Research on the Application of the Face Recognition Technology in Cybersecurity and Personal Privacy Protection

Jingbo Yu*

Department of Mathematics and Computer Science, Adelphi University, New York 11530, United States

Abstract: Through a large number of literature surveys, this paper finds that: In the application of face recognition technology, although countries in the world today have established different personal data protection mechanisms, promulgated data security laws and regulations, and many technical prevention measures, there are still a large number of cases of malignant leakage, damage or tampering of corporate and personal data around the world. This shows that there are vulnerabilities in technical preventive measures, industry norms and national laws and regulations policies. Through a large number of investigation and literature research and analysis, this paper puts forward the following views: The application of face recognition technology must be parallel from the three dimensions of technical means, industry standards, laws and regulations, and implement a multi-directional, full-life cycle effective protection of personal privacy information.

Keywords: Face Recognition; Cybersecurity; Privacy Protection; Technical Means; CCPA; GDPR

DOI: 10.57237/j.cst.2024.04.004

1 Introduction

Application and development of face recognition technology.

Face recognition technology has been developed for more than 150 years since the early 1870s. From the beginning, the British court first tried to identify the face by comparing part of the face photo [3]. In recent years, automatic computer processing has been adopted to add artificial neural network algorithm, convolutional neural network algorithm, biometric recognition and other technologies to face recognition technology [2], so that the recognition results have practical recognition rate and recognition speed. Nowadays, "face recognition system" integrates artificial intelligence, machine recognition, machine learning, model theory, expert system, video image processing and other professional technologies, and is widely used in security monitoring, attendance management [2], financial payment [2], campus security, as well as virtual learning and other fields, the future, with the continuous progress of science and technology, Face recognition technology will also be more intelligent and personalized, face recognition technology will be further developed and improved, which brings more convenience and security to people's lives and work.

2 Face Recognition Technology Application Risks and Measures

Face recognition technology is a kind of biometric identification technology that authenticates people's facial

*Corresponding author: Jingbo Yu, jingboyu@mail.adelphi.edu

Received: 7 November 2024; Accepted: 24 December 2024; Published Online: 9 January 2025 http://www.computscitech.com

features. Face recognition technology generally includes: face image acquisition and detection, face feature information extraction, face image processing, and matching with the existing data in the database, so as to verify the real identity of users [5].

The application of facial recognition technology involves information collection, transmission, storage, identification, sharing, transfer, public disclosure, deletion and other information processing links, which contain a large number of personal privacy sensitive information, therefore, face recognition technology is widely used at the same time, personal privacy information leakage risks and cybersecurity risks are also increasing. There are mainly the following risks and countermeasures:

(1) Hardware device security risks - physical attacks [7], side channel attacks [6], hardware Trojan attacks, etc.

Countermeasures: strengthen equipment safety protection; Adopt encryption chip, security start, port encryption and other technical means, adopt electromagnetic shielding, mask technology, noise addition and other technologies to increase the defense capability.

(2) Software security risks - hackers carry out attacks through vulnerabilities in software systems, tamper with information, and steal user privacy information;

Countermeasures:

a. Data transmission and storage encryption

During the transmission and storage process, sensitive personal information is encrypted using a high-intensity algorithm to protect it from being illegally obtained by attackers. HTTPS encryption is used throughout the process [8]. The working principle is as follows: After the original transmission content (plaintext) is transformed by certain rules (by bit or), it is converted into ciphertext for transmission, and then the ciphertext is converted into plaintext, for example:

Suppose, plaintext a = 1234, key =6666,

Then encrypt a ^ key to get the ciphertext b = 7896.

So when you decrypt it, you use b ^ key to get the original plaintext a = 1234.

This is an example of HTTPS simple encryption principle, the actual encryption and decryption process is very complex, and different encryption algorithms can be used, but the basic principle is similar, using this method to ensure the security of personal sensitive information in the transmission and storage process.

