Lecture Notes in Networks and Systems 149

Prasant Kumar Pattnaik
Mangal Sain
Ahmed A. Al-Absi
Pardeep Kumar *Editors*

Proceedings of International Conference on Smart Computing and Cyber Security

Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2020)

Springer

Real-Time Access Control System Method Using Face Recognition

Mohammed Abdulhakim Al-Absi, Gabit Tolendiyev, Hoon Jae Lee, and Ahmed Abdulhakim Al-Absi

Abstract Face recognition has been widely studied and studied for many years, but most PC-based face recognition systems have very limited portability and mobility. Face recognition is a process of dynamically capturing facial features through a camera connected to a computer and simultaneously comparing the captured facial features with the facial features previously entered into the personnel library. Face recognition-based person authentication system has been popular among other biometrics recently. This technology can be applied to important departments such as public security, banking, and customs to provide convenient and efficient detection methods. In this paper, we discuss a method of access control system using face recognition technology for entrance limited places. Some face recognition technologies that have shown state-of-the-art performance at their time are discussed. Here we present a method for access control system using facial recognition technology.

Keywords Face recognition · Face verification · Access control · Attendee management

M. A. Al-Absi · G. Tolendiyev
Department of Computer Engineering, Dongseo University, 47 Jurye-ro, Sasang-gu, Busan 47011, Republic of Korea
e-mail: Mohammed.a.absi@gmail.com

G. Tolendiyev
e-mail: tkgabit@gmail.com

H. J. Lee
Division of Information and Communication Engineering, Dongseo University, 47 Jurye-ro, Sasang-gu, Busan 47011, Republic of Korea
e-mail: hjlee@dongseo.ac.kr

A. A. Al-Absi (✉)
Department of Smart Computing, Kyungdong University, Gosung, Gangwon-do, Republic of Korea
e-mail: absiahmed@kduniv.ac.kr

P. K. Pattnaik et al. (eds.), *Proceedings of International Conference on Smart Computing and Cyber Security*, Lecture Notes in Networks and Systems 149,
https://doi.org/10.1007/978-981-15-7990-5_9

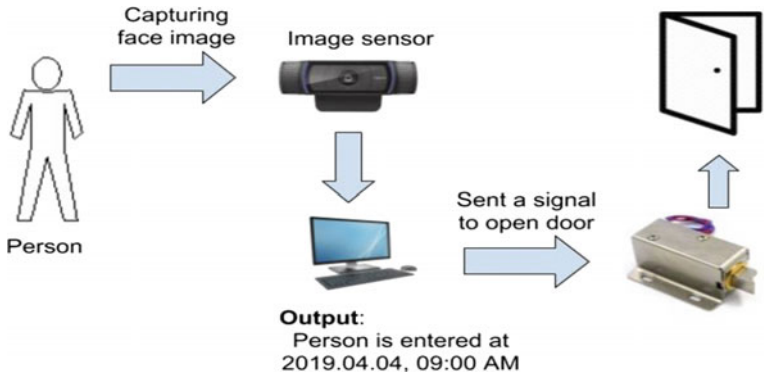

Fig. 1 An illustration of access control system using face recognition

1 Introduction

The research of face recognition technology began in the 1960s. Especially since the 1990s, with the urgent demand of face recognition systems in various industries, a large number of scholars have been engaged in the research of practical face recognition technology.

Recently, facial recognition technology performance has increased thanks to deep convolutional networks. Face recognition is popular than other biometrics such as fingerprint and eye iris recognition. Because it is contactless and non-invasive. We already have experience unlocking phone, verifying payment, and also face recognition access control system being used in the entrance of large-scale event [15] instead of ID card. In near feature, this technique might replace all people who is in charge of verify someone's identity by comparing their actual face appearance with face photography.

Figure 1 depicted an access control system using face recognition. Face recognition identity authentication system is generally authenticated by the client, application system, and face authentication as shown in Fig. 2.

2 Related Works

Face recognition system has been active topic in computer vision and pattern recognition field in last decades. Face recognition is more popular than other biometric systems such as fingerprint, palm vein and eye iris recognition. A big reason of using face recognition is its contactless, non-invasiveness and secureness (Table 1).

