25. FACE RECOGNITION ALGORITHM USING STATE-OF-THE-ART TECHNOLOGY

Kuznetsova S.A.

Belarusian State University, Minsk, Republic of Belarus

Sitnikova T.V. — Senior Lecturer,

Vidisheva S.K. — Senior Lecturer

This paper discusses how face recognition technology works to identify an individual from facial images and its application in various fields. The advantages and disadvantages of the development are considered, as well as possible ways to overcome the disadvantages.

Biometric face recognition systems operate on general principles and consist of two stages. The first stage involves detecting and capturing a person's face, whether they are alone or in a crowd. Detection is the process of determining the location of faces in an image. Face recognition, supported by computer vision, allows you to detect and identify a person's face in an image containing one or more faces. Facial data can be detected from both frontal and profile face contours.

The second stage involves analyzing the photos. Face recognition software analyses key points such as eye spacing, cheekbone shape, eye size and shape, eyebrows, nose and lips. These facial features are then converted into a digital code called a "face print". The code is then compared to a database of facial prints. The technology can also scan, store, and recognize facial shapes or thermal images using infrared thermography, three-dimensional measurements, and skeletal analysis. It can be used to verify identities by comparing a camera-captured facial image with a stored database of photographs.

For instance, the analysis of photographs with pixel-level modifications, known as face patches, is proposed in [3]. Examples that utilize various image generation methods with distortions leading to misclassification are described in articles [1, 2].

Recently, face recognition technology has been widely used in various countries and industries. Authentication of bank payments and ICT services is one such industry as it can be conveniently used without the need to memorize or carry it around. Biometric authentication provides excellent security, as there is no need to set a password, which is difficult to forget or copy, and there is no need to worry about theft or loss. For example, in China, face recognition technology is used to pay in the subway and stores, and in December 2019, a decree was introduced requiring face scanning to register new mobile phones.

One of the undeniable advantages of image-based face identification technology is that it does not require physical contact with the device, as in the case with other biometric indicators, making it the most preferable for mass adoption in terms of convenience and hygiene.

Face recognition technology is also used by law enforcement agencies to prevent and investigate crime. In order to improve the efficiency of searching for suspects, law enforcement agencies are working on creating 3D images and analyzing 2D video based on existing criminal databases.

The main security challenges associated with facial recognition include vulnerabilities in facial authentication technology, identity theft through information leakage, and privacy violations such as revealing travel routes and shopping patterns when verifying identity through facial recognition. Unlike other biometrics, facial information used for face recognition can be easily obtained by others through photos posted on social media or through illegal recordings, etc.

Many countries, including the United States and Europe, have introduced guidelines or enacted laws at the state level regarding face recognition technology. For example, in the US state of Illinois, the Biometric Information Privacy Act (BIPA) prohibits the collection of biometric information without the written consent of the subject of the information.

The technology also has another disadvantage, which is the dependence of the quality of the facial recognition result on factors such as position, angle, lighting conditions, etc. However, this problem can be solved by developing 3D recognition technology.

The 3D face spoofing system is a method used to combat spoofing attacks in face recognition systems. Spoofing attacks can involve the use of photos, videos, or 3D face models to trick the system and gain unauthorized access.

The 3D face spoofing system is designed to detect and prevent such attacks by analyzing the geometric and textural features of the face. Instead of a traditional 2D face image, the 3D face spoofing system works with a three-dimensional face model that contains information about the shape and surface of the face.

The main steps of the 3D face spoofing system include:

1. Capture of a 3D face model: specialized sensors such as 3D facial scanners or stereo cameras can be used to create a 3D facial model to capture geometric information about the face.

2. Texture and geometry analysis of the face: the resulting 3D face model is analyzed for textural and geometric features that may indicate spoofing. For example, the system may look for differences in lighting, texture patterns, or facial depth.

3. Detection of spoofing attacks: the system compares the resulting 3D face model with the base face model representing the user's original data. If significant differences are detected, this may indicate a spoofing attack, and the system takes appropriate measures, such as rejecting the access request.

