ISSN: 2710-0170 DOI: 10.29561/FHSS.202111_1(8).0003

National Security Analysis of Face Recognition Technology

Yulong Xing

Yiwu Institute of Northwest University of Political Science and Law, Yiwu, China

Abstract

Face as a unique biological information, coupled with certain data acquisition, operation processing ability and the corresponding database, in all kinds of social activities has a rich application scenarios. After several generations of changes, face recognition technology has been widely used in identity recognition, trajectory recognition and other fields with powerful data acquisition and processing capabilities. However, face recognition technology to meet people's various needs at the same time, but also some people with ulterior motives as other way, to the normal social order has brought a certain impact. Similarly, the misuse of facial recognition technology, under certain circumstances, can also pose a huge risk to national security.

Keywords

Security; Face Recognition; Data Analysis.

1. Introduction

Upholding an overall national security concept is an important part of Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era. The 19th National Congress of the Communist Party of China made it clear that upholding the overall concept of national security was included in the basic strategy for upholding and developing socialism with Chinese characteristics in the new era, and made an overall plan for improving the system of national security and strengthening national security capacity building. With the increasing importance of data in various fields, data risks and data security issues are becoming more and more prominent, bringing unprecedented challenges to human beings and society. In this context, data protection and governance are not only related to the development, utilization and security of data itself as an important factor of production, but also closely related to national sovereignty, national security, social order and public interests. Therefore, it is necessary to strictly regulate the application of face recognition technology in accordance with the requirements of the overall national security concept.

2. Introduction to Face Recognition Technology

2.1. Ace Recognition Technology Definition, Characteristics

National standard "Information security technology technical requirements for remote face recognition System" (GB/T 38671-2020) of face recognition is defined as: "to identify the individual identity as a person's facial features of an individual biometric identification method. It generates sample feature sequence by analyzing and extracting user face image digital features, and compares the sample feature sequence with the stored template feature sequence to identify user identity." Face information is a kind of biometric information, different faces have different features, technical personnel use deep neural network based on face database learning, automatically summed up the most suitable for computer understanding and distinguishing face features. Each face can be represented as a coordinate, that is, a point in the feature space, and the same person's face in different photos is very close to each other in the feature space. Technical aspects of face recognition mainly refers to the collection and analysis of images, mainly involving optical imaging technology and the corresponding image processing technology, which involves the content of algorithm model construction, and has certain requirements for computer computing power. as a facial information collection technology, compared with other biological information collection technologies, it has the main characteristics of non-mandatory, non-contact, concurrent, basic and large internal capacity. Non-mandatory refers to the user does not need to specially cooperate with the face acquisition equipment, almost can obtain face images in an unconscious state, such sampling method is not "mandatory"; Non-contact refers to the user does not need to directly contact with the device can obtain face images; Concurrency refers to the sorting, judgment and recognition of multiple faces in practical application scenarios. Large volume refers to the fact that a single face recognition device can collect all the past facial information within its coverage area. In addition, it also has the characteristics of fast, hidden, users only need to set up a small imaging equipment, with background data processing equipment can easily obtain their face information without the knowledge of the parties.

2.2. Face Recognition Technology Application Basis

The core feature of face recognition technology is that it can provide mature early data for the follow-up activities of the main body. These mature basic biological information data, with specific databases, will have rich application scenarios. In different dynamic scenes, facial feature information of individuals can be automatically detected and positioned, tracked and collected, compared and extracted, separated and stored, and the identity of natural persons can be confirmed by verifying with the registered face in the database, or the complete process of searching in the database for the existence of the designated portrait. At present, from entry and exit identification, illegal behavior exposure to identity verification in criminal cases, from direct bank face recognition customer identity verification, 3D face recognition to unlock smart phones to mobile face payment face recognition applications are more and more widely. Face recognition system using massive data mining and neural network technology has become a new field of artificial intelligence and blockchain business applications. China supports the construction of an online identity authentication system based on facial recognition and other recognition technologies, according to a draft guideline on Promoting the development of the Cybersecurity Industry released by the Ministry of Industry and Information Technology on September 27, 2019. It should be noted that personal biometric information needs to be combined with a specific database to be of real value. Database based on the main body, purpose difference, each has its own strengths, such as the public security machine to household identity data as the basis, through face recognition technology to obtain the facial information of the object to check, can accurately verify the identity of the parties; The smart phone can unlock the user's face accurately by storing the user's face information as data. Based on the facial information collected by all visitors, the sales department can accurately identify customers visiting for the first time to achieve accurate marketing.

Face recognition technology, in essence, is a unique collection and analysis of biological information technology, today's social data is the most extensive way to store such information, biological information is basically the essence of biological information storage carrier, that is, the abuse of data.

