International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

AI Consent-Driven Photo Security Platform

B. Balakrishna[1], M. Sruthi[2], P. Vyshnavi[3]

[1]Assistant Professor, CSE(AI&ML), Vignans Institute of Management and Technology for Women, HYD, India

[2,3]B.Tech 4th year Student, CSE (AI&ML), Vignan's Institute of Management and Technology for Women, Hyderabad, India.

Abstract:
As artificial intelligence keeps evolving at a fast pace, it's also bringing along some serious concerns—especially when it comes to manipulated images and deepfakes. These technologies can easily be misused, leading to problems like privacy invasion, identity theft, and even online harassment.
To tackle this, we're suggesting a platform that puts control back into the hands of individuals. The idea is simple: whenever someone uploads a photo, the system creates a unique digital signature based on their face and stores it securely. If someone later tries to edit that image or use it to create a deepfake, the system recognizes the signature and immediately notifies the original owner. Nothing can move forward unless they give clear permission.
On top of that, every action on the platform is recorded in a secure and tamper-proof log. This means there's always a clear record of what happened and who was involved, adding an extra layer of trust and accountability.
By combining facial recognition technology with user consent and transparent tracking, this approach focuses on protecting people—not just data—making the digital space a bit safer and more respectful.

Index Terms: Deepfake Detection, Image Manipulation Se- curity, Consent-Driven Systems, Facial Recognition Technology, Digital Identity Protection, Tamper-Proof Audit Systems.

I. INTRODUCTION

Today, artificial intelligence and image processing technolo- gies are evolving faster than ever. One area that has attracted a lot of attention is deepfake technology, which makes it possible to create highly realistic but fake images and videos by altering a person's facial features. While this can be useful in fields like entertainment and media, it also raises serious concerns when misused, especially regarding personal privacy.
One major issue is that deepfakes can be created without a person's knowledge or permission. This opens the door to identity misuse, reputational harm, and various forms of online abuse. With the rapid growth of social media, images are being shared more widely than ever, increasing the chances of such misuse. Most existing solutions focus on detecting deepfakes after they have already been created, rather than stopping them beforehand. At the same time, there is still no strong system that allows individuals to truly control how their facial images are used online.
To address these problems, this research introduces an AI-based Consent-Driven Photo Security Platform. The goal of this system is to protect individuals from unauthorized manipulation of their images. It works by using artificial intelligence to recognize faces in uploaded images and gener- ate a unique digital facial signature for each user. Whenever someone attempts to edit an image or create a deepfake, the system checks for this signature and sends a consent request to the original owner. The process only continues if the person approves it; otherwise, the attempt is blocked and recorded.
By focusing on user permission and accountability, this platform offers a more proactive approach to image security. It not only helps protect individual privacy but also encourages the ethical and responsible use of AI-powered image editing technologies.

II. RELATED WORK

Recent progress in artificial intelligence has played a major role in the rise of deepfake media, making it possible to create highly realistic manipulated images and videos. A key technology behind this is the Generative Adversarial Network (GAN), introduced by Ian Goodfellow and his team in 2014. GANs work using two neural networks—one that generates synthetic content and another that evaluates how realistic it looks. Together, they can produce media that is often difficult to distinguish from real content. While this has opened new possibilities in digital creation, it has also raised serious concerns about misuse and manipulation.

In response to these risks, many researchers have focused on detecting deepfake content after it has already been created and shared. For instance, Yuezun Li and his team have worked on identifying manipulated facial images by analyzing inconsistencies and visual artifacts. Similarly, Andreas Ro¨ssler and his team introduced the FaceForensics++ dataset, which has become widely used for training and evaluating deepfake detection systems. Although these efforts have improved de- tection methods, they mainly address the problem after the damage may already be done.

Other research has explored the use of facial recognition technology to verify identities in digital media. This approach relies on identifying unique facial features to authenticate individuals. While effective for identity verification, these systems typically do not give individuals control over how their images are used, especially in cases involving editing or deepfake generation.

More recently, there has been interest in secure logging methods, such as blockchain-based systems, to track owner- ship and usage of digital media. These approaches can improve transparency and accountability by maintaining tamper- resistant records. However, like other existing solutions, they often lack mechanisms that actively involve user consent in the process of image manipulation.

In contrast to these existing approaches, the proposed AI Consent-Driven Photo Security Platform introduces a different perspective. Instead of focusing only on detection or verifica- tion, it emphasizes prevention and user control. By creating a unique digital facial signature and requiring explicit consent before any manipulation occurs, the system aims to provide a more secure and user-centered solution for managing digital images.

