Secure Image Publishing System Using Facial Identity Verification

Mrs. N. Sujithaa[1], U. Jeevarathinam[2], N.R.S. Ramana[3], S. Jeyasakthi[4]
[1]Assistant Professor, Dept of Computer Science and Engineering
[2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4] Sree Sowdambika College of Engineering, Chettikurchi, Virudhunagar, Tamilnadu.

Abstract- *With the rapid growth of social media platforms, unauthorized sharing and misuse of personal images has become a major privacy concern. Many users upload photos containing other individuals without their permission, which may lead to privacy violations and identity misuse. This paper proposes a Secure Image Publishing System Using Facial Identity Verification that detects faces in uploaded images and verifies whether the person in the image has granted permission for the upload. The system uses computer vision techniques to detect faces and compare them with registered user data stored in a secure database. If a match is found, the system sends a notification to the identified person and requests approval before allowing the image to be published. The proposed system integrates technologies such as Python, OpenCV, and machine learning–based face recognition to ensure accurate identification and permission control. By introducing an automated permission mechanism, the system helps prevent unauthorized photo sharing and enhances privacy protection on social media platforms. Experimental results demonstrate that the system can effectively detect faces and manage image ownership permissions with reliable performance.*

Keywords: Face Recognition, Image Ownership Protection, Privacy Protection, Computer Vision, Image Permission System, Social Media Security, Artificial Intelligence

I. INTRODUCTION

With the rapid growth of social media platforms, sharing images has become a common activity among users. However, many images uploaded online contain other individuals whose consent has not been obtained. This leads to serious privacy concerns and misuse of personal identity. Unauthorized sharing of images may result in cyberbullying, identity theft, and violation of personal rights.

Traditional social media platforms do not provide an automatic mechanism to verify whether the person appearing in an image has permitted its upload. As a result, images containing multiple individuals can be shared without the knowledge or approval of the people in them.

To address this problem, this project proposes a Secure Image Publishing System Using Facial Identity Verification. The system detects faces present in an uploaded image and compares them with registered user data stored in a database.

If a face match is found, the system automatically sends a notification to the identified individual requesting permission before allowing the image to be published.

By integrating computer vision and machine learning techniques, the proposed system aims to enhance privacy protection and ensure that users have control over images that contain their faces.

II. LITERATURE REVIEW

Several research studies have been conducted in the field of face recognition and privacy protection systems.

1) **Matsumoto et al. (2025)** proposed a person identification system that focuses on improving face image recognition accuracy while maintaining user privacy. Their system evaluates different recognition techniques and discusses how privacy protection can be maintained when using face data. The study highlights the importance of balancing identification accuracy with data security.
2) **Laishram et al. (2025)** presented a survey on privacy-preserving face recognition systems. The research analyses possible data leakages that may occur in face recognition systems and suggests various security solutions to protect sensitive biometric information. The study emphasizes the need for secure systems that prevent unauthorized access to facial data.
3) **Manikanta and Jeevan Babu (2025)** developed a face recognition system using Convolutional Neural Networks (CNN). Their work focuses on improving recognition accuracy by using deep learning models for feature extraction and classification. The results demonstrate that CNN-based methods provide higher accuracy compared to traditional recognition techniques.

4) **Pandey et al. (2025)** proposed a human face recognition system based on image processing techniques. Their research explains how face detection, feature extraction, and matching can be implemented using computer vision methods. The study shows that image processing techniques can effectively identify individuals in digital images
5) **Attrapadung et al. (2025)** introduced fast and privacy-preserving protocols for 1-to-N face identification. Their work focuses on improving identification speed while protecting biometric data from potential security threats. The research highlights the importance of secure computation methods in large-scale face recognition systems.

III. PROBLEM STATEMENT

Social media platforms currently lack an automated mechanism to verify whether individuals appearing in an image have authorized its upload. This leads to unauthorized sharing of personal photos and privacy violations. Therefore, a system is required that can automatically detect faces in images and obtain permission from the identified individuals before allowing the image to be published.

IV. OBJECTIVE

The main objectives of this project are:

- To detect human faces in uploaded images.
- To identify individuals using face recognition techniques.
- To compare detected faces with a registered user database.
- To notify the identified user and request permission before publishing the image.
- To prevent unauthorized image sharing and enhance privacy protection.

V. EXISTING SYSTEM

In the existing social media systems, users can upload images freely without verifying whether the people appearing in the image have given permission. Many platforms provide features such as photo tagging and face recognition suggestions, but these systems mainly focus on identifying individuals rather than protecting their privacy. Some face recognition systems are used for applications like security surveillance, attendance systems, and identity verification. These systems can detect and recognize faces in images using computer vision and machine learning techniques. However, they do not include a mechanism to control image sharing based on the consent of the individuals present in the image.

As a result, images containing other people can be uploaded and shared without their knowledge or approval. This may lead to privacy violations, misuse of personal photos, and identity-related issues. Therefore, the existing systems lack an automated method to ensure that individuals have granted permission before their images are published online.

VI. PROPOSED SYSTEM

The proposed system introduces an intelligent mechanism that verifies image ownership before publication. When a user uploads an image, the system performs face detection to identify all faces present in the image.

Each detected face is then compared with a stored face database using a face recognition model. If a match is found, the system sends a notification to the identified person requesting approval. The image will only be published if permission is granted.

This approach ensures that individuals maintain control over images containing their faces and reduces unauthorized sharing on social media platforms.

VII. METHODOLOGY

The working process of the system consists of several steps:

- **User Registration**
  Users register in the system and upload their facial images for identity verification.

- **Image Upload**
  A user uploads an image containing one or more individuals.

- **Face Detection**
  The system detects faces in the uploaded image using computer vision techniques.

- **Face Recognition**
  The detected faces are compared with the stored facial database.

- **Permission Request**
  If a face match is found, the system sends a notification to the identified person.

- **Approval Process**
  The image is published only if permission is granted by the identified user

VIII. SYSTEM ARCHITECTURE