Face recognition systems can be classified largely into two types. In case of first type of face recognition, person's intents to be identified by directly looking at the camera and camera are installed in well-conditioned environment for recognition. In

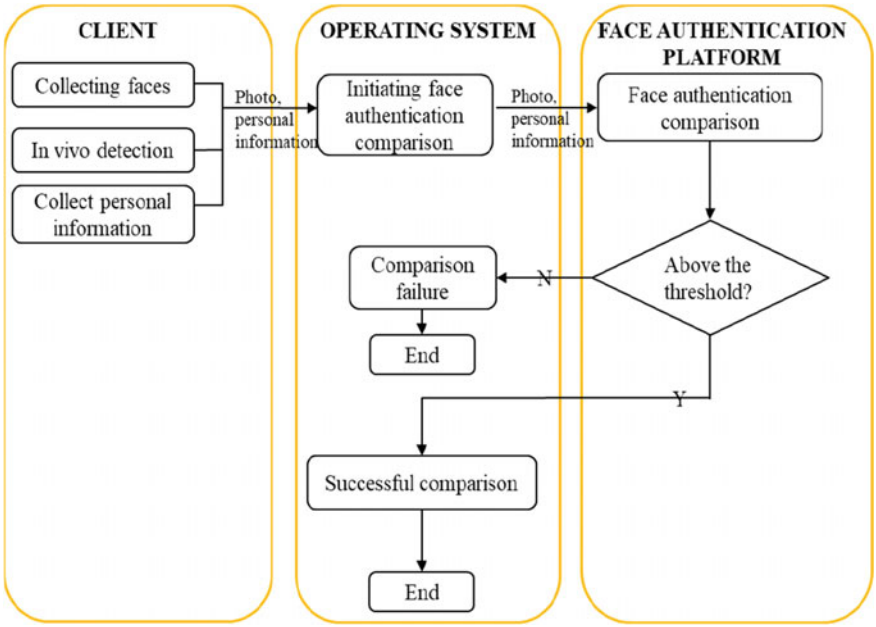

Fig. 2 Face authentication process

Table 1 Comparison of biometric system in term of technical and non-technical weaknesses

Biometric system	Weakness of techniques	Non-technical weakness
Fingerprint	Slow	Contackness
Iris	slow	–
Face recognition	Requires large data to train the model that generalizes well a face image	Contactless, user-friendly

another case, some authorities, e.g., police, security guard intend to try to identify people. In this case, camera might not capture good face image and environment cause difficulties as well. The second case face recognition is more difficult problem to solve than first one.

In face recognition, there are several difficulties:

- Illumination. Less of illumination and direct light effects on image acquiring;
- Pose: persons do not directly look at the camera;
- Occlusion: partial occlusion of face by other objects, i.e., hands;
- Accessories: sunglasses, cap, etc.
- In order to address these problems and achieve better recognition accuracy, many approaches have been proposed:
- Employing large-scale deep CNN containing more than 1.6B parameters.

- Training the model on very huge dataset, i.e., more than 200 M image of 8 M different identities;
- Better loss function then distinguishes two-face images (Contrastive loss [10], triplet loss [11], center loss [12], large margin softmax (L-Softmax) [13], angular softmax (A-Softmax) [14]), and large margin cosine loss [4], and cosine loss [3].

3 Face Recognition System

Face recognition is a technique that identifies a person with his or her facial image by comparing their image stored in database. First of all, we convert cropped face image to 128-dimensional vector. After that measure distance between them. Distance between face images of the same person is less than distance of the face images of the different person. To convert face image to some real number vector, we use convolutional neural networks. This CNN generalizes a face image to vector. To achieve a model that generalizes well a face image to vector, we train the CNN on large data, number of hundreds of million images of million different identities. We can use public available models [1–3] and if necessary, train and build own model on public face datasets [5, 6] and our own data. Popular datasets for testing face verification are Labeled Faces in the Wild (LFW) database, YouTube database (YTD), and MegaFace Challenge.

We developed person authentication system using open-source face recognition model [1]. Figure 2 depicted interface of the system. The system works automatic mode as default without need of any person. However, if it is necessary security person or manager can monitor it. The system also records people enter and exit time, so this can be used as attendee management system as well. One advantage of face recognition to other object identification system is we do not need to train the model for registering a new person. The face recognition model well generalizes a new dataset.

4 Face Verification Method

Euclidean distance calculation similarity is the simplest and most understandable method of all similarity calculation. It takes the items that have been unanimously evaluated as the coordinate axes and then draws the people who participated in the evaluation onto the coordinate system and calculates the linear distance between them. Euclidean distance is the most commonly used distance calculation formula. It measures the absolute distance between points in a multidimensional space. This is a good calculation method when the data is very dense and continuous.