III. PROPOSED SYSTEM

The proposed system introduces an AI-powered, consent- based photo security platform designed to prevent unautho- rized image editing, sharing, and deepfake creation. Unlike traditional approaches, it focuses on proactive protection by combining facial recognition, deep learning techniques, and user consent mechanisms.

At the heart of the system is a facial signature generation process. Each uploaded image is analyzed to capture unique facial features, which are then converted into a secure digital representation referred to as a “face-lock.” This face-lock is stored in encrypted form and is later used to identify individuals during any future image-related activity.

Whenever an image is edited, shared, or processed, the system activates a face-matching and verification step. It compares the faces in the new image with the stored face-locks to check for a match. If a match is found, the system further analyzes the image using deep learning models to detect any signs of manipulation, including potential deepfake content.

A key feature of the platform is its real-time consent mechanism. As soon as a registered user’s face is detected, the system automatically sends them a request for permission. The requested action—whether editing, sharing, or generating new content—only proceeds if the user explicitly approves it. If consent is denied or not provided, the system immediately blocks the action.

In addition, the platform maintains secure and tamper- resistant logs of all activities. This ensures that every ac- tion is recorded and can be traced when needed, improving transparency and accountability. By addressing the gaps in existing solutions, this system provides a more reliable and user-focused approach, promoting ethical use of digital images while protecting individual privacy and identity.

IV. OVERVIEW

The rapid growth of artificial intelligence, particularly in computer vision and deep learning for image generation, has completely changed how digital images are created, shared, and used. While these advancements have opened the door to many innovative applications, they have also introduced serious challenges, especially in the form of deepfakes and image manipulation. These issues raise important concerns around privacy, identity theft, and the ethical use of personal data.

To address these challenges, this paper presents an AI- powered photo security platform focused on both protection and user control. The system uses facial recognition technol- ogy to create a unique digital signature for each user's face, allowing it to identify individuals in images accurately. It also integrates deep learning models to detect whether an image has been altered or artificially generated.

A key strength of the platform is its consent-driven ap- proach. Before any image is edited, shared, or manipulated, the system seeks explicit approval from the user. It also provides real-time notifications to keep users informed of any activity involving their images, while maintaining secure logs to ensure transparency and accountability.

Overall, the proposed platform aims to give users greater control over their digital presence. By combining security, consent, and intelligent detection, it promotes safer and more responsible use of AI technologies, helping build trust in an increasingly digital world.

V. SYSTEM ARCHITECTURE MODULES

A. System Architecture

The architecture of the proposed AI-driven photo security system is designed to be modular and layered, ensuring strong security, efficient image processing, and user-focused consent management.

The system is organized into three main layers: the User Interface Layer, the Application Layer, and the Data Layer. The User Interface Layer handles all interactions with the user, such as uploading images, receiving notifications, and providing consent. The Application Layer performs the core operations of the system, including face recognition, deepfake detection, consent handling, and decision-making. The Data Layer is responsible for securely storing user information, facial signatures (face-locks), and system activity logs.

When a user uploads an image, the system first generates a unique facial signature and stores it in the database. Later, if someone attempts to edit or share an image, the system runs face recognition and deepfake detection processes. If a matching facial signature is found, a real-time consent request is sent to the respective user. The system then either allows or blocks the requested action based on the user's response. Every step in this process is recorded to ensure transparency and accountability.

Overall, this layered architecture supports secure image handling, continuous monitoring, and effective prevention of unauthorized image manipulation, while keeping the user in full control.

B. System Modules

The system, as designed, comprises the following system modules:

1) User Management Module: This module handles user registration, authentication, and profile management, en- suring that only authorized users can access the system.

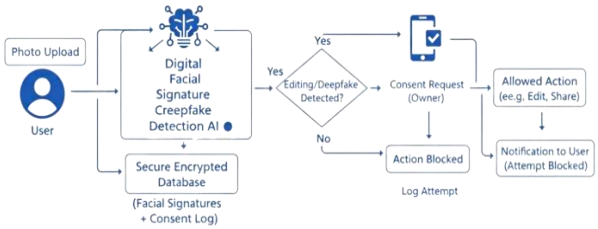

Fig. 1. System Architecture

It incorporates secure methods such as password en- cryption and verification to protect user credentials and maintain overall system security.

2) Photo Upload and Storage Module: This module allows users to upload their photos in a secure manner. During the upload process, the system performs image prepro- cessing to enhance security and prevent any unautho- rized access or misuse.

3) Facial Signature Generation Module: This module ap- plies deep learning techniques to extract distinctive facial features from uploaded images and generate a unique face-lock signature for each user.

