ARTIFICIAL INTELLIGENCE BASED METHODS OF IDENTIFICATION AND AUTHENTICATION BY FACE IMAGE

Kamola Erkinovna Saurova
Department of "Information Technologies", Urganch Branch of Tashkent University of Information Technologies Named after Muhammad al-Khwarizmi
kamolaerkinovna@gmail.com

Dilafroz Koshnazarovna Hayitbaeva
Department of "Information Technologies", Urganch Branch of Tashkent University of information Technologies Named after Muhammad al-Khwarizmi
dilafrozhayitbayeva@gmail.com

ABSTRACT

A facial recognition system is a technology that can match a human face from a digital image or video frame to a database of faces. Such a system is typically used to authenticate users through identity verification services and works by accurately defining and measuring facial features from a given image. In the 1960s, development began on similar systems, which began as a form of computer application. Since its inception, facial recognition systems have recently become more widely used in smartphones and other forms of technology such as robotics. This paper explores the classical and artificial intelligence-based methods of face image identification and authentication, identifies the existing barriers to face recognition, and presents several methods to overcome them. The article proposes several methods for building a facial image-based authentication system and improving its effectiveness. Methods such as artificial neural networks, machine learning algorithms, etc. are widely used in the construction of the proposed system. The created system helps to improve the efficiency of biometric authentication systems based on facial images.

Keywords: facial recognition, authentication, identification, artificial intelligence, machine learning.

INTRODUCTION

Facial recognition systems are used by governments and private companies around the world today. Their effectiveness varies, and some systems have previously been abandoned due to ineffectiveness. The use of facial recognition systems has also sparked controversy, with claims that the systems violate citizens' privacy, commonly misidentify,

encourage gender norms and racial profiling, and fail to protect sensitive biometric data [1]. The emergence of fake media such as Deepfakes has also raised concerns about its security. These claims have led to bans on facial recognition systems in several cities in the United States. Growing social concerns led social networking company Meta Platforms to shut down Facebook's facial recognition system in 2021, deleting the face scan data of more than a billion users. This change is one of the biggest changes in the use of facial recognition in the history of technology [2].

Because computerized facial recognition involves measuring a person's physiological characteristics, facial recognition systems are classified as biometric. Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely used due to the contactless process. Facial recognition systems have been used in advanced human-computer interaction, video surveillance, and automatic image indexing [3].

LITERATURE ANALYSIS AND METHODOLOGY

Facial recognition is a family of biometric software that maps a person's facial features and stores the data as a facial copy. The software uses deep learning algorithms to verify an identity by comparing a live captured image with a stored facial print. Image processing and machine learning are the backbone of this technology. Due to human activity found in various security applications such as airport, crime detection, face tracking, forensics, etc., facial recognition has received much attention from researchers [4]. The relevance of research in this direction is confirmed by many works of Russian and foreign scientists. The study of various aspects of facial biometrics problems is devoted to the researches of G.A. Kukhareva, I.N.Spiridonova, O.S.Ushmayeva, P.Viola, M.J.Jones, Anil K.Jain, A.Ross, D.Zhan and other foreign scientists. However, the problem of recognizing and confirming the authenticity of the authentication object has not been fully resolved [5].

Volkova Svetlana Sergeevna studied the following in her dissertation entitled "Methods for improving the efficiency of biometric authentication systems for users of information systems based on facial images".

1. A method to improve the accuracy of authentication by improving the sub-system of facial image recognition and processing.

2. A method of increasing the accuracy of authentication by using several images of a person, a method of grouping people's faces in a video stream, a method of optimal selection of the required number of images.

3. Methodology for assessing the accuracy of localization of control points of the face.

4. Methods of combating fraud attacks that allow to increase the resistance of biometric systems of user authentication to spoofing attacks based on facial images in the biometric data entry module [6].

Detecting facial liveliness using artificial intelligence techniques: In this paper, researchers Smita Khairnar, Shilpa Gite, Ketan Kotecha, and Sudeep D. Thepade conducted a systematic review using the PRISMA approach by exploring the most relevant electronic databases. Conceptual analysis examined data from selected articles. The study discusses face spoofing attacks, various feature extraction strategies, and artificial intelligence approaches to facial liveliness detection. The study discusses artificial intelligence-based methods, including Machine Learning and Deep Learning algorithms used to detect the liveliness of a face [7].

Challenges of Face Image Authentication and Suggested Solutions: In this article, researchers Zahraa Aqeel Salih, Rasha Thabit, Khamis A. Zidan, and Bee Ee Khoo provide a brief review of facial image manipulation techniques and their detection, followed by methods for detecting manipulation that may be encountered provided a summary of the limitations and challenges. Next, the paper presents some suggestions that may be considered for future research on this interesting and intriguing research topic [8].

RESULTS

Image processing and machine learning are the backbone of this technology. Compared to other biometrics like iris, fingerprint, etc., facial biometrics may not be bothersome. Facial recognition involves capturing facial images from a video or surveillance camera [9]. They are compared to the stored database. Face recognition involves training certain images, classifying them with certain classes, and then storing them in a database. When a test image is given to the system, it is classified and compared with the stored database.