Figure 3 illustrated a method of face verification system. First of all, captured person's face image is cropped, aligned and resized to required size of the CNN, and deep CNN extract face feature, i.e., transforms a face image to 128-dimensional

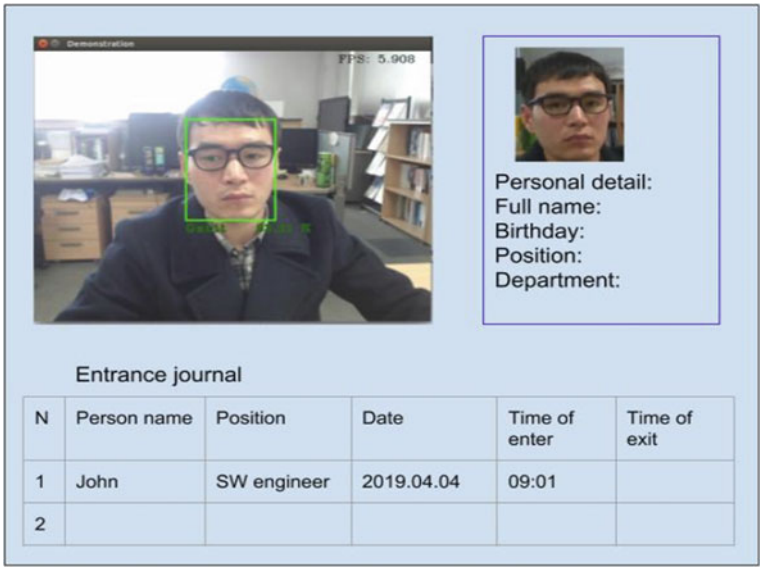

Fig. 3 Interface of the system

vector. After that in order to compare the image with image in database, distance between two vectors of face image is measured. The system makes decision by thresholding distance value, if the distance less than the thresholding value (e.g., 0.3), the system results as the two images of the same person, otherwise different.

When data items A and B are used as points in the graph, the similarity between the two is r distance (A, B), which can be calculated by the Euclidean distance. The formula for calculating the Euclidean distance in n-dimensional space is measured by Eq. (1).

$$r = \text{sqrt}\left(\sum (x_{i1} - y_{i2})^2\right) \text{ where } i = 1, 2, \ldots n$$

$$r(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{1}$$

where x_{i1} represents the i-dimensional coordinate of the first point, and y_{i2} represents the i-dimensional coordinate of the second point. The n-dimensional Euclidean space is a set of points, and each of its points can be expressed as $(x(1), x(2), \ldots x(n))(x(1), x(2), \ldots x(n))$, where $x(i)(i = 1, 2 \ldots n)$ is a real number, called the i-th coordinate of x, the distance $r(x, y)$ between two points x and $(y{=}y(1), y(2), \ldots y(n))$ is defined as the above formula (Fig. 4).

The cosine similarity uses the cosine of the angles of the two vectors in the vector space as the measure of the difference between the two individuals. Compared to

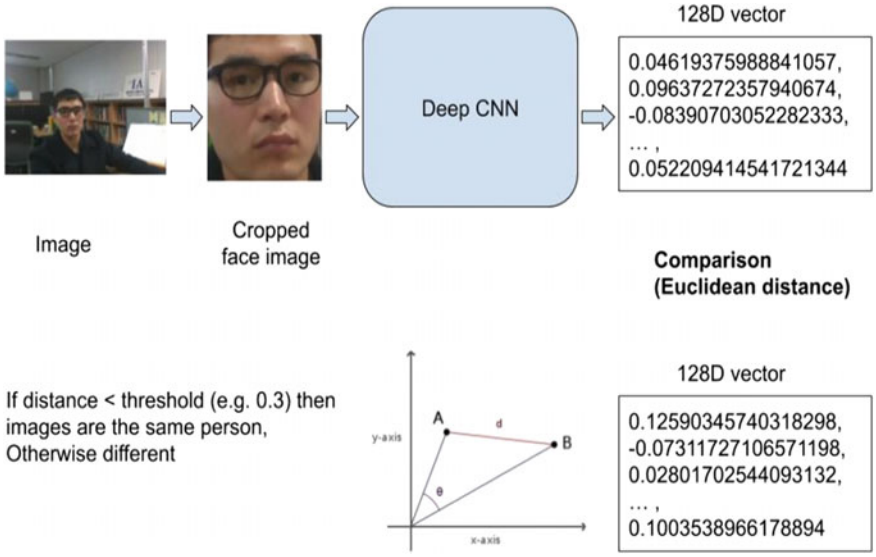

Fig. 4 Face verification method

distance metrics, cosine similarity pays more attention to the difference in direction between two vectors, rather than distance or length. As can be seen from the above figure, the Euclidean distance measures the absolute distance of each point i the space, which is directly related to the position coordinates of each point; and the cosine distance measures the angle between the space vectors, which is more reflected in the direction instead of location. If the position of point *A* is kept unchanged and point *B* is away from the origin of the coordinate axis in the original direction, then the cosine distance remains unchanged at this time(because the angle does not change). The distance between *A* and *B* is points *A* and *B* which is obviously changing, that is the difference between the Euclidean distance and the cosine similarity.

