The Disruption and Reconstruction of Portrait Rights by AI Face-Swapping Technology: From Individual Rights Protection to Platform Responsibility

Han Wang*

School of Journalism and Communication, Hunan University, Changsha, China

*Corresponding author: 2783932936@qq.com

Keywords: AI face-swapping; portrait rights; liability allocation mechanisms; dynamic consent mechanism; traceability technology

Abstract: The explosive proliferation of AI face-swapping technology has given rise to novel forms of infringement concerning portrait rights. Traditional legal frameworks and rights protection mechanisms struggle to address the challenges stemming from this technological disruption of rights. Systematic research is urgently needed to address these pressing practical concerns. Currently, most studies focus on analyzing individual infringement cases or interpreting legal provisions, lacking comprehensive discussions on the boundaries of portrait rights, infringement determination standards, and liability allocation mechanisms in the context of technological advancements. This paper deconstructs the dissemination mechanisms and legal dilemmas associated with AI face-swapping technology and proposes a dynamic consent mechanism alongside traceability technology for the propagation chain to address the current challenges. Drawing on typical cases and empirical data, it clarifies the core scope of portrait rights protection in AI face-swapping scenarios, diverse rights protection pathways, and delineates the responsibilities of platforms. It proposes a collaborative governance framework of "technical regulation + legal refinement + platform self-governance" to balance technological innovation with rights protection, and to promote the improvement of relevant legislation and the development of industry norms. This provides theoretical support and practical references for balancing technological innovation with rights protection, and for promoting the refinement of relevant legislation and the development of industry norms.

1. Introduction

In the current era of rapid technological advancement, AI face-swapping technology, distinguished by its unique innovative attributes, has rapidly proliferated across various domains. AI face-swapping technology (Deepfake) is a facial feature migration technology based on the Generative Adversarial Network (GAN)[1]. Through algorithms, it replaces the target face onto a specific carrier (such as videos or images), generating innovative value in fields such as film and television production and social entertainment. However, its high degree of realism also poses systemic challenges to the protection of portrait rights. Article 1019 of the Civil Code stipulates: "No organization or individual may infringe upon the portrait rights of others through defamation, damage, or forgery using information technology. Without the consent of the portrait rights holder[2], no one shall produce, use, or disclose their portrait, unless otherwise provided by law." This provision explicitly identifies "forgery using information technology" as a mode of infringing portrait rights, a category into which AI face-swapping technology squarely falls. While this clause aims to address infringements upon personal dignity resulting from technological forgery, it did not anticipate how AI face-swapping would fundamentally challenge the "identifiability" requirement inherent in portrait rights.

Currently, both academia and judicial practice have conducted numerous studies examining the relationship between AI face-swapping technology[3] and portrait rights. These studies primarily focus on whether AI face-swapping constitutes an infringement of portrait rights and how such infringing acts should be defined. Some studies focus on the "identifiability" requirement of portrait rights, analyzing whether auxiliary elements like body shape and contextual details can serve as evidence for infringement determination when facial features are replaced. Significant differences

  DOI: 10.25236/ieesasm.2025.006

exist among these studies. The affirmative view contends that elements like body movements and contextual details retain identification power; the negative view holds that once facial features are replaced, the remaining bodily image constitutes merely personal information, not a portrait. Judicial practice reflects a lack of consensus among courts on whether AI face-swapping infringes portrait rights. For example, the Nanjing Jiangbei District People's Court of Jiangsu Province concluded a case of portrait rights dispute. Plaintiff Lin found a video template in the "AI video face-swapping" WeChat mini-program operated by the defendant Nanjing Company, which showed an external image of herself wearing traditional Chinese clothing and with complete traditional makeup. The Nanjing Jiangbei District People's Court held that the template could identify the subject of the video as the plaintiff, thus infringing upon the plaintiff's portrait rights. Conversely, in a case adjudicated by the Beijing Internet Court, the court held that the defendant company, by technically replacing the plaintiff's facial features, had removed the core element enabling portrait identifiability. Consequently, the court determined that the behavior did not constitute portrait rights infringement, finding instead that it infringed upon the plaintiff's personal information rights. Other studies focus on the attribution of liability in scenarios of rights abuse, using the case of the dispute between online celebrity Xiaozhi and the AI face-swapping APP operating company heard by the People's Court of Jinshan District, Shanghai as an example, clarifying that the platform must bear the infringement liability when using others' portraits as face-swapping templates without authorization.