The commonly used data encryption algorithms are: Elliptic curve encryption ECC [18], Triple DES [13], Blowfish algorithm [20], RSA algorithm [19], advanced encryption standard AES [12], etc., with high security and efficiency, has been widely used in various information security fields, such as e-commerce, online banking, network communication and so on.

b. Image transmission and storage encryption

Image encryption is an important technology to protect image information security. In modern information society, image, as an important medium, is widely used in various fields, including medical imaging, network transmission, military reconnaissance and so on. Therefore, it is necessary to encrypt images in transmission and storage.

Basic principles of image encryption and decryption [9]:

The image is composed of many pixel values with different intensities. These pixel values are expressed in a numerical range according to the bit depth of the image, and the pixel value size is 0-255. The pixel can be expressed as a binary string. The encrypted image and the key image are decrypted by bit-by-bit exclusive-OR operation again, in particular, the encryption of pixels is realized. For example, the value of a pixel is 216 (plaintext), the key is 178 (the value is freely determined by the encryptor), and the encryption and decryption are carried out through the exclusive-OR operation, the specific process is as follows:

Plaintext a = 216, key =178,

Encrypting a ^ key yields ciphertext b = 106.

Decrypt b ^ key to get the original plaintext a = 216.

Repeat the above operations for each pixel in the image to complete the encryption and decryption of the image.

Figure 1 Image encryption processing effect [23]

"Lena" is a plaintext (raw) image that needs to be encrypted.

"Key" is a key image used in the encryption and decryption process. The image is generated by random numbers.

"Encryption" is to encrypt images, which is obtained by the bit-by-bit XOR operation of the plaintext image Lena and the key of the key image.

"Decryption" is the decryption of image, the encryption of image and the key of key image obtained by bit-by-bit XOR operation.

c. Face image encryption based on LDA secure face recognition system [10]

The image encryption technique consists of two main stages, the first stage: pixel replacement, during which each pixel value is replaced by a new value generated by performing an XOR operation on each pixel bit. The second stage: in the pixel scrambling stage, CA is used to shuffle the pixel position to the new position. This image encryption method can solve the deception vulnerability problem in the face image recognition system.

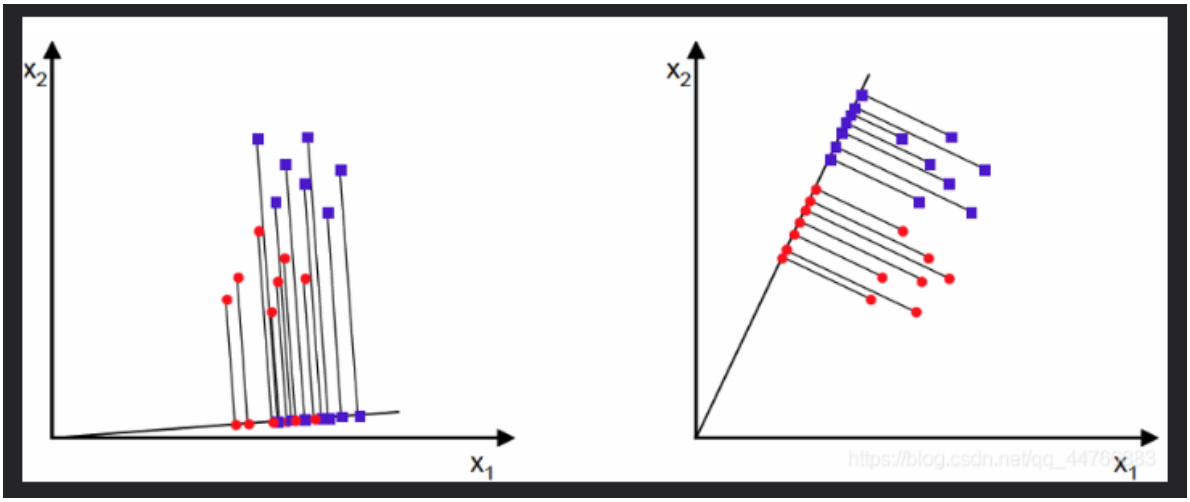

Figure 2 Schematic diagram of linear Discriminant Analysis (LDA) [10]

Features are extracted from encrypted images, data dimension is reduced, image classification is performed, and face recognition is carried out. This LDA-based encrypted face recognition model has a high accuracy rate of 96.25% in the classification of encrypted face images with the same encryption key [10].

