Face Recognition Technology Risks and Regulatory Issues

Yuying Bao[1a], Zhenyuan Du[1b, *]

[1]*School of Health Economics and Management, NJUTCM, 136 Xianlin Avenue, Nanjing, Jiangsu, CHINA;*
[2]*School of Medical Humanities, NJUTCM, 136 Xianlin Avenue, Nanjing, Jiangsu,CHINA;*
[*]*Corresponding author*
{Yuying Bao, zhenyuan Du} yuyingbao@njutcm.edu.com, newde5@126.com

Abstract:
Face recognition technology has the characteristics of convenient attributes, no compulsion, no contact, etc.. Due to the defects of face recognition Algorithms, the similarity of face features, and the risks of unauthorized access and circumvention of authentication caused by face synthesis, which brings the issues of rationality, security, privacy protection and informed consent. It is necessary to strengthen the supervision of face recognition technology, clarify the authority and boundary of the collection and use of face recognition technology, and strengthen the restriction and sanction of legal norms.

Keywords: *face recognition, technical ethics, regulatory strategies*

1 INTRODUCTION

Face recognition is a biometric technology based on facial features. It has the characteristics of convenience, non-mandatory and non-contact, but there are also technical risks. The existing risk research field mainly starts from the improvement of technical security. The technology is not only a technical security issue, but also raises ethical and legal system issues in terms of rationality, security, privacy protection, and informed consent. Therefore, it is necessary to discuss the ethical and legal issues arising from this in combination with technical risks. This paper improves the supervision system of face recognition technology and the legal system that clarifies the access, use rights and restrictions of face recognition technology, which has great practical significance.

2 THE RISK OF FACE RECOGNITION TECHNOLOGY

2.1 Characterization

Face recognition technology uses a common camera as the sensor of information, and uses the "facial pattern encoding" method of identification, which is more convenient and faster than the original password and fingerprint identification in the collection and use of information. Face recognition technology also has non-compulsory, non-contact characteristics: face facial features have the characteristics of openness, intuitiveness, uniqueness and unchangeability, so that face recognition and identification can be accomplished non-compulsively and non-contactly, without the consent of the identified person for identification.

2.2 Technical risks of face recognition technology

The procedure of face recognition is divided into three steps: firstly, the staff collects the face file of the relevant user, or forms the user's photo into a face file and stores it to establish a face file of the face. The next step is to capture the current human face with the camera. Finally, the captured portraits are identified and compared with the faces in the face profile. The technology has some of its technology-specific security risk pitfalls, such as algorithm flaws, face feature similarity, face synthesis and other situations that trigger authentication bypass risks, which can lead to risks such as unauthorized access and customer information leakage [2].

B. Fox et al. (Eds.): IC-ICAIE 2022, AHCS 9, pp. 652-656, 2023.
https://doi.org/10.2991/978-94-6463-040-4_99

2.2.1 Authentication triggered by algorithm flaws

Defect of face recognition algorithm bypassing risk are mainly reflected in the live detection, face comparison and algorithm SDK sections, as shown in Figure 1. Attackers use photos, videos, simulated molds and prosthesis vulnerabilities to bypass face recognition. Face recognition is also affected by various factors such as lighting conditions and face coverings, and there is a risk that unauthorized personnel can successfully bypass face recognition algorithm authentication.

2.2.2 Authentication bypass risk caused by similar facial features

When the face is heavily obscured, or at different viewing angles, the algorithm cannot accurately identify the face position and locate the key points of the five senses.