Erik Gerstner[4] discuss the “FakeApp” and the technology behind it. Next, he discuss the state of the relevant law and examine how face swaps have and will continue to intersect with applicable statutory and case law. Finally, he discuss potential judicial and legislative solutions to present and future problems arising from these sorts of Al technologies.Put forward feasible suggestions for the infringement of portrait rights caused by AI face-swapping. Kugler, Matthew B.;Preminger, Alice[5] changes to how right of publicity law treats expressive uses and also considers the problems raised by current right of publicity licenses and the overbroad terms they regularly contain.New canons of interpretation are needed to prevent the contracts being used to justify uses beyond what the contracting parties could have imagined. Duquette, Hayley[6] explore such developments in terms of their implications on individuals with commercially viable personas. She examine a proposed amendment to New York's right of publicity law that reflects the fear of emerging technology's potential uses, discussing the rapid advancements in face-swapping technology, followed by Section C's exploration of social media's dominating influence on today's society.

Research papers addressing portrait rights infringement caused by AI face-swapping technology primarily focus on legal regulation, technical countermeasures, and ethical discussions. Additionally, much of the literature emphasizes the need for technical remedies, such as developing anti-deepfake detection models[7], and delves into ethical dilemmas like the blurred boundary between fair use and infringement, and the imbalance between technological innovation and portrait rights protection. This literature often calls for collaborative governance involving legal frameworks, technological solutions, and industry self-regulation.

However, the existing research still has significant shortcomings: Firstly, there is a triple ambiguity in platform responsibility: the absence of pre-event review standards, the abuse of the technical neutrality defense in the process, and the controversy over the scope of joint liability; Secondly, key issues in individual rights protection have not been fully addressed, such as the balance of costs and benefits in the individual rights protection process, and the efficient methods for fixing infringement evidence in complex technical scenarios, and there are still no feasible solutions.

Given these gaps, this paper adopts "Individual Rights Protection - Platform Responsibility" as its central analytical framework, systematically analyzes the process of AI face-swapping technology's deconstruction and reconstruction of the right to portrait. By sorting out the underlying operational logic of AI face-swapping technology, it reveals the technology's disruption to traditional concepts of portrait rights and its impact on infringement determination standards, and subsequently explores effective rights protection pathways for individuals encountering AI face-swapping infringement; At the same time, it focuses on clarifying the responsibility boundaries and obligation contents of the platform in the application of AI face-swapping technology, aiming to improve the protection system

of the right to portrait in the context of AI face-swapping, and provide new ideas for related judicial practice and theoretical research.

2. AI Face Swapping's Transmission Mechanism and Legal Dilemmas

2.1 The Underlying Logic of Viral Spread

In the current era of rapid information flow, viral dissemination has become widespread. A piece of content can penetrate different social circles in a short period of time and trigger nationwide discussions. The underlying logic behind this is a complex and ingenious set of rules, namely, the celebrity effect triggers a transfer of online users' emotional trust, thereby lowering the audience's psychological defense threshold and creating a crucial link in the communication chain.

The celebrity effect refers to the phenomenon where the social influence of celebrities attracts attention, amplifies messages, and expands impact, or the psychological mechanism driving people to imitate celebrity behavior. Its core lies in the social credibility and appeal of celebrities. The celebrity effect is the "start switch" of viral dissemination. It can capture the public's attention at the lowest cost and make people imitate the behaviors of celebrities. During this process, audiences are likely to convert their favorable feelings towards celebrities into recognition and spontaneous sharing of information and products,that is,an "emotional trust migration" occurs, reducing the psychological defense threshold of the audience and clearing the resistance obstacles for information dissemination. For example,in December 2024, a video of national anti-epidemic expert Dr. Zhang Wenhong promoting protein bars was circulating on the internet. Verification revealed that the video was fabricated using AI face-swapping technology and did not originate from Dr. Zhang himself. Many netizens believed the video to be authentic and placed purchase orders. Dr. Zhang Wenhong, as the director of the Department of Infectious Diseases at Huashan Hospital of Fudan University, has made significant contributions in the field of medicine and has a wide influence and a large fan base. The merchants were precisely using the celebrity effect of Dr. Zhang Wenhong to promote protein bars, which led netizens to convert their trust in Dr. Zhang Wenhong into trust in the protein bar products, lowering their psychological defense threshold and forming a viral dissemination.

2.2 Legal Applicability Dilemma

Currently, the dual nature of AI face-swapping technology is becoming increasingly prominent, especially the issue of infringement of portrait rights is becoming increasingly serious. In terms of legal application, multiple difficulties have emerged, primarily manifested in judicial disagreements over identifiability determination standards, blurred boundaries of platform responsibility, and an imbalance between the costs incurred and benefits obtained in rights protection.

2.2.1 Judicial Disagreements on Identifiability Determination

"Identifiability" is a crucial element in the determination of portrait infringement, but significant differences exist in determination standards across courts, directly impacting case outcomes.

Some courts adopt the "comprehensive feature determination standard", believing that portrait identification should not be limited to the face, but should be judged based on the overall features. For example, in the case of blogger Zhao from an ancient-style short video, whose appearance in the video wearing a custom Hanfu and with a unique hairstyle was used as a template by a face-swapping software, and the user replaced the face to generate a new video for dissemination. The court held that although the face was replaced, the Hanfu patterns, body postures, and background scenes in the video were all exclusive features of Zhao, and the general public could still associate them with Zhao through these elements, thus determining that it met the "identifiability" criterion, and the software operator was found to have committed portrait infringement.

Other courts adhere to the "facial core determination standard", considering the face as the sole key element for portrait identification. For instance, in the case of Wu suing a face-swapping platform, Wu's "excessive sweetness" life video was captured by the platform, and the user replaced his face to post it. The court pointed out that the core value of a portrait lies in the uniqueness of the face, and

after the face is replaced, the video loses the direct identification basis pointing to Wu. Even if other personal features remain, the court held this did not constitute a legally recognizable "portrait." Consequently, it did not find portrait rights infringement, ruling instead that the platform was liable for infringing Wu's personal information rights.

This standard difference leads to completely different judicial outcomes for similar cases, making it difficult for parties to predict the prospects of safeguard rights and weakening the legal guidance role of AI face-swapping behavior.

2.2.2 Blurred Boundary of Platform Responsibility

The dissemination of AI face-swapping content heavily relies on online platforms. However, the current legal definition of platform responsibility is ambiguous. A typical case is the "ZAO Face Swapping APP case".

ZAO APP once allowed users to upload their personal photos and replace the faces of celebrities in film and television clips to generate "co-presenting with celebrities" videos. During this process, the platform used the portraits of a large number of film and television stars without authorization, triggering a large-scale infringement dispute. From a legal perspective, the nature of the responsibility that the platform should bear, such as direct infringement or indirect infringement, and the scope of obligations, such as active review or passive response, all lack clear regulations. On one hand, the platform claimed to only bear the passive obligation of "notification - deletion" by citing "user-generated content (UGC)", believing that it is impossible to fully review the massive content; on the other hand, the regulatory authorities and the victims believed that AI face-swapping technology has obvious infringement risks, and the platform, as a technology provider, should assume a higher obligation of active review, such as presetting an authorization mechanism for portrait rights and developing AI face-swapping content recognition technology.

Ultimately, although ZAO APP adjusted its function due to public opinion pressure, it did not clearly assume the infringement liability and did not form a replicable standard for platform responsibility determination. In subsequent similar cases, the platform and the victims often fell into "responsibility shifting" - the platform claimed to have fulfilled the "notification - deletion" obligation, while the victims believed that the platform did not actively prevent infringement, and the court was also unable to make a clear division of responsibility due to the lack of clear legal basis.

2.2.3 Imbalance between Cost and Benefit of Rights Protection

In cases of AI face-swapping infringement, the victims have to bear extremely high costs for rights protection, but they often fail to receive corresponding compensation, which leads most people to give up their efforts to seek justice.

Table 1. Comparison of costs and compensation in some judged cases

Volume Number	Case Name	Costs	Penalty Payment
(2024) Sichuan 7101 Civil Initial Case No. 5615	First Instance Civil Judgment of Portrait Right Dispute between Mi Mou and Beijing XX Technology Co., Ltd.	The legal fees for the plaintiff's defend rights activities have reached 2,000 yuan.	The plaintiff claims economic losses and reasonable costs for defend rights activities totaling 10,000 yuan. The court has lawfully determined that the defendant shall compensate the plaintiff for economic losses and reasonable costs for protect rights activities of 2,000 yuan.
(2023) Shanghai 0115 Civil Initial Case No. 9795	First Instance Civil Judgment on Portrait Rights Dispute between Wang Mou and a Certain Company	The plaintiff claims that the defendant should compensate for economic losses and expenses for defend rights (protection of rights) totaling 10,000 yuan.	The court decides to have the defendant compensate the plaintiff for economic losses and defend rights expenses totaling 1,000 yuan, based on circumstances.
(2022) Shanghai 0116 Civil Initial Case No. 13856	First Instance Civil Judgment of Portrait Rights Dispute between Liao and Shanghai Fishwort Information Technology Co., Ltd.	The judgment orders the defendant to compensate the plaintiff for total economic losses and reasonable defend rights expenses amounting to 50,000 yuan (economic losses 48,000 yuan,defend rights expenses 2,000 yuan)	The defendant shall be taken into consideration the circumstances ordered to compensate the plaintiff with economic losses of 4,000 yuan and reasonable defend rights expenses of 200 yuan
(2022) Shanghai 0116 Civil Initial Case No. 13225	First Instance Civil Judgment of Portrait Right Dispute between Zhao Xihan and Shanghai Huifan Information Technology Co., Ltd.	The judgment orders the defendant to compensate the plaintiff for total economic losses and reasonable expenses for defend rights (legal protection) totaling 50,000 yuan (economic losses 48,000 yuan, reasonable expenses 2,000 yuan)	The defendant Shanghai Huifan Information Technology Co., Ltd. shall compensate plaintiff Zhao Xihan 5,200 yuan within ten days after the entry of this judgment.

As shown in Table 1, the costs and expenses that the plaintiff needs to bear in the early stage of

protecting their rights include three items: First, they need to entrust a notary institution to fix the evidence of the infringing advertisement and pay the notary fee; second, they need to hire a lawyer to obtain the advertising data of the brand and the browsing records of users, and the lawyer's fee is spent; third, if the brand's registration location and the location of the infringement are across provinces and cities, they need to travel back and forth between the two places to participate in the lawsuit, and the transportation and accommodation expenses are incurred. Even if they ultimately win the lawsuit, the court, considering factors such as the severity of the infringement and the profits of the brand, often judges the defendant to compensate the plaintiff's costs, which is usually lower than the plaintiff's initial cost of protection. This leads to an imbalance between the cost and the return of protection. More commonly, when ordinary citizens encounter AI face-swapping infringement, due to the lack of professional legal knowledge, it is more difficult to obtain evidence, and the infringing party is mostly individual users or small institutions, with limited compensation capacity. After winning the lawsuit, they often can only receive a compensation of several thousand yuan, which is even insufficient to cover the notary fee. This "high cost, low return" reality forces a large number of victims to choose to "bear it silently", objectively allowing the proliferation of AI face-swapping infringement.

In conclusion, the challenge of AI face-swapping technology to the protection of portrait rights is essentially a manifestation of the lag of law behind technological development. Only by legislating to clearly define the "identifiability" determination standard, detailing the responsibility boundaries of the platform, and establishing a reasonable infringement compensation mechanism can we balance technological innovation and rights protection, and build a healthy digital legal environment.

3. Core Mechanism Construction: Dynamic Consent Mechanism and Traceability Technology of Transmission Chain

To address the aforementioned challenges, we have proposed the construction of two core mechanisms, namely the dynamic consent mechanism and the traceability technology of the transmission chain. Firstly, the dynamic consent mechanism effectively reduces the generation of infringing content through pre-event risk filtering. At the same time, the traceability technology of the transmission chain is employed to precisely determine responsibility after the event, thereby enhancing the efficiency of rights protection.

3.1 Dynamic Consent Mechanism: Scenario-based Graded Authorization

According to Article 14 of the Personal Information Protection Law regarding "separate consent", "When processing personal information based on individual consent, such consent should be voluntarily and clearly made by the individual under full awareness. Where laws and administrative regulations stipulate that processing personal information requires obtaining individual separate consent or written consent, such provisions shall prevail. If the processing purpose, method, and types of processed personal information change, individual consent should be re-obtained."

This study proposes a dynamic consent mechanism (see Figure 1), which is based on the risk levels of different communication scenarios and designs a graded authorization system and a real-time permission management portrait usage licensing system, thereby avoiding the traditional "one-time general authorization" model. Specifically, during the use of AI face-swapping technology, users conduct risk-level assessment of the communication scenarios. If the usage scenarios are relatively safe or risk-free (not exceeding a specific threshold), such as entertainment-based face-swapping, a single static authorization is sufficient; if the usage scenarios are relatively risky (exceeding a specific threshold), such as involving public figures or commercial purposes, a dynamic real-time authorization is adopted, and the authorization status is verified in real time through blockchain. For example, when a video is forwarded to a new platform (such as sharing from Douyin to WeChat), a cross-platform authorization verification protocol will be automatically triggered. If the verification fails, the dissemination will be frozen and a warning will be pushed (such as "This content has not obtained cross-platform authorization").

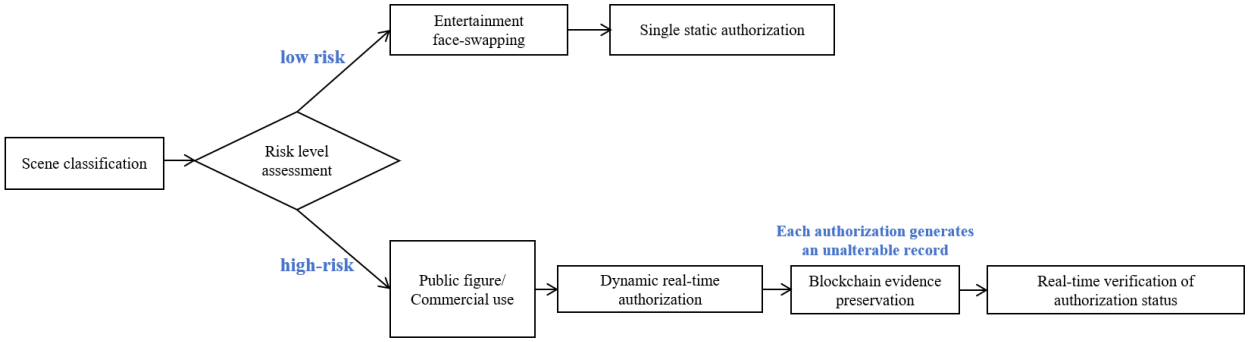

Fig.1 A dynamic consent mechanism

The specific process of authorized evidence storage for the dynamic consent mechanism (as shown in Figure 2) is as follows: It initiates the authorization for the use of the portrait (including the scope and validity period) from the user end to the authorization platform, generates an evidence data package to the blockchain node, broadcasts the transaction request to form a consortium chain, generates a new block from the consortium chain to the blockchain node, returns the evidence certificate to the authorization platform, and the platform returns the authorized certificate with digital watermark to the user end. Thus, one authorization evidence storage is completed.

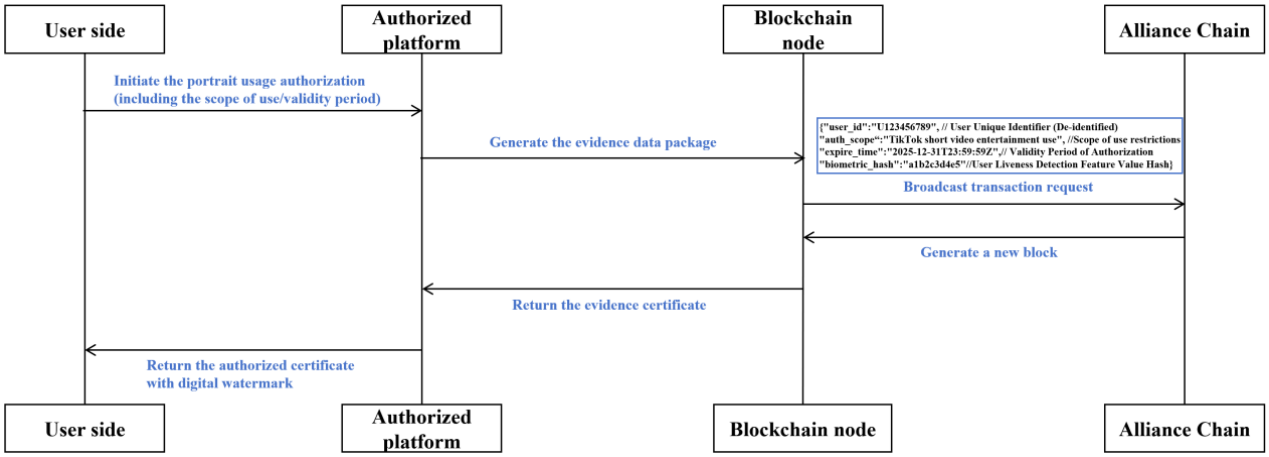

Fig.2 The specific process of authorized evidence storage in the dynamic consent mechanism

According to Article 7 of the "Electronic Signature Law": "Data electronic documents shall not be refused to be used as evidence merely because they are generated, sent, received or stored by means of electronic, optical, magnetic or similar methods." This legal provision proves that blockchain-based evidence storage can directly serve as electronic evidence. And establishing a dynamic consent mechanism for scenario-based hierarchical authorization can make the cost of avoiding infringement approach zero (see Table 2).

Table 2. The cost of the rights protection process and the corresponding dynamic consent mechanism

Rights protection section	Dynamic consent mechanism cost
Evidence fixation	¥0 (automatically stored)
Authorization status proof	¥0 (chain-verified)

3.2 Traceability Technology for Transmission Chain: Full Traceability of Infringement Liability

This technology integrates digital watermarking and cross-platform traceability systems to achieve the complete traceability of the dissemination path of AI-generated videos, identifying the source of infringement. By embedding QR code matrices in video frames (invisible to the naked eye, requiring a dedicated decoder to read), the platform ID of the generator, the generation time, and the initial authorization scope (such as "Only for entertainment use on Douyin") are generated. The platforms

such as WeChat, Douyin, and Kuaishou are forced to intervene at the central traceability node. When the video dissemination volume exceeds the threshold, an automatic traceability request is initiated to the database.

3.2.1 Digital Watermark Embedding

Using the DCT domain QR matrix, leveraging the technical advantages of the fast response matrix code (QR Code) generation principle and strong error correction capabilities, a remote sensing image digital watermarking algorithm based on QR code and quantized DCT is formed. Firstly, the original watermark information is generated as a QR code and preprocessed, the data encoding and error correction encoding of the QR code are saved, and the data encoding and feature watermark are combined to generate the watermarked information to be embedded; then, the 8×8 block DCT is performed on the carrier remote sensing image, and the watermark information is embedded into the DC coefficients of the DCT domain of the carrier remote sensing image according to the quantization rules; finally, the proposed algorithm is verified, and digital watermarks are embedded in video frames.

When checking whether the sensitivity threshold is reached, the risk score is defined as a comprehensive consideration of the propagation speed coefficient, content authenticity, and social sensitivity. The coefficients corresponding to these three factors, namely,, are the importance of the factors to the risk score. The coefficient values of,, can be set separately according to specific circumstances to obtain a specific risk score. When the risk score is greater than 8.0 or involves sensitive individuals, the content is automatically frozen and traced. The specific calculation is as follows:

Carrying information: Generator ID + Timestamp + Initial Authorization Scope (in JSON format)

```
risk_score = (transmission rate coefficient × α) + (content authenticity × β) + (ocial sensitivity ×γ)
   if risk_score > 8.0 or involves sensitive individuals:
         Automatically freeze the content and initiate traceability.
```

3.2.2 Cross-platform Traceability Mechanism

To establish and improve the cross-platform traceability mechanism, the national traceability center must first build a watermark key repository and a judicial forensics interface (see Table 3). The watermark key repository is managed by the Cyberspace Administration of China, aiming to store or interpret watermark data. The Ministry of Public Security is responsible for setting up the judicial forensics interface, which will allow data retrieval to be made available to the public security authorities.

Table 3. Cross-platform traceability mechanism

Component	Function	Responsible Institution
Watermark Key Repository	Stores and parses watermark data	Network Information Office
Judicial Forensics Interface	Provides data retrieval access to the public security authorities	Ministry of Public Security

Secondly, multi-platform collaboration is required for the operation. Firstly, short-video platforms (such as Douyin/Keke) need to deploy edge computing nodes to calculate the risk value in real time. Each edge computing node is responsible for a portion (see Figure 3). Secondly, social platforms (such as WeChat/Weibo) should enforce the verification of authorization tags when users share content to ensure precise accountability in the future.

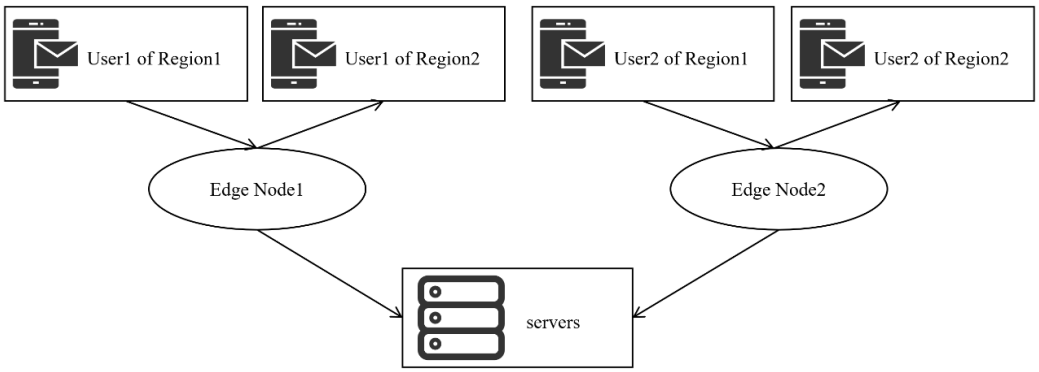

Fig.3 Multi-platform collaboration

4. Platform Responsibility System Reengineering

4.1 Beforehand: Mandatory Review of High-Risk Templates

(1) Establish a Database of Celebrity Portraits

The platform should actively establish a comprehensive database of celebrity portraits. The database should contain detailed information about public tasks and celebrity portraits, including facial features for facial recognition; the authorization status of the portraits, clearly indicating whether they are allowed for use in scenarios such as AI face-swapping; the scope of use, defining in which fields and forms the portraits can be legally used. By building the database, the platform can systematically manage and coordinate the use of celebrity portraits, avoiding unauthorized abuse.

(2) Mandatory Review Mechanism

The platform should establish a strict mandatory review mechanism to ensure that any content involving celebrity portraits undergoes authorized verification. Unauthorized portraits are not allowed to be used in AI face-swapping. Only after authorized verification and confirming that the use of the portrait complies with the regulations, can it be used for AI face-swapping, thereby protecting the portrait rights of celebrities and safeguarding their legitimate interests.

(3) Compliance Review

The platform should arrange a dedicated review team to conduct compliance reviews for special cases where use is permitted, such as when others indicate that the portrait can be used except for commercial purposes. Thoroughly review whether the AI face-swapping content complies with the relevant regulations for portrait protection to ensure that every AI face-swapping content is legal and compliant, effectively preventing legal disputes and social controversies caused by content violations.

4.2 In Progress: Deployment of Risk Pre-screening Algorithm

(1) Deployment of the Pre-screening Algorithm

Train the image recognition model based on the celebrity portrait library constructed in the previous platform, and integrate the pre-screened image recognition algorithm that has been trained for use. When it is identified that both are completely consistent and there are no special circumstances allowing for its use, direct interception will be carried out, thereby controlling the risk at a relatively low level in the in-progress stage.

(2) Intercepting High-Risk Instructions

When a user posts high-risk instructions, such as those involving political figures or state secrets, a prompt will directly pop up on the page stating "The instruction contains sensitive words / The instruction does not conform to the norms, please change the instruction".

(3) Dynamic Risk Control

Based on the user's behavior and the characteristics of the generated content, conduct a risk assessment of the generated content and dynamically adjust the review standards. For certain high-risk scenarios, the platform should adopt stricter review requirements. For example, when a user posts the first high-risk instruction, the platform will issue a warning, and when the platform detects that the user is likely to post high-risk instructions again, it will directly suspend the account. That is, as

the number of historical unsafe behaviors increases, the frequency of user review and the platform's penalty intensity are directly proportional. The platform should dynamically adjust the review standards.

4.3 After the Fact: Deepfake Liability Insurance

As mentioned earlier, the platform should bear the responsibility for any infringement incidents. However, if all the liability is attributed to the platform, it might lead to users no longer using AI technology. Many instructions have ambiguous risk definitions and it is difficult to accurately determine whether they fall under high-risk instructions. Therefore, this article proposes deepfake liability insurance. Users will bear part of the insurance premium for claims. When the instructions posted by users do not pose any risks or are merely for entertainment, the platform does not charge any fees. When the instructions posted by users have a high risk level, the platform assesses the risk level and charges the corresponding fees based on the risk level. The higher the risk, the higher the fee. This fee is the cost for purchasing the liability insurance. If there is a subsequent infringement, the insurance company can handle the corresponding claims.

5. Summary

The rapid iteration and wide application of AI face-swapping technology have led to new characteristics such as anonymity, scale, and cross-platformization in portrait rights infringement. The traditional "one-to-one" protect rights model and static legal norms are unable to cope with the challenges brought by technology to the disintegration of rights. Therefore, it is urgent to establish a portrait rights protection system and governance framework that is compatible with technological development.

This paper first deconstructs the core contradiction in portrait rights protection in the AI face-swapping scenario from the dual dimensions of technological dissemination logic and legal application difficulties, and clarifies the three core issues of blurred rights boundaries, difficult infringement traceability, and unbalanced responsibility allocation. On this basis, it proposes a dual solution of "technology empowerment + system improvement": at the technical level, a dynamic consent mechanism and a full-chain traceability system are constructed to achieve full-process control from source authorization to infringement tracking.

At the same time, this paper focuses on the core hub role of platforms in the dissemination of AI face-swapping technology, defines the legal responsibilities and autonomous boundaries of platforms in content review, technical control, and infringement response, and finally forms a "technical regulation + legal improvement + platform autonomy" collaborative governance solution. The feasibility and adaptability of the solution are verified through typical cases.

This research provides a systematic solution to the portrait rights protection dilemma brought by AI face-swapping technology through theoretical construction and practical verification. It not only provides a clear path guidance for individual rights protection but also offers theoretical support and empirical references for relevant legislative revisions, regulatory policy formulation, and industry norm improvement, helping to balance the dynamic relationship between technological innovation and rights protection.

Future research can further expand in three directions: first, by combining emerging scenarios such as the metaverse and virtual humans, explore the cross-protection issues of AI face-swapping technology and virtual portrait rights; second, through large-sample empirical research, quantitatively analyze the implementation effect and optimization space of the collaborative governance solution in different types of platforms; third, compare the legal regulatory paths of different countries and regions to explore the collaborative mechanism for portrait rights protection in cross-border application of AI face-swapping technology.

References

[1] Y. Li, Z. Shi, and C. Liu, “Transformer-enabled generative adversarial imputation network with

selective generation (SGT-GAIN) for missing region imputation," IISE Transactions, vol. 56, no. Compendex, pp. 975–987, 2024.

[2] J. Peffer, "Owners of their faces: Privacy, copyright, and Africa's portrait photography," Res: Anthropology and Aesthetics, vol. 81–82, pp. 245–256, Dec. 2024.

[3] T. T. Nguyen, T. M. Dinh, H. T. H. Le, K. A. Pham, A. D. Nguyen, and H. K. Pham, "Impact of Perceived Benefits and Risks on Face Swap Applications Usage Intentions," Sage Open, vol. 15, no. 3, p. 21582440251367590, July 2025.

[4] E. Gerstner, "Face/Off: 'DeepFake' Face Swaps and Privacy Laws," DEFENSE COUNSEL JOURNAL, vol. 1, Jan. 2020.

[5] A. Preminger and M. B. Kugler, "The Right of Publicity Can Save Actors From Deepfake Armageddon," Berkeley Tech. L.J., 2024.

[6] H. Duquette, "DIGITAL FAME: AMENDING THE RIGHT OF PUBLICITY TO COMBAT ADVANCES IN FACE-SWAPPING TECHNOLOGY," The Journal of High Technology Law, Vol. 20, No. 1, Jan. 2020, Accessed: Nov. 27, 2025.

[7] R. Salariya and D. Malhotra, "ADFB: Anti-deepfake Framework for Facial Biometric Authentication Systems," in Proceedings of International Conference on Recent Innovations in Computing, Y. Singh, P. J. S. Gonçalves, P. K. Singh, and M. H. Kolekar, Eds., Singapore: Springer Nature, 2024, pp. 233–255.