Image processing and machine learning. Image processing by computers includes the process of Computer Vision. It deals with high-level understanding of digital images or videos. The requirement is to automate tasks that human visual systems can do. So a computer should be able to recognize things like a human face or even a statue. The computer reads any image as a range of values from 0 to 255. There are 3 primary colors for any color image - red, green and blue. A matrix is created for each primary color and these matrices are then combined to provide pixel values for the R, G, B colors. Each element of the matrix provides information about the intensity of pixel brightness [10].

Machine learning. Every machine learning algorithm takes a set of data as input and learns from the data, which basically

means that the algorithm learns from the input and output provided as data. It detects patterns in the data and provides the required algorithm. For example, several things can be considered as patterns to determine whose face is in a given picture: [11].

• Face height and width - Height and width may not be reliable because the image can be resized to a smaller face or grid. However, even after resizing, the proportions that remain unchanged are the ratio of the height of the face and the width of the face.

• Face color;

• Width of other parts of the face like lips, nose, etc.

There is a pattern - different faces have different sizes as above. Similar faces have similar sizes. Machine learning algorithms only understand numbers, so it's very difficult. This digital representation of a "face" (or an element in the training set) is called a feature vector. A feature vector consists of different numbers in a certain order [12].

Machine learning serves three main functions in facial recognition technology. These are listed below: [13].

1. Feature vector extraction: It is difficult to enumerate all the features manually because there are so many of them. A machine learning algorithm can intelligently define many such features. For example, a complex feature can be the ratio of the height of the nose to the width of the forehead.

2. Matching Algorithms: After the feature vectors are obtained, the machine learning algorithm must match the new image with the set of feature vectors available in the corpus.

3. Facial recognition operations: Technology systems can vary when it comes to facial recognition. Different software uses different methods and tools for facial recognition. The step-by-step method is as follows:

Face detection: To begin with, the camera detects and recognizes a face. Face detection works best when a person is looking directly at the camera, as this makes it easier to recognize the face. As technology advances, this improves to where a face can be detected with only slight changes in the position of the face facing the camera.

Many quality cameras are recommended for both recording and identification. In face studies, it is recommended that the distance between the two eyes of a face in a video or image is 50 pixels, 75 pixels and more for very good face recognition systems. This distance should be natural, that is, the size of the image should be reduced. The minimum image size for image recognition and registration is 640x480 pixels. Images of this size can be taken using a web camera or smartphone without affecting the quality [14].

Facial analysis: A picture of the face is then taken and analyzed. Many people rely on 2D images rather than the familiar 3D face recognition because it is easier to match the database. Facial recognition software analyzes the distance between your eyes or the shape of your cheekbones [15].

Convert image to data: Now it is converted into a mathematical formula and these facial features are converted into numbers. This digital code is a known face print. Just as each person has a unique fingerprint, they also have a unique facial imprint.

Matching: The code is then compared to another database of face prints. This database contains photos with comparable identification. The technology then determines the match for your specific characteristics in the provided database. It comes back with matching and attached information such as names and addresses, or depending on the information stored in the person's database.

Checking face images for reflection. The process may fail if face detection is performed using mirrored images, but face detection succeeds when using non-reflected images. Many cameras and devices are configured to capture reflected images that are used during registration and identification. Considering that all images can be natural or reflected, it is important to check face images for reflections [16].

Based on the conclusions, knowledge, concepts and analysis obtained above, the article presents the process of building a facial image recognition system software tool. Neural networks, machine learning algorithms and several software tools are used in the construction of the proposed face recognition system software. Below is information about one of the important components, the Resnet50 neural network.

Image classification is a method of digitally extracting image class information. In short, it was used to classify images. Image classification can be supervised (each image is labeled) or unsupervised. As mentioned above, this article uses Resnet50 layers, one of the CNN architectures. In summary, the CNN flow is as follows:

- Convolution layer (extraction feature with filtering)
- Steps (moving pixels over the input matrix)
- Filling
- Rectified linear unit (RelU) (linear to network (insert absence)
- Fill layer (reduce the number of parameters)
- Fully connected layer (align the matrix to a vector and make it fully send to the connected neural network layer.)