In fact, image encryption can use a variety of technologies, including chaotic encryption, permutation encryption, optical encryption, DNA (DNA) encryption, frequency encryption, hashing encryption, evolutionary encryption, bit-plane encryption, double (multiple) image encryption, image encryption based on scrambling, etc. Many existing image encryption methods are proposed based on different techniques, including scanning, circular random grid, elliptic curve, Gray code, wave transmission, vector quantization, discrete wavelet transform, P-Fibonacci transform, chaotic sequence, etc. [16, 18].

(3) Face recognition other technical risks - the risk of counterfeiting and deception.

Countermeasures: Multi-factor authentication (such as iris recognition, fingerprint recognition, voice print recognition, etc.) and live detection (such as blinking, opening mouth, etc.) to prevent fake face attacks and forgery attacks.

(4) Privacy protection compliance risk - illegal operation and internal theft of information.

Countermeasures: Many countries have established personal data protection mechanisms and promulgated data security laws and regulations. By 2020, a total of 142 countries have enacted data privacy legislation, which stipulates that network operators should take measures to protect the security of personal information and prevent the leakage, destruction or alteration of personal information [4].

3 Discussion and Research on Privacy Protection of Face Recognition

A. Investigation conclusions and research objectives

A number of measures have been proposed in the survey literature to address various risks, and countries have established personal data protection mechanisms and promulgated data security laws and regulations; The United States has also established ethics compliance reviews to address accountability and transparency issues to mitigate risks; Cybersecurity Law in China stipulates that network operators shall take measures to protect the security of personal information and prevent the leakage, damage or tampering of personal information. These actions and measures have a positive effect on controlling the various risks caused by the wide application of face recognition technology, and have achieved certain effects on the privacy protection of personal information in face recognition.

However, the attack methods of some criminals and hackers are also constantly improving, and they try their best to find vulnerabilities and carry out malicious attacks. In recent years, a large number of serious personal data leaks have occurred around the world: for example, the 2019 Facebook data breach in the United States affected 540 million people [1]; China Deep Web Vision's non-compliant and illegal data processing practices have exposed billions of facial data [1]; The Finnish National Police informed the Office of the Data Protection Ombudsman in April 2021 of a personal data breach [21] involving the trial of facial recognition software by the National Bureau of Investigation in early 2020, which was caused by a failure to comply with the responsibility of the controller in the operation. Nor do the measures taken by the controller prevent the illegal processing of personal data [21]; Suprema, a security firm used by British police, banks and military contractors, reported that a security breach at a British biometrics company called Suprema compromised 28 million records and 23GB of data, including fingerprints, facial recognition data, passwords and security clearance information. This risk puts 5,700 organizations in 83 countries (including the UK's Metropolitan Police) at high risk. [22] At the national level, the impact of physiological data breaches can be far-reaching, for example, the Equifax hack, which exposed the data of 143 million US citizens [1], posing a serious threat to US national security. The frequency and scale of these data leaks are shocking, touching people's great concerns about the increasingly widespread use of face recognition technology, and even the use of facial recognition by federal agencies has aroused the anger of lawmakers, which has a negative impact on the further development of face recognition technology applications, so how to ensure the security of personal information privacy while developing face recognition technology applications? How to take effective countermeasures is a new round of challenges facing the further application of face recognition technology, and it is also the focus and research goal of this paper.

Through the review of a large number of privacy leakage incidents in the literature investigation, it can be seen that illegal attackers mainly adopt the following methods:

a. Use technical vulnerabilities to invade the server or client device of the face recognition system and implant illegal malware such as Trojans, zombies, Alpha Bay, and Hansa to obtain face recognition data and personal privacy information;
b. Use management vulnerabilities to carry out illegal operations and illegally process personal data in multiple information processing links such as face recognition data transmission, storage, identification, sharing, transfer, public disclosure, and deletion, resulting in leakage of personal privacy information;
c. Take advantage of vulnerabilities in laws and regulations to illegally obtain face images without permission in public places and violate personal privacy.