3. The National Security Risks of Face Recognition Technology

Big data era, single face recognition (body) the individual facial biological information collected is likely to be huge, through the treatment for these information, can again mining capacity is huge, by analyzing the mass data processing, can provide all kinds of activities based on different purposes with a variety of data to support. Once these data are used to endanger national security, it will cause great damage to national security. The security risk of face recognition technology is mainly reflected in two aspects: technical risk and application risk. Technical risk refers to the risk caused by technical defects. The core performance is the identification error, algorithm discrimination and vulnerability to hacker attacks caused by algorithm errors (flaws). Application risks refer to the risks of data collection, use, and leakage during application. Specifically reflected in the national security level, involving the following aspects:

3.1. Uncontrolled Information Leakage

From the Angle of information leakage analysis, mainly including illegal collection of information, existing information leakage.

3.1.1. Illegal Collection of Information

Illegal collection of information refers to face recognition technology users against the will of the collection of relevant information. From the categories of information collection devices, there are mainly two cases, one is the use of mobile devices to illegally collect user face information, the other is through fixed devices to illegally collect face information. For example, all kinds of mobile application service providers collect users' facial information without informing users and obtaining users' consent based on specific purposes; In order to gain additional competitive advantages, various operators obtain customers' facial information in a hidden way through fixed devices. After being collected, such information may be used to obtain additional commercial benefits, or to commit crimes against the law, as well as crimes against national security. According to media reports, thousands of pictures containing face information can be bought on online platforms only for a few yuan. Once these pictures are used by criminals, they will pose a huge risk.

The illegal collection of information is relative to the legal collection of information. The "illegal" criterion in this paper is mainly based on the "harm to national security", which may involve the relevant provisions of the Criminal Law and the National Security Law. Specifically, refers to the actor based on the purpose of engaging in the above behavior, in order to achieve specific criminal behavior, and face information collection, analysis activities. For example, based on the purpose of promoting terrorism and extremism to specific subjects, face information is collected in specific areas to analyze the behavior and activity track of specific subjects and then analyze their willingness to engage in related activities, screen suitable candidates, so as to achieve targeted and accurate publicity. Although this type of collection has not been implemented on specific charges, similar collection models exist, such as the sales department to collect customers' facial information for accurate promotion.

3.1.2. Leakage of Existing Information

It mainly includes hacking attacks caused by technical problems, collection and leakage based on illegal purposes in the application process. In the information age, individual information has been collected many times in different scenarios, and the leakage of the existing information can still have a huge impact on national security. In particular, the technical threshold of the face recognition system provided by the providers of different face recognition schemes on the market is uneven, and the applicable standards are also different. Data is stored in different ways. Some are directly stored in the customer's own storage media, lacking necessary data protection measures. Some are uploaded over the network to storage media provided by service providers, but the firewall specifications are lower. These existing data can easily be obtained by a third party through technical means, resulting in information leakage.

3.2. The Abuse of Face Recognition Technology

From the perspective of misuse of face recognition technology, the main package is used for security crimes, to provide support for other crimes. Face recognition may be used for improper purposes, such as in the preparatory stage of the crime, through face recognition technology to analyze the law of the activity of the object of the crime; Choose the best place to commit the crime; Plan the best escape route, etc. These application scenarios may seem fanciful, but they have practical value.

4. Regulation Strategy

4.1. Restricting the Behavior of Data Holders

Holders of large amounts of data based on technological and scale advantages should be severely limited. The first is to limit its right to obtain new data unnecessarily, avoiding unnecessary expansion of the existing data scale. Secondly, it restricts the excessive exploitation and use of existing data and sticks to the minimization principle of data acquisition and analysis. Finally, it is necessary to strengthen its data security obligation and take necessary measures to ensure data security.

4.2. Standardizing Data Transactions

Data is the basis of all analytical processing, and measures should be taken to ensure that data is sold without need. First, it is necessary to standardize the collection of data, so that the information collected is informed and voluntary. For potential data transactions, the data collected should be fully aware. Second, for the collected data, the collector should have sufficient capacity to ensure the safety and stability of the data and ensure that the data will not be passively transferred. Third, measures should be taken to strictly crack down on all kinds of illegal acts against data and ensure the security of citizens' personal information.

4.3. Try Diversified Data Protection Measures

The multi-attribute of the legal interests of personal biological information covers the protection of privacy rights, personality rights, property rights and security legal interests, and determines the multi-value of its reasonable use and right protection. Therefore, in the process of their protection, we should try to protect them from industry regulation, civil, criminal and other aspects of diversification.

References

[1] Security Problems facing large-scale application of face recognition [J]. China Public Security. 2017 (05).

[2] Personal information protection in face recognition technology -- Also on the construction of dynamic consent mode [J]. Shi Jiayou, Liu Siqi. Financial and Economic Law. 2021(02).

[3] Research on Face Recognition Based on Deep Learning [J]. Wang Yanping, Lu Xin, Zhao Yu-dan.

[4] Liu Rong. Journal of Anhui Police Professional College. 2021(02).

[5] Research on legal Regulation of face recognition Technology [J]. Liu Rong, Ding Zhao-zeng. 2021 (09).