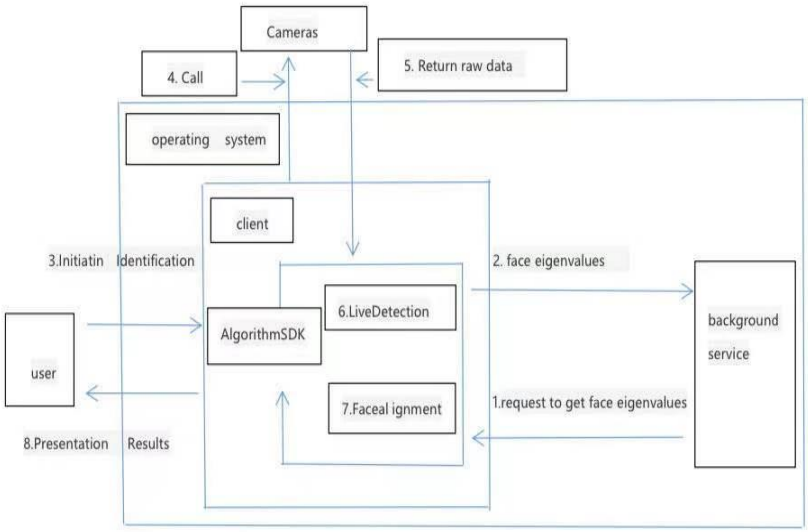

Figure1: flow chart of face recognition technology

When the number of face feature values detected by the face recognition algorithm is small, there may be a defect of similar feature values, which can be exploited by attackers for authentication by pass. As shown in figure 2 [2].

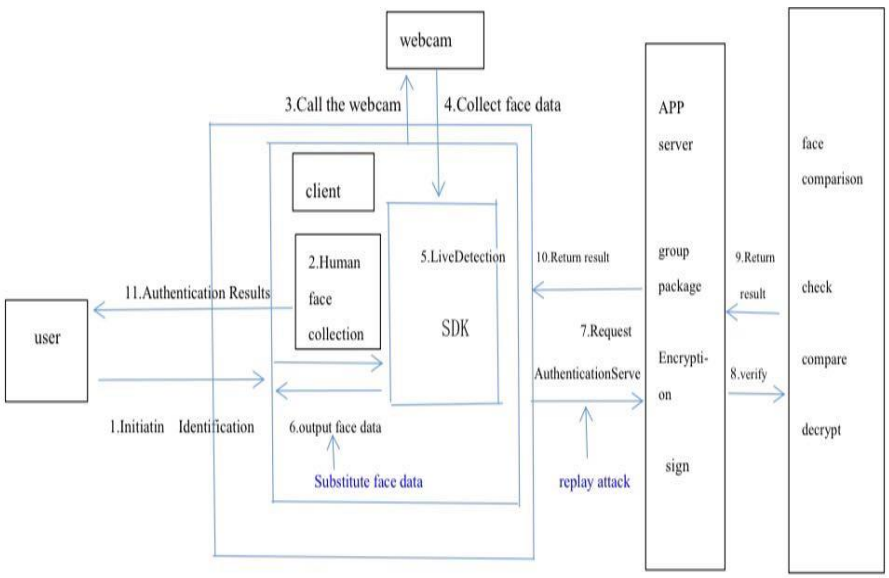

Figure2: Bypassing Face Recognition Using Replay Attack Vulnerability

3 PROBLEMS FACED BY FACE RECOGNITION TECHNOLOGY

3.1 The technical reasonableness of the "electric curtain" dilemma and the disregard for the right to informed consent

The modern science and technology represented by the face recognition system has triggered a profound reflection and serious challenge to the way of existence and life of human beings, which can be called the "electric curtain" problem. When face recognition technology is used to obtain the personal information of ordinary citizens, and it is continuously gathered in the hands of huge organizations, combined with the personal privacy information such as name, gender, ID number, hobbies, home address, love and marriage status leaked in the Internet, the problem of subjectivity crisis under the bombardment of "electric curtain" is bound to arise. The problem of subjectivity crisis under the bombardment of "electric curtain" is bound to arise [4].

The artificial intelligence ethics research group of Southern Metropolis Daily investigated ten types of face recognition scenarios (payment transfer, account opening and cancellation, real-name registration, unlocking and decryption, face-changing entertainment, government affairs, traffic safety, access control and attendance, campus/online education and public safety supervision), more than 20,000 anonymous questionnaires were recovered. The research group set up a scale question in the questionnaire, and asked the respondents to score according to their own experience, with 1 being the lowest and 5 being the highest. The results show that in terms of security perception, the scores given by the respondents are obviously low, only the traffic security check scene has an average score of more than 4 points, which reflects the anxiety of the respondents about the security risks of face recognition. 64.39% of the respondents believed that Facial recognition technology has a tendency to be abused. The most unacceptable scenario for respondents is "some shopping malls will use face recognition technology to collect customer behavior and purchase methods" (42.68%), followed by "some colleges and universities use face recognition technology to collect student head-up rates and classrooms posture" (28.36%), "applications based on face image analysis, such as personality judgment, health condition prediction, etc.".(19.01%).Relatively speaking, respondents are more accepting of face recognition applications based on security scenarios.