Through the analysis of various risks of face recognition in literature investigation, this paper can see that because face recognition technology is not a single technology, in terms of information collection, there are multiple information processing links such as transmission, storage, recognition, sharing, transfer, public disclosure and deletion. There are various technical links such as hardware equipment, software algorithms, face deception, and technical hidden dangers, as well as various management links such as the privacy information compliance industry management system, and the national supervision level. There may be vulnerabilities in many of these links, which are the targets that criminals and hackers can use and carry out malicious attacks. It is also the focus of privacy protection measures to be taken. This paper summarizes, summarizes and classifies these different links, which can be divided into:

a. Technical vulnerability response measures;
b. Countermeasures for vulnerabilities in industry standards;
c. Countermeasures for vulnerabilities in laws and regulations.

B. Face recognition privacy protection measures

a. Technical vulnerability

In view of the increasingly distributed, complicated, automated and constantly updated technical means of network attacks and unknown and changing attack behaviors, countermeasures should be taken from intrusion detection, threat intelligence, vulnerability analysis, malicious code detection and response, with the focus on strengthening and improving vulnerability analysis technology, using privacy enhancement technology, and strengthening the protection of users' privacy data. Guard against attacks and intrusions by criminals and hackers.

For example, a security analysis software can be designed to detect vulnerabilities in a facial recognition system by using machine learning and statistical models to look for malware family characteristics, predict the direction of evolution, advance defense, establish a conceptual framework to identify potential vulnerabilities, and create mechanisms to assess the robustness of the system. Ensure that it effectively protects against security threats.

Conceptual framework

(1) Overview of face recognition systems: Face recognition systems generally involve three main steps: face detection, feature extraction and identity verification or recognition. They often rely on deep learning models, particularly convolutional neural networks (CNNS), to learn and recognize facial features from large image datasets.

(2) Vulnerability Assessment Tool: This tool will simulate common attack vectors against face recognition systems, such as:

Print attack: Using a printed photo of an authorized user's face.

Replay attack: Display video or digital images of authorized users.

3D mask attack: Use a 3D mask with the facial features of an authorized user.

Deepfake attack: Create composite images that mix features of different faces.

(3) Analyze software components

Security analysis software includes input, attack simulation, detection, and reporting modules for assessing system vulnerabilities.

Input module: Input the details of the face recognition system and the data classes it uses, utilizing various databases of face images, including legitimate faces, spoofed faces (e.g. printed photos, masks), and adversarial examples (images that have been tampered with to fool the system). The database serves as the basis for testing system vulnerabilities.

Attack Simulation Module: Create or use prefabricated attack vectors, this vulnerability assessment tool simulates attacks such as printing, replay, 3D masks, and Deepfake attacks.

Detection module: The face recognition system uses face detection, feature extraction and authentication, usually using CNN, to analyze the response of the face recognition system to simulated attacks to determine its sensitivity.

Reporting module: Outputs a detailed report on the detected vulnerability, including the type of attack and system response.

Working principle

The principle behind the software is to assess how well a facial recognition system can withstand an attempted breach using a technology that exploits known vulnerabilities.

Face detection robustness: The software will attempt to provide altered images or videos to see if the system can correctly detect a real face with a photo or screen.

Feature extraction analysis: It will analyze the system's feature extraction mechanism to determine if it can distinguish between a high-quality 3D mask or altered image and a real face.

Recognition/verification test: The software will check if the system is fooled by similar, twin, or deep fake images that could fool recognition algorithms.

By systematically testing these aspects, the software can identify specific weaknesses in face recognition systems. For example, if the system fails during a print attack simulation, it indicates that the face detection algorithm is not strong enough to distinguish between a flat photo and a real face, a common vulnerability.

Implementation mode

Development stack: The software can be developed using high-level programming languages such as Python, which provides libraries such as OpenCV for image processing, TensorFlow or PyTorch for processing machine learning models, and Flask or Django for creating Web interfaces.

Model training: Consider incorporating a training model module to recognize deep forge images and other advanced attack vectors.

Modularity: Ensure that each component is modular and can be updated independently to deal with new vulnerabilities.

User interface: Design a user-friendly interface for security teams to run simulations without extensive technical expertise.