3D face spoofing systems enhance the security of face recognition systems by preventing forgery and deception. However, they also require more complex and costly hardware infrastructure for capturing three-dimensional face data. In addition, to effectively counter new fraud and spoofing techniques, attack detection algorithms must be continuously developed and improved.

Due to their widespread practical applications, as shown in Figure 1, in security systems, crowd control, forensic analysis and more, face recognition algorithms have generated significant interest and are expected to continue to shape our interaction with technology.

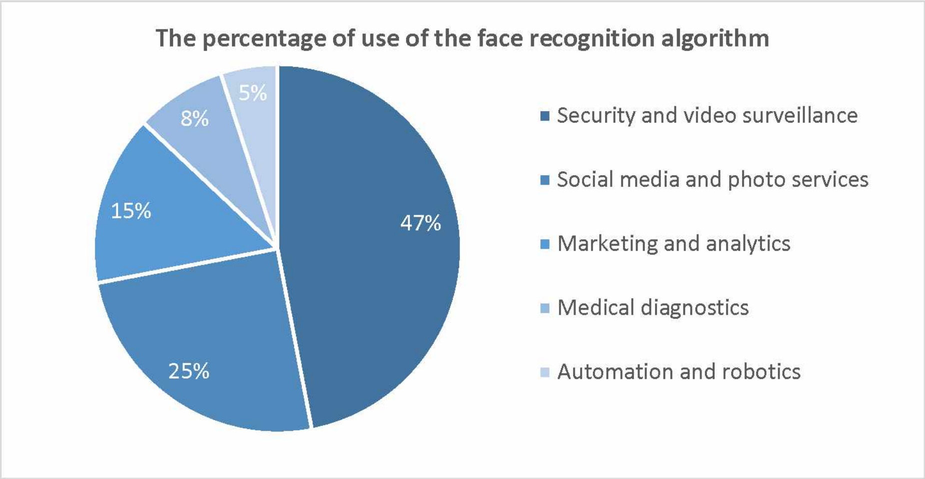

Figure 1 – The percentage of use of the face recognition algorithm

Nowadays, there are several face recognition technologies that are widely used in computer vision. Some of them are as follows:

1. Principal Component Analysis (PCA): PCA is one of the most common face recognition techniques. It extracts principal components from a set of face images and uses them to represent and classify faces.

2. Local Binary Patterns (LBP): LBP uses texture features of a face for recognition; it analyses local texture patterns of pixels around each pixel and applies them to create unique face descriptors.

3. Deep learning methods can be used to extract different classes of features from face images.

4. Descriptor-based methods (SIFT, SURF, etc.) extract key points and descriptors from the face image and can be used for matching and classification.

5. Histogram methods extract histograms of features based on the direction of gradients of pixels in an image. The histograms are used for face classification.

6. Object detection-based methods (e.g. Viola-Jones method) use an object detector to detect faces in an image based on features such as borders and eyes.

In conclusion, it can be stated that the emergence and advancement of face recognition algorithms have revolutionized various aspects of our lives. These technologies offer more convenient and secure means of identification and verification, reducing the reliance on traditional authentication methods. As technology continues to evolve and advances, it is crucial to strike a balance between the benefits these algorithms offer and the ethical considerations related to privacy and data protection. Overall, face recognition algorithms have great potential to improve efficiency, accuracy, and security in a wide range of fields, paving the way for a future where biometric systems play a crucial role in our daily lives.

***References**:*

1. ZOO: Zeroth Order Optimization Based Black box Attacks to Deep Neural Networks without Training Substitute Models / P. Chen [et al.] // AI Sec 17: Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, 2017 – P. 15–26.

2. Fast geometrically perturbed adversarial faces / A. Dabouei [et al.] // IEEE Winter Conference on Applications of Computer Vision (WACV), 2019 – P. 1979-1988.

3. Protecting Personal Privacy against Unauthorized Deep Learning Models / S. Shan [et al.] // Proceedings of USENIX Security Symposium, 2020 – P. 1-16.