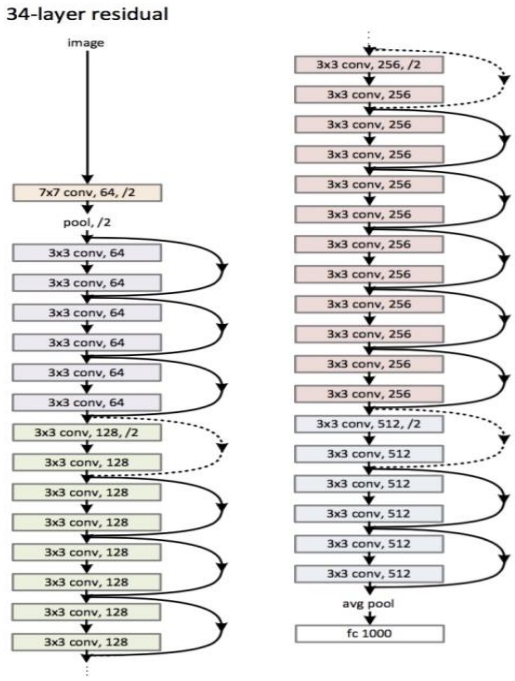

Figure 1. Resnet50 architecture with 34 layers of residuals

Machine learning algorithms ML.NET were used in the construction of the facial image recognition system software tool proposed in the article. The working process of the facial image detection software package is as follows: more than 20 state images of facial images of two different classes are entered into the program, the program identifies these selected facial images using 2 different features and displays the obtained result, i.e., the degree of compatibility and accuracy of the facial images.

DISCUSSION

The use of artificial intelligence-based systems and the Computer Vision process in the analysis of facial images helps to prevent errors in image recognition and eliminate existing shortcomings. As a result of several articles studied and analyzed, attention is paid to the study and analysis of ways to improve the effectiveness of biometric authentication systems for users of information systems based on facial images. Also, several methods were proposed to build a facial image-based authentication system and improve its effectiveness.

CONCLUSION

At the end of the article, based on the conclusions, concepts, and analysis, the existing problems and shortcomings in the identification of face images were identified, and several recommendations were made to eliminate these problems. Also, as a result of research, it was possible to

increase the effectiveness of biometric authentication systems in recognizing facial images. To do this, it was proposed to create a software tool using neural networks and machine learning algorithms. The created system helps to improve the efficiency of biometric authentication systems based on facial images.

REFERENCES

1. “Face Recognition based Smart Attendance System Using IoT” (PDF). International Research Journal of Engineering and Technology. 9 (3): 5. March 2022.
2. Wiggers, Kyle (March 5, 2022). “Study warns deeepfakes can fool facial recognition”. VentureBeat. Retrieved June 4, 2022.
3. Chen, S.K; Chang, Y.H (2014). 2014 International Conference on Artificial Intelligence and Software Engineering (AISE2014). DEStech Publications, Inc. p. 21. ISBN 9781605951508
4. Himanshu Srivastava, “A Comparison Based Study on Biometrics for Human Recognition”, IOSR Journal of Computer Engineering (IOSR-JCE), vol. 15, pp.22-29, 2013.
5. Viola, Paul, and Michael J. Jones. "Robust real-time face detection." International journal of computer vision 57.2 (2004): 137-154.
6. Волкова Светлана Сергеевна, Методы повышения эффективности систем биометрической аутентификации пользователей информационных систем по изображению лица. Диссертация. Санкт-Петербург-2017.
7. Face liveness detection using artificial intelligence techniques: a systematic literature review and future directions: Smita Khairnar, Shilpa Gite, Ketan Kotecha, and Sudeep D. Thepade. Bid data and Cognitive Computing (February 2023).
8. Challenges of Face Image Authentication and Suggested Solutions: Zahraa Aqeel Salih, Rasha Thabit, Khamis A. Zidan, and Bee Ee Khoo. International Conference on Information Technology Systems and Innovation (ICITSI)
Bandung, November 8-9, 2022
9. Simon Llu and Mark Silverman, “A practical guide to biometric security technology,” IT Pro, 2001.
10. Heisele, Bernd, Tomaso Poggio, and Massimiliano Pontil. "Face detection in still gray images." (2000).
11. X. S. Kuzibayev, T.Q. Urazmatov MapReduce and Apache spark: technology analysis, advantages and disadvantages Journal of Physics: Conference Series, 2022
12. Rubal Jain, Chander Kant. Attacks on Biometric Systems: An Overview. International Journal of Advances in Scientific Research 2015;
1(07): 283-288. 10.7439/ijasr.

13. B.Zhou, Z. Xie, F. Ye, Multi-modal face authentication using deep visual and acoustic features, in 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1-6..
14. E. Pagnin, A. Mitrokotsa, Privacy-preserving biometric authentication: challenges and directions, Secur. Commun. Netw. 2017 (2017).
15. V. Matyáš, Z. Ríha, Biometric authentication—security and usability, in: Advanced Communications and Multimedia Security, Springer, 2002, pp. 227–239.
16. O.Djumanazarov, A. Väänänen, K. Haataja, P.Toivanen, "An overview of IoT-based architecture model for Smart Home Systems" 21st International Conference on Intelligent Systems Design and Applications. December 13-15, 2021.ISSN 2367-3370, https://doi.org/10.1007/978-3-030-96308-8_65
17. N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40 (3) (2001) 614–634.
18. J.S. Arteaga-Falconi, H. Al Osman, A. El Saddik, ECG and fin-gerprint bimodal authentication, Sustainable Cities Soc. 40 (2018) 274–283.