OpenCV: Open source computer vision library, provides powerful image processing and computer vision capabilities, supports multiple programming languages, including face detection and recognition.

Contribution: OpenCV can be used for face detection, feature extraction, and image preprocessing, which are all essential steps in face recognition. However, it does not directly address the vulnerabilities in face recognition systems, but rather provides the basic tools needed for analysis.

TensorFlow: A powerful open source software library for building and training deep neural networks and processing machine learning models, including image recognition and face recognition models.

Contribution: TensorFlow can be used to build and train face recognition models. In vulnerability analysis, TensorFlow can help assess the robustness and reliability of face recognition systems, including identifying potential weaknesses or vulnerabilities in the model.

PyTorch is an open source Python machine learning library for applications such as natural language processing. It mainly provides two advanced features: powerful GPU-accelerated tensor computing capabilities; a powerful NN library for building and training neural networks, providing dynamic computation graphs and a more Pythonic interface.

Contribution: Like TensorFlow, PyTorch can be used to develop face recognition models and assess vulnerabilities. Researchers choose between TensorFlow and PyTorch based on their preferences and specific project requirements.

Flask: A lightweight Web framework for creating Web interface libraries.

Contribution: It can be used to create a Web interface or API for deploying face recognition models. In terms of vulnerability analysis, Flask can facilitate the integration of face recognition models into web-based systems for testing and evaluation.

Django is a high-level Python Web framework for creating libraries for Web interfaces that facilitate rapid development and clean, pragmatic design.

Contribution: Similar to Flask, Django can be used to develop Web interfaces or APIs for deploying and testing face recognition models. It provides like user authentication, session management, and database integration that can be used to build a comprehensive vulnerability analysis tool or platform.

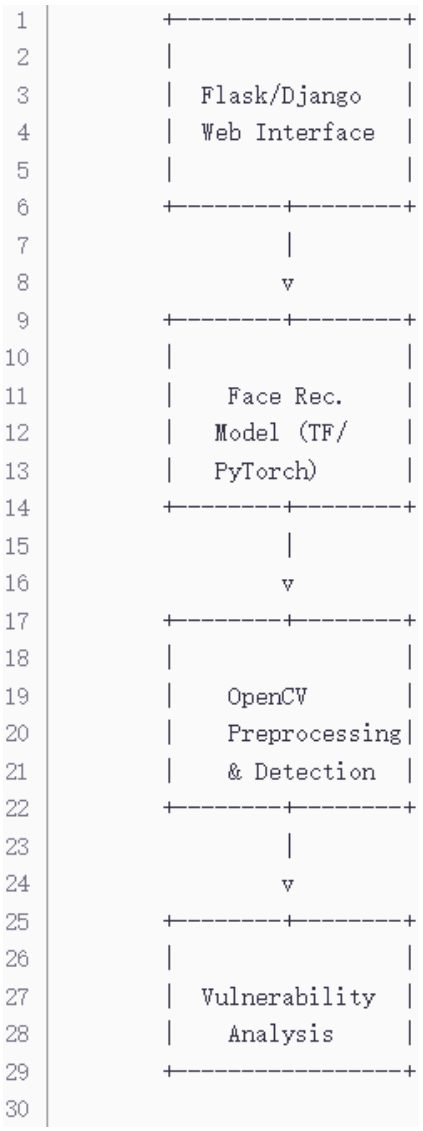

Figure 3 Relationship Model

OpenCV is used to pre-process and detect faces in images and input them into face recognition.

Perform face recognition tasks using a face recognition model developed by TensorFlow or PyTorch.

Flask or Django provides a Web interface for interacting with a face recognition system.

Use vulnerability analysis tools or methods to evaluate the robustness and security of face recognition systems. The model illustrates how these components work together to build, deploy, and analyze a face recognition system, with each component playing a crucial role in the process.

Python and OpenCV library combination:

Role in vulnerability analysis: OpenCV is mainly re-

sponsible for image preprocessing and face detection. In the event of a vulnerability, OpenCV's face detection algorithm may have limitations or weaknesses that could be exploited. For example, if a face detection algorithm is not robust enough, it may not be able to detect certain faces, or it may be vulnerable to adversarial attacks in which manipulated images fool the system.

