Concept of face recognition technique

thedailyguardian.com/concept-of-face-recognition-technique

March 1, 2023

Facial recognition is a category of biometric software that maps an individual's facial features mathematically and stores the data as a faceprint. The software uses deep learning algorithms to compare a live capture or digital image to the stored faceprint in order to verify an individual's identity. Did you know that every time we upload an image to a site like facebook they use facial recognition to recognize faces in it ? Certain governments around the world also use face recognition to identify and catch criminals and to prevent . And today we can unlock our phone with face unlock. Technology has evolved from being a problem-solving force to being a purpose-driven entity for humans. Back in the 1990s, technology was limited to computers, the internet, email, and wired phones, but advances in technology have profoundly changed its role as an essential necessity in our lives and societies. One of the most important advances is the emergence of artificial intelligence (AI) and machine learning (ML). Artificial intelligence (AI) and machine learning (ML) are designed to replace human intervention in daily operations and to process and protect mission-critical applications. In the sections below, we look at the breadth of AI and ML in various use cases to understand their role in one of the most advanced forms of biometric security, facial recognition. Artificial intelligence has proven to be one of the most revolutionary and at the same time one of the most controversial technologies. AI is an important part of our daily lives today. Everything from social media to digital assistants to email communications to video streaming app recommendations is powered by AI technology.

The face identifier procedure simply requires any device that has digital photographic technology to generate and obtain the images and data necessary to create and record the biometric facial pattern of the person that needs to be identified.

Unlike other identification solutions such as passwords, verification by email, selfies or images, or fingerprint identification, Biometric facial recognition uses unique mathematical and dynamic patterns works as a face scanner that make this system one of the safest and most effective ones. The goal of face recognition is to find, from an input image, a set of data for the same face from a set of training images in a database. The main difficulty is ensuring that this process runs in real time. This is not available with all biometric face recognition software providers.

We often think how does this facial recognition work ? They compare the relevant information of the input image signal in real time with the photos or videos in the database, which is much more reliable and secure than the information available with static images. This biometric facial recognition process requires an internet connection. This is because the database is hosted on the server and cannot be on the capture device. This face comparison is an error-free mathematical analysis of the input image and matches the biometric data with the person who needs to use the service or requests access to an application, system or even building. This software identifies 80 nodes in a human face. A node in this context is an endpoint used to measure dimensions of a

person's face, such as nose length and width, eye socket depth, and cheekbone shape. The system collects data for nodes on a digital image of a person's face and saves the resulting data as faceprints. Face prints are used as a basis for comparison with data captured from the face in images or videos.
The facial recognition system he uses only 80 nodes, but in the right conditions can identify targets quickly and accurately. However, if the person's face is partially obscured or if they are not looking forward and are in profile, this type of software is less reliable. According to the National Institute of Standards and Technology (NIST), the rate of false alarms from facial recognition systems has halved every two years since 1993.
Using artificial intelligence (AI) and machine learning technology, the facial recognition system operates with the highest standards of security and reliability. Likewise, the integration of these algorithms and computing techniques allows processes to be executed in real time. Face recognition example
High-quality cameras in mobile devices have made facial recognition a viable option for authentication and identification. For example, Apple's iPhone X and Xs include Face ID technology, which allows users to unlock their phones with a facial fingerprint captured by the phone's camera. Designed using 3D modeling to prevent counterfeiting of photos and masks, the phone's software captures and compares over 30,000 variables. Face ID can be used to authenticate purchases on Apple Pay, the iTunes Store, the App Store, and the iBooks Store. Apple encrypts face recognition data and stores it in the cloud, but authentication happens directly on the device. Smart ads at airports can now identify the gender, ethnicity and approximate age of passers-by and show ads targeted to that person's demographics.

Application of face recognition technology
Facial recognition can be used in many ways, from security to advertising. Examples of usage include:
• Mobile phone manufacturers like Apple for consumer safety.
• Through the Department of Homeland Security, airports to identify those who may stay beyond visas.
• Law enforcement by collecting facial photographs from local, state, and federal resources for comparison against databases.
• Social media such as Facebook that tags people in photos.
• Corporate security, as businesses can use facial recognition to access buildings. and
• Marketing that allows marketers to target specific audiences by using facial recognition to determine age, gender, and ethnicity.
Facebook uses facial recognition software to tag people in photos. Every time a person is tagged in a photo, the software stores mapping information about that person's facial features. Once enough data is collected, the software can use that information to identify the faces of specific people in new photos. To protect people's privacy, a feature called Photo Review notifies her Facebook members who have been identified. Other examples of facial recognition include Amazon, MasterCard and Alibaba. These have introduced a facial recognition payment method commonly referred to as Selfie Pay. The Google Arts & Culture app uses facial recognition to identify museum look-alikes by matching real-life headshots with portrait headshots.

Advantage

Using facial recognition has a variety of potential benefits, including:

• No physical contact with the device for authentication – Compared to other contact-based biometric authentication technologies such as fingerprint scanners, it may not work properly if a person's hands are dirty.
• Increased security level.
• Less processing compared to other biometric technologies.
• Easy integration with existing security features.
• The accuracy of measurements has improved over time. and
• Can be used for authentication automation.

The Ministry of Railways, Government of India, also plans to use facial recognition to tackle crime. The system is under trial in Bengaluru, every about half a million faces are scanned every day, and using AI, these are matched against faces part of a police database of criminals. Besides, the Ministry also plans to extend these facial recognition applications onboard trains. The advent of facial recognition technology has generated abuse warnings from legal experts, privacy advocates, and human rights activists. Many cite the example of China, where everything from security surveillance to jaywalking to speeding to border controls is under surveillance. The country has been at the forefront of adopting high AI standards, but has been heavily criticized for "spying" on its inhabitants.

Tripti Bhushan