial recognition works in three steps: detection, analysis, and recognition.

Detection:

Detection is the process of finding a face in an image. Enabled by computer vision, facial recognition can detect and identify individual faces from an image containing one or many people's faces. It can detect facial data in both front and side face profiles.

Computer Vision:

Machines use computer vision to identify people, places, and things in images with accuracy at or above human levels and with much greater speed and efficiency. Using complex artificial intelligence (AI) technology, computer vision automates extraction, analysis, classification, and understanding of useful information from image data. The image data takes many forms, such as the following:

Single images

Video sequences

Views from multiple cameras

Three-dimensional data

Analysis:

The facial recognition system then analyzes the image of the face. It maps and reads face geometry and facial expressions. It identifies facial landmarks that are key to distinguishing a face from other objects. The facial recognition technology typically looks for the following:

Distance between the eyes

Distance from the forehead to the chin

Distance between the nose and mouth

Depth of the eye sockets

Shape of the cheekbones

Contour of the lips, ears, and chin

The system then converts the face recognition data into a string of numbers or points called a faceprint. Each person has a unique faceprint, similar to a fingerprint. The information used by facial recognition can also be used in reverse to digitally reconstruct a person's face.

Recognition:

Facial recognition can identify a person by comparing the faces in two or more images and assessing the likelihood of a face match. For example, it can verify that the face shown in a selfie taken by a mobile camera matches the face in an image of a government-issued ID like a driver's license or passport, as well as verify that the face shown in the selfie does not match a face in a collection of faces previously captured.

Is facial recognition accurate?

Facial recognition algorithms have near-perfect accuracy in ideal conditions. There is a higher success rate in controlled settings but generally a lower performance rate in the real world. It is difficult to accurately predict the success rate of this technology, as no single measure provides a complete picture.

For instance, facial verification algorithms matching people to clear reference images, such as a driver's license or a mugshot, achieve high-accuracy scores. However, this degree of accuracy is only possible with the following:

Consistent positioning and lighting

Clear and unobstructed facial features

Controlled colors and background

Camera quality and image resolution

Another factor that impacts error rates is aging. Over time, changes in the face make it difficult to match photos taken years earlier.

Is facial recognition safe?

Human face recognition systems use unique mathematical patterns to store biometric data. Hence, they are among the safest and most effective identification methods in biometric technology. Facial data can be anonymized

and kept private to reduce the risk of unauthorized access. Liveness detection technology distinguishes live users from their facial images. This prevents the system from being tricked by the photograph of a live user.

What is a confidence score in facial recognition?

Confidence scores, also known as similarity scores, are crucial for face detection and comparison systems. They provide feedback about how similar two images are to each other. A higher confidence score indicates a higher likelihood that two images are of the same person. Thus, confidence scores use AI to predict whether a face exists in an image or matches a face in another image.

Confidence score Threshold:

Every prediction that the facial recognition system makes using AI has a corresponding score threshold level that you can change. In a typical scenario, most automated matches are made on a very high percentage, for example, above a 99% confidence score. Matches with lower confidence scores may be used to see the next closest potential matches, which are then further evaluated by a human investigator.

What are other types of Biometric Identification Technology?

Biometric identification is the process of identifying individuals based on unique, distinguishable traits. Besides facial recognition, there are many other types of biometric identification:

Fingerprint Verification:

Fingerprint recognition software verifies an individual's identity by comparing their fingerprint against one or more fingerprints in a database.

DNA Matching:

DNA matching identifies an individual by analyzing segments from their DNA. The technology sequences the DNA in a lab and compares it with samples in a database.

Eye Recognition:

Eye recognition analyzes features in the iris or patterns of the veins in the retina to determine a match and identify an individual.

Hand Geometry Recognition:

You can uniquely identify individuals through the geometric features of their hands, such as the length of the fingers and width of the hand. A camera captures a silhouette image of the hand and compares it against a database.

Voice Recognition:

Voice recognition systems extract the characteristics that distinguish an individual's speech from others. It creates a voiceprint that is similar to a fingerprint or faceprint and matches it to samples in a database.

Signature Recognition:

You can use technology to analyze handwriting style or compare two scanned signatures using advanced algorithms.