Python combined with the TensorFlow library:

Role in vulnerabilities: TensorFlow and PyTorch are used to build and train face recognition models. These models can be vulnerable to various attacks, such as adversarial examples or spoofing attacks. Adversarial examples are inputs specifically designed to fool the model, while spoofing attacks involve presenting fake or manipulated faces to bypass recognition systems.

Create a Web interface using Python and Flask libraries:

Role in vulnerability: Flask frameworks are commonly used to deploy face recognition systems as Web applications or APIs. In terms of vulnerabilities, if not implemented securely, these frameworks can present security risks such as injection attacks, authentication bypassing, or data breaches. In addition, improper handling of user input or inadequate access control mechanisms can also lead to vulnerabilities in the overall system.

Creating a Web interface using Python and Django libraries:

Role in vulnerabilities: Web interfaces created with Django provide a potential attack surface for adversaries. Vulnerabilities in an interface, such as insecure authentication mechanisms, cross-site scripting (XSS), or cross-site request forgery (CSRF), can be exploited to gain unauthorized access to a system or manipulate its behavior.

The vulnerability analysis software is designed to identify and mitigate security vulnerabilities in face recognition systems. The software works by exposing a face recognition system to known vulnerabilities in order to assess its resilience, which includes assessing the system's sensitivity to various attacks, assessing the effectiveness of countermeasures, and identifying potential areas for improvement. Techniques such as penetration testing, threat modeling, and code review are often used in vulnerability analysis to enhance a system's security posture. This proactive approach to security ensures that face recognition systems are tested against ever-changing threats, helping to build stronger and more reliable AI biometric security solutions.

The vulnerability risk measures should also be iteratively updated to enhance encryption technology to meet the new challenges of face recognition privacy protection.

b. Countermeasures for vulnerabilities in industry standards

At present, different countries and regions have corresponding industry standards for the protection of personal privacy when using facial recognition technology, but they vary greatly and are not perfect enough. Some countries may not have specific standards, such as the California Consumer Privacy Act (CCPA), although face recognition also belongs to the protection of biometric data [3]. The EU General Data Protection Regulation (GDPR) is one of the most comprehensive data protection laws in the world [3], but both CCPA and GDPR lack industry standards specifically for the application of face recognition technology, which may have vulnerabilities in the leakage of personal privacy information, such as the mentioned personal data leakage incident in Finland [21]. This leakage incident is caused by the failure to perform the responsibility of the controller in the operation, and the measures taken by the controller did not prevent the illegal processing of personal data. Therefore, the author suggests that industry standards for the application of face recognition technology should be established or improved to ensure that face recognition information is processed in the collection. Standardize operation in multiple information processing links such as transmission, storage, identification, sharing, transfer, public disclosure, and deletion to deal with the vulnerability risk of personal privacy leakage caused by illegal operations and internal data theft by practitioners. At the same time, it is necessary to study and develop technical standards such as biometric basic technology, feature extraction, and security encryption, clarify the application scenarios and security requirements of biometric information, and eliminate vulnerabilities in all aspects of face recognition information processing.

c. Countermeasures for vulnerabilities in laws and regulations

Recently reported the British LabHost phishing service platform incident, although the London police successfully banned the phishing service platform "LabHost", a total of 37 people were arrested around the world, but the crime was as long as 3 years, engaged in stealing information and illegally making profits, as many as 70,000 victims [24]. This shows that in addition to the technical vulnerabilities of the account protection system, the more

important reason is the use of legal and regulatory vulnerabilities. The author suggests that all countries in the world should formulate corresponding rules for legal and regulatory investigation, strengthen the crackdown on criminals, effectively prevent illegal attackers from using legal and regulatory vulnerabilities to commit crimes, in particular, strengthen accountability. According to the consequences and severity of the destruction and leakage of personal information system are graded, and the corresponding laws and regulations are formulated to provide a legal conviction basis for the unification of the scale of criminal judgment, bring criminal acts to justice, and provide legal deterrence, so that criminals are discouraged, and ensure the protection of personal privacy information of face recognition.