Lack of personal autonomy due to disregard for informed consent. Informed consent, also known as an informed commitment or commitment, emphasizes the need to respect the dignity, integrity and freedom of a person as a subject who can freely choose actions involving him or her. In public places, such as subways, airports, hotels and other places, as well as institutions that use facial recognition to obtain facial recognition information, they do not provide the public with the right and freedom of choice, and do not inform the public of the necessity and feasibility of facial recognition. There is also no fundamental commitment to secrecy and responsibility for leaks. Even if commercial organizations induce people to use face recognition "voluntarily" with little profit or convenience, safety and other factors, it is difficult to form effective user informed consent, because most of them have the problem of insufficient information disclosure, so it is impossible to determine the reasonableness of its use.

3.2 Technical security challenges arising from privacy protection and personal information data leakage

Privacy is one of the basic human rights of modern society. The reason why the law protects personal privacy and residential freedom is to allow individuals to have autonomous space, which is not allowed to be invaded by others. Many organizations now obtain the public's extremely private biological information through different channels. Once the privacy is leaked, the potential biological harm and damage to commercial interests are particularly worrying and anxious for the public. Individuals should have a legitimate legal right to oppose the arbitrary access to their biological data by others. Others here, not only refer to other individuals or general organizations, but also include governments and countries.

While face recognition brings convenience to the public and users, its risks cannot be underestimated. Intelligent data has become the second body of human beings [3]. Through the processing of big data, relevant information can be arranged, integrated and summarized, can be automatically analyzed to obtain customer privacy information, accurately delineate personal information database. Face recognition technology is generally contracted to a third party to collect and run the information stored in the third party, before the collection, there is no malicious use and theft of the relevant audit and proof. There are big technical risks, such as in the business sector, companies use face recognition technology to target specific consumer groups, for their development of products and services to find business opportunities.

4 SUPERVISION STRATEGY OF FACE RECOGNITION TECHNOLOGY

4.1 Clarify the authority and boundary of face recognition technology acquisition and use

Face recognition is being used more and more widely, but there is no specific law to regulate its authority and boundaries. The lack of authority regulations and supervision, on the one hand, brings extreme anxiety and anxiety to the public, and also lays the groundwork for future financial risks and various crimes. If we cannot build a "safety" information protection mechanism equivalent to the "convenience" of face recognition, it is equivalent to exchanging personal privacy for the convenience of life.

Facial recognition technology involves the collection of biological data that is important to an individual, and the relevant organization or institution must prove the legality of this practice before collecting it. If the government is the subject of collection, it needs to be explicitly authorized by law. If it is done by enterprises or other institutions, the collection of personal biological data requires the explicit consent of the person to be collected; the collection of information without informed consent is an act of illegally obtaining personal information of citizens.

4.2 Strengthen the constraints and sanctions of legal norms

Article 37 of the Constitution of the People's Republic of China clearly stipulates that the collection of ordinary personal information must obtain the prior consent of the person to be collected: ordinary personal information, including addresses, phone numbers, email addresses, accounts, and whereabouts, etc., must be collected with the prior consent of the person being collected because it is identifiable. At the same time, if the collecting party improperly uses, sells or leaks the corresponding information, it may also lead to legal liabilities including criminal responsibility. The "Information Security Technology Personal Information Security Specification" implemented on October 1, 2020 included personal information, including face recognition information, into personal sensitive information, and clearly stipulated the collection of personal information. Article 1034 of the Civil Code of the People's Republic of China implemented in China on January 1, 2021 stipulates that the personal information of natural persons is protected by law. Article 1035 of the "Civil Code" stipulates that the processing of personal information shall follow the principles of legality, legitimacy, necessity and meet the following conditions: ① Obtain the consent of the natural person or his guardian, but laws and administrative regulations provide otherwise ② The rules for disclosing information processing; ③The purpose, method and scope of information processing are expressly stated; ④It does not violate the provisions of laws, administrative regulations and the agreement of both parties [1].