4) Deepfake Detection and Monitoring Module: This mod- ule uses AI-based methods to continuously monitor how images are used, identifying any signs of manipulation, including the creation of deepfake content.

5) Consent Verification Module: This module sends real- time consent requests to users whenever their face is detected in an image processing activity. It also records the user's response to ensure proper tracking and ac- countability.

6) Authorization and Decision Module: This module pro- cesses user responses to consent requests, allowing or denying actions such as editing or sharing images based on the user's decision.

7) Notification and Alert Module: This module delivers real-time alerts to users through multiple channels, such as push notifications and email, ensuring they stay informed about any activity involving their images.

8) Logging and Reporting Module: This module keeps a detailed record of all system activities, including image uploads, detection results, and user responses, ensuring transparency and easy tracking.

9) Security and Encryption Module: This module applies security measures such as encryption to protect data and ensure safe communication within the system.

10) Admin Dashboard Module: This module is designed for system administrators to monitor overall system activity, manage users, and ensure the platform operates smoothly and securely.

VI. IMPLEMENTATION DETAILS

The proposed system is implemented using a modular de- sign that integrates AI technologies such as facial recognition, deep learning-based deepfake detection, and a consent-driven authorization mechanism. The implementation is carefully designed to ensure scalability, strong security, and efficient real-time performance.

A. Development Environment

The system is primarily developed using Python for backend processing and integration with AI models. To build RESTful APIs, frameworks such as Flask or FastAPI can be utilized. For the user interface, standard web technologies like HTML, CSS, and JavaScript are used to create an interactive experience. On the AI side, deep learning frameworks such as Tensor- Flow or PyTorch are used to design and train models, while OpenCV supports image processing tasks. During develop- ment, tools like Visual Studio

Code, Jupyter Notebook, and GitHub are used to streamline coding, testing, and version control.

B. Core Functional Implementation

- User Authentication Management: The system provides secure user authentication by using encrypted credentials along with a token-based mechanism. This ensures that only verified users are able to access the platform.
- Image Upload and Preprocessing: The images are then preprocessed by applying steps such as resizing, normal- ization, and noise reduction. This prepares them for more accurate and efficient analysis in the later stages.
- Facial Signature Generation: The system uses a deep learning-based face recognition model to extract key fa- cial features and generate a unique, non-reversible digital signature, known as a face-lock. This signature is then securely stored in the database for future reference.
- Deepfake Detection Mechanism: The system uses deep learning models to analyze images and accurately detect deepfake content. This helps ensure that only genuine and verified images are processed further by the system.
- Consent Verification Workflow: When a matching face is detected during an image processing request, the system immediately sends a real-time consent request to the user. It then proceeds based on the user's response, either allowing or blocking the action.
- Decision and Authorization Engine: The system then approves or rejects the request based on the consent provided by the user.

C. Data Storage and Security

The system uses databases such as MySQL or MongoDB to store user information, facial signatures, and activity logs. Data is protected through encryption, while secure communication is maintained using protocols like HTTPS and SSL/TLS.

In addition, all system activities—such as image uploads, detection results, and user consent—are recorded in logs to ensure transparency and accountability.

D. Notification and Deployment

The system includes real-time notification services that keep users informed about consent requests and any potential misuse of their images. Notifications can be delivered through mobile push alerts, emails, or in-app messages.

For deployment, the platform can be containerized using Docker and hosted on cloud services such as AWS or Azure, allowing it to efficiently handle multiple simultaneous re- quests.

VII. ALGORITHM

The proposed system uses a structured algorithm for the safe manipulation of images, deepfake detection, and the use of the concept of consent for authorization. The system uses a combination of facial recognition, AI-based verification, and approval processes for the safe manipulation of images.

A. Algorithm: Consent-Driven Deepfake Prevention

Input: Uploading image I, Database D for facial signatures

Output: Allow or Block the request for image manipulation

B. Process

1) Start
2) User uploads the image I
3) Preprocess the image I
4) Extract facial features
5) Generate facial signature F (face-lock)
6) Store the facial signature F in the database D for the user's images
7) On receiving the request for editing/sharing the image
8) Extract facial features for the image I
9) Compare the facial features with the facial signatures in the database D

10) If a match is found:
- Detect deepfake for the image I
- Send a request for consent to the original user
- Wait for the response

11) If the user allows the request
- Allow the manipulation of the image

12) Else (user does not allow or does not respond)
- Block the manipulation of the image

13) Else (no face detected)
Block the request as suspicious

14) Log all activities (requests, decisions, detections)

15) End

VIII. RESULTS AND DISCUSSION

The proposed AI-based photo security system was tested to determine its effectiveness in facial recognition, deepfake detection, and consent-based authorization. Based on the re- sults, the system is effective in ensuring that unauthorized modifications of photos do not take place while maintaining user privacy.

A. Functional Evaluation

Facial recognition was performed accurately, generating unique face-lock signatures that could be reliably identified even across different photos. The deepfake detection feature proved effective, successfully identifying any form of image manipulation before further processing could occur.

The consent verification system also functioned as intended, allowing users to approve or deny actions in real time. Based on their responses, the system enforced access control, pre- venting any unauthorized modifications to images and ensuring user privacy and security.

B. Performance Metrics

The performance of the system was tested using the follow- ing parameters:

1) **Detection Accuracy:** The performance of deep learning models was highly accurate in detecting facial matches and recognizing manipulated images.
2) **Latency:** The system ensured low latency in responding to consent requests and decision-making processes.
3) **Security:** The encryption process ensured that sensitive information was securely stored and transmitted.
4) **Scalability:** The system design is flexible enough to handle multiple user requests.

C. Comparative Discussion

The proposed system can be compared to existing solutions that focus primarily on verifying user consent. Its key advan- tage lies in the integration of deepfake detection alongside user authorization. This dual-layer approach enhances the system's reliability and accuracy, reducing the risk of violating user consent through manipulated or deepfake content.

Additionally, features such as real-time notifications and secure logging further strengthen trust and transparency in the system. However, challenges may arise when handling large- scale datasets or when more sophisticated deepfake techniques are developed, which could require ongoing updates and improvements to maintain system effectiveness.

D. Discussion

Experimental evaluation demonstrates that the proposed sys- tem successfully integrates facial recognition, deepfake detec- tion, and consent-based authorization into a unified framework. By combining content authenticity checks with user consent, it addresses many of the limitations seen in previous systems. One of the system's key strengths is its proactive security mechanism, which ensures that user consent is obtained before any image manipulation occurs. This approach makes it

much harder for malicious actors to misuse content in ways that could harm others.

Real-time notifications further enhance the system by en- abling users to make timely decisions about how their images are used. Additionally, the use of immutable logs ensures transparency and accountability, which are essential in today's digital environment.

However, certain limitations remain. Deepfake detection accuracy may vary depending on the complexity of the ma- nipulated content, and system performance could be affected when handling large-scale datasets.

Overall, these findings indicate that the proposed system has strong potential to provide a robust, user-centric solution for safeguarding digital images, combining security, control, and transparency in a single platform.

IX. CONCLUSION

In this paper, an AI-driven consent-based photo security system is proposed to mitigate the rising threats of image tampering and deep learning-based fake media generation. This system ensures that users have complete control over the use and sharing of their digital media.

The system incorporates effective proactive security mea- sures with user-centric permission controls to enable secure image handling and prevent any form of image tampering or deep learning-based fake media generation. The imple- mentation of real-time notifications and immutable logs also improves the overall system's transparency and user trust.

The experimental analysis shows that the system is effective in ensuring the secure handling of digital media through facial recognition, identifying image tampering, and enforcing user consent. This system is also better compared to traditional ap- proaches, as it incorporates an overall framework for verifying image authenticity and user consent.

In conclusion, this system is an effective solution for ensur- ing the secure handling and sharing of digital media in today's AI-driven world. This system is also beneficial for promoting the ethical use of artificial intelligence and ensuring the overall privacy of digital media users.

REFERENCES:

1) H. Kim, "Novel Deep Learning-Based Facial Forgery Detection for Effective Biometric Recognition," Applied Sciences, vol. 15, no. 7, p. 3613, 2025.
2) N. Kumar and A. Kundu, "SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data An- alytics," Sensors, vol. 24, no. 19, p. 6300, 2024.
3) K. Suresh, S. Sariyu, P. A. Dhapte, K. Subash Chandra, and T. Sathvika, "Enhancing Privacy in Social Media Photo Sharing: A User-Centric Framework Integrating Multi-Party Consent and Blockchain Technologies," In- ternational Journal of Computer Engineering in Research Trends, vol. 11, no. 1, pp. 31–37, 2024.
4) J. M. Mase, N. Leesakul, G. P. Figueredo, and M. T. Torres, "Facial Identity Protection Using Deep Learning Technologies: An Application in Affective Computing," AI and Ethics, vol. 3, no. 3, pp. 937–946, 2023.
5) Z. Akhtar, "Deepfakes Generation and Detection: A Short Survey," Journal of Imaging, vol. 9, no. 1, p. 18, 2023.