4 Face Recognition Technology Application and Various Risk Countermeasures for Personal Privacy Protection

Through literature survey, this paper records various potential vulnerabilities and personal privacy security risks existing in the application of face recognition technology, finds out various risk countermeasures, looks up a large number of personal privacy leakage cases, sorts out, analyzes, summarizes and classifies various vulnerabilities and risks existing in the application of face recognition technology, and the main risks are roughly divided into: (1) Hardware equipment security risks; (2) Software security risks; (3) Face recognition fraud risk; (4) Privacy protection compliance risks, and corresponding countermeasures for these four types of risks.

In the literature survey, the author also found that not only have a number of countermeasures been proposed for various risks in the application of face recognition technology, but also countries around the world have established personal data protection mechanisms and promulgated data security laws and regulations, and personal information privacy protection has achieved certain results. These actions and measures have a positive role in controlling the various risks brought about by the wide application of face recognition technology, and have achieved certain results in the protection of personal information privacy. However, in recent years, why have a large number of serious personal data leaks still occurred in the world? This has aroused the attention and thinking of the author, which shows that the application of face recognition technology is developing rapidly at the same time, the attack ability of illegal attackers and hackers is also developing rapidly, and the intrusion means are constantly improving, which has a great impact on the further development of face recognition technology application. In this point, how to ensure the security of personal information privacy while developing the application of face recognition technology? How to take effective countermeasures is a new round of challenges facing the further application of face recognition technology, and it is also the focus and research goal of this paper.

By combing through a large number of privacy leakage incidents in the literature investigation, this paper concludes that the main means used by illegal attackers are as follows:

1) Use technical vulnerabilities to invade the server or client device of the face recognition system and implant illegal malware such as Trojans, zombies, Alpha Bay, and Hansa to obtain face recognition data and personal privacy information;
2) The use of management vulnerabilities, in the face recognition data transmission, storage, identification, sharing, transfer, public disclosure, deletion and other information processing links, illegal operations, illegal processing of personal data, resulting in personal privacy information leakage;
3) Take advantage of vulnerabilities in laws and regulations to illegally obtain face images without permission in public places and violate personal privacy.

Through the analysis of various risks of face recognition in literature investigation, it can be seen that face recognition technology is not a single technology, and there may be vulnerabilities in various management links such as information collection and processing, technology application, privacy information compliance industry management system, and national supervision. These are the targets that criminals and hackers can use and carry out malicious attacks, and are also the focus of privacy protection measures to be taken. This paper summarizes three types of vulnerabilities:

1) technical vulnerabilities,
2) industry standard vulnerabilities, and
3) legal and regulatory vulnerabilities.

In this paper, the author puts forward the author's suggestions on the vulnerability countermeasures in the above three aspects of technology, industry standards and

laws and regulations, and makes a specific introduction to the measures, in order to cope with the new risks and challenges faced by the application of face recognition technology.

5 Conclusions & Summary

By investigating, evaluating and analyzing the privacy leakage and cybersecurity risks of face recognition and the countermeasures, this paper proposes the application of face recognition technology. In terms of technical means, it constantly researches and upgrades the face recognition intelligent algorithm and privacy enhancement technologies. In terms of industry standards, establish and improve the standardized management system in all aspects of face recognition information processing; In terms of laws and regulations, speed up the improvement of laws and regulations on the use of personal information, establish the protection level of information security system, strengthen responsibility investigation, and strengthen punishment against lawbreakers, so as to effectively avoid the vulnerability risks generated by these three aspects, and implement multi-directional and full-life effective protection of personal privacy information. Ensure the further development of face recognition technology in cybersecurity and personal privacy protection.

References

[1] Meng Wang, "Identifying Personal Physiological Data Risks to the Internet of Everything: the case of facial data breach risks". School of Journalism and Information Communication, Huazhong University of Science and Technology, Wuhan, Hubei Province, China. (2023).

[2] Hafiz Sheikh Adnan, "Ahmed Facial Recognition Technology and Privacy Concerns". Date Published: 21 December 2022.