5 Conclusion

Face recognition has been widely studied for many years, but most PC-based face recognition systems have very limited portability and mobility. In special applications such as smart communities, outdoor observation points and personal observation, it is very convenient to use a face recognition system to provide new requirements. Research on face recognition in embedded systems has practical meaning and a wide range of applications. As a point of view, many companies have built-in systems with access control systems based on attendance at this stage, but most are face recognition

systems or PC-based structures, an integrated front face image and display recognition results. The face recognition algorithm is implemented in the computer background. As computer technology advances, embedded systems become an integral part of the computer field, compact microprocessor and built-in operating system to improve performance and become the foundation for the integrated face recognition research system.

This paper studied a person authentication method using facial recognition system. Nowadays, there are publicly available face recognition models such as OpenFace, ArcFace model which engineers can use for their project. Face recognition person authentication system is a powerful security among other biometric system such as fingerprint and iris recognition. Face recognition is also being used in our daily life such as payment verification, door unlock, phone unlock. In the feature, all digital door lock devices might include also face recognition feature. A method of person authentication for access control system of entrance limited places is proposed.

References

1. B. Amos, B. Ludwiczuk, M. Satyanarayanan, *OpenFace: A General-purpose Face Recognition Library with Mobile Applications*. Technical report, CMU-CS-16-118, CMU School of Computer Science (2016)
2. F. Schroff, D. Kalenichenko, J. Philbin, *Facenet: A Unified Embedding for Face Recognition and Clustering*. arXiv preprint arXiv:1503.03832 (2015)
3. J. Deng, J. Guo, S. Zafeiriou, *ArcFace: Additive Angular Margin Loss for Deep Face Recognition*. arXiv:1801.07698 (2018)
4. H. Wang, Y. Wang, Z. Zhou, X. Ji, Z. Li, D. Gong, J. Zhou, W. Liu, Cosface: large margin cosine loss for deep face recognition, in *CVPR* (2018)
5. D. Yi, Z. Lei, S. Liao, S. Z. Li, *Learning Face Representation from Scratch*. arXiv preprint ss (2014)
6. H.-W. Ng, S. Winkler, A data-driven approach to cleaning large face datasets, in *Proceedings of the ICIP* (2014). https://vinstage.winklerbros.net/facescrub.html
7. A. Okumura, T. Hoshino, S. Hada, Yugo Nishiyama, M. Tabuchi, Identity verification of ticket holders at large-scale events using face recognition. J. Inf. Process. **25**, 448–458 (2017)
8. P. Li, C. Cadell, *Chine Eyes 'Black Tech' to Boost Security as Parliament Meets*. (March 10, 2018) Retrieved April 4, 2019 from Technology News from Reuters website: https://www.reuters.com/article/us-china-parliament-surveillance/china-eyes-black-tech-to-boost-security-as-parliament-meets-idUSKBN1GM06M?utm_campaign=trueAnthem:+Trending+Content&utm_content=5aa3f9fd04d30121e40e5e73&utm_medium=trueAnthem&utm_source=twitter
9. G. Fleishman, *Face ID on the iPhone X: Everything you Need to Know About Apple's Facial Recognition*, (2017, December 1) Retrieved December 4, 2017 from the Macworld from IDG website: https://www.macworld.com/article/3225406/iphone-ipad/face-id-iphone-x-faq.html
10. S. Chopra, R. Hadsell, Y. LeCun, Learning a similarity metric discriminatively, with application to face verification, in *Conference on Computer Vision and Pattern Recognition (CVPR)* (2005)
11. E. Hoffer, N. Ailon, Deep metric learning using triplet network, in *International Workshop on Similarity-Based Pattern Recognition* (2015)
12. Y. Wen, K. Zhang, Z. Li, Y. Qiao, A discriminative feature learning approach for deep face recognition, in *European Conference on Computer Vision (ECCV)* (2016), pp. 499–515
13. W. Liu, Y. Wen, Z. Yu, M. Yang, Large-margin softmax loss for convolutional neural networks, in *International Conference on Machine Learning (ICML)* (2016)

14. W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, L. Song, SphereFace: deep hypersphere embedding for face recognition, in *Conference on Computer Vision and Pattern Recognition (CVPR)* (2017)
15. Global Times, *AI, Robots Help Provide Security for SCO Summit in Qingdao*. Retrieved April 4ss, 2019 from Global Times website: https://www.globaltimes.cn/content/1106310.shtmla