4.3 Other improvements

4.3.1 Improve the security of facial recognition technology

By improving the algorithm mode of face recognition technology and improving the performance of image and voiceprint recognition, it provides safe protection for the development of face recognition technology. The traditional face recognition system (As shown in figure 3) mainly extracts effective identification information from existing face images or establishes a classifier, and then identifies, compares and determines the identity of the face or uses a trained classifier to perform face ID confirmation. If the real-name authentication service is added to the model, and the authenticity of the certificate and the consistency of the personal certificate are verified in the authentication process, effective identification can be carried out and the identification performance can be improved.

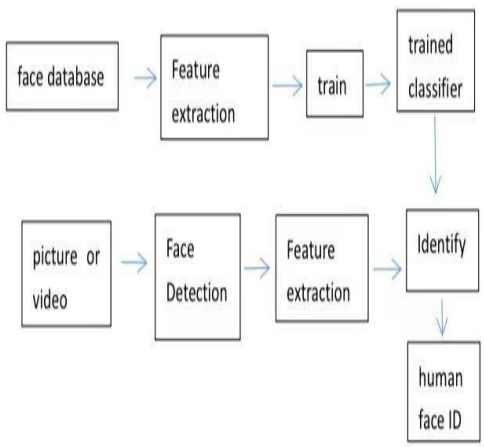

Figure 3: traditional face recognition system

Relying on a series of comprehensive authentication capabilities such as portrait comparison, liveness detection, web pattern comparison, NFC ID card verification, and anti-Hank attack, it realizes the security risk prevention and control capabilities of ID card inspection and personal ID comparison (As shown in figure 4).

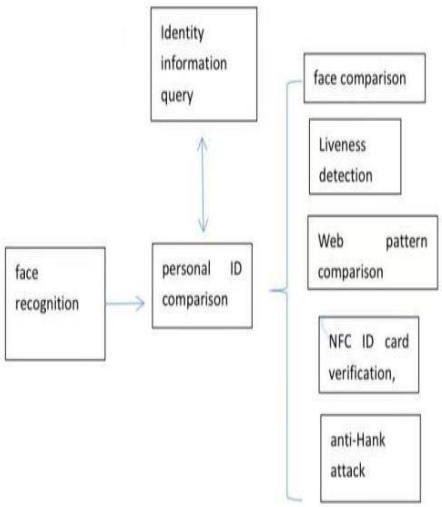

Figure 4: Improved face recognition system

4.3.2 Enhance the public's sensitivity and awareness of participation in the protection of personal information

The personal orientation of biological data is clear and clearly more important to individuals than general personal information. Is the public face, such as personal information provider and facial recognition unlawful infringement behavior potential victims, to face information identification of unreasonable collect said "no", and timely use legal weapons to protect individual legitimate rights and interests of information collection, the user to carry on the effective supervision, jointly create a safe and efficient information society.

5 CONCLUSION

This paper analyzes the risk of abuse of face recognition technology while bringing convenience to the public, and holds that the lack of individual subjectivity and the disregard of informed consent in the use of face recognition technology have led to doubts about the rationality of the technology. The lack of effective protection of privacy and the risk of personal information data leakage lead to technical security challenges. Should clarify the face recognition technology collection, use of authority and boundaries; It is necessary to strengthen the constraints and sanctions of legal norms and establish a matching security defense system for supervision. Enhance the public's sensitivity and awareness of participation in the protection of personal information.

REFERENCES

[1] Hu H. M.and Zhai H. M. (2018) on the privacy protection of biometrics.

[2] Liu Tao and Song Guixiang, (2021) Research and practice of security based on face recognition technology application. Telecommunications Engineering Technology and Standardization, Commun., 34, 40–41.

[3] Robin Li. (2017) *Intelligent Revolution*. CITIC Publishing Group, Beijing,2nd edition.

[4] Wu, Jun. (2016) the Age of Intelligence. CITIC Publishing Group, Beijing,2nd edition.