[3] Insaf Adjabi, "Past, Present, and Future of Face Recognition: A Review". Electronics 2020, 9(8), 1188; https://doi.org/10.3390/electronics9081188

[4] Eimad Abusham, "Facial Image Encryption for Secure Face Recognition System". Electronics 2023, 12(3), 774; https://doi.org/10.3390/electronics12030774

[5] Lixiang LiA, "Review of Face Recognition Technology". Electronic ISSN: 2169 (2020): 3536; https://ieeexplore.ieee.org/document/9145558

[6] Gavin Wright, "Side-channel Attack". TechTarget; (2023). https://www.techtarget.com/searchsecurity/definition/side-channel-attack

[7] Zhiyuan Cheng, "Physical Attack on Monocular Depth Estimation with Optimal Adversarial Patches". Computer Science > Computer Vision and Pattern, Recognition; (2022). https://arxiv.org/abs/2207.04718

[8] Rushank Shah, IEEE Xplore; "Encryption of Data over HTTP (Hypertext Transfer Protocol) / HTTPS (Hypertext Transfer Protocol Secure) Requests for Secure Data transfers over the Internet". (2021) https://ieeexplore.ieee.org/document/9573978

[9] Akhil Bhadwal, upGrad; "Image Encryption: An Information Security Perceptive". (2023) https://www.knowledgehut.com/blog/security/encrypting-images#what-is-image-encryption?%C2%A0

[10] Ambika, Medium; "Image Encryption: Linear Discriminant Analysis (LDA) in Machine Learning: Example, Concept and Applications". (2023) https://medium.com/aimonks/linear-discriminant-analysis-lda-in-machine-learning-example-concept-and-applications-37f27e7c7e98

[11] Kaeli Britt, NEVADA Today; "How are deep fakes dangerous?". (2023) https://www.unr.edu/nevada-today/news/2023/atp-deepfakes

[12] Rahul Awati, TechTarget; "Advanced Encryption Standard (AES)". (2023) https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

[13] Peter Loshin, TechTarget; "Advanced Encryption Standard (DES)". (2023) https://www.techtarget.com/searchsecurity/definition/Data-Encryption-Standard

[14] Basel, PMC PubMed "Central; Face Image Encryption Based on Feature with Optimization Using Secure Crypto General Adversarial Neural Network and Optical Chaotic Map". (2023) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9921757/

[15] Luoyin Feng, PMC PubMed Central; "Image Recognition and Encryption Algorithm Based on Artificial Neural Network and Multidimensional Chaotic Sequence". (2022) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9410944/

[16] Hendrik Richter, International Journal of Bifurcation and Chaos 12(6): 1371-1384; (2002) "The Generalized HÉnon Maps: Examples for Higher-Dimensional Chaos". https://www.researchgate.net/publication/220265334_The_Generalized_HEnon_Maps_Examples_for_Higher-Dimensional_Chaos

[17] Mustafa Kamil Khairullah, Electronics 2021, 10(17), 2116; "Designing 1D Chaotic Maps for Fast Chaotic Image Encryption". https://www.mdpi.com/2079-9292/10/17/2116

[18] Andrew Froehlich, Cryptography (ECC). "Elliptical Curve" (2023) https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography

[19] Michael Cobb, TechTarget; "RSA Algorithm (Rivest-Shamir-Adleman)"; (2023) https://www.techtarget.com/searchsecurity/definition/RSA

[20] Rahul Awati, TechTarget; "Blowfish". (2023) https://www.techtarget.com/searchsecurity/definition/Blowfish

[21] Rahul Awati, National Police Board; "Finnish SA: Police Reprimanded for Illegal Processing of Personal Data with Facial Recognition Software". (2021) https://www.edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en

[22] Chetan Conikee, Medium; "Suprema Security Breach: Protecting Apps from BioMetric Security Flaws". (2019) https://blog.shiftleft.io/protecting-from-biometric-security-flaws-36618f7b020b

[23] Mandeep Kaur, Hindawi; "Computational Image Encryption Techniques: A Comprehensive Review". (2021) https://www.hindawi.com/journals/mpe/2021/5012496/

[24] Mark Thompson, CNN; "Police take down $249-a-month global phishing service used by 2,000 hackers" (2024). https://www.cnn.com/2024/04/18/tech/labhost-cybercrime-phishing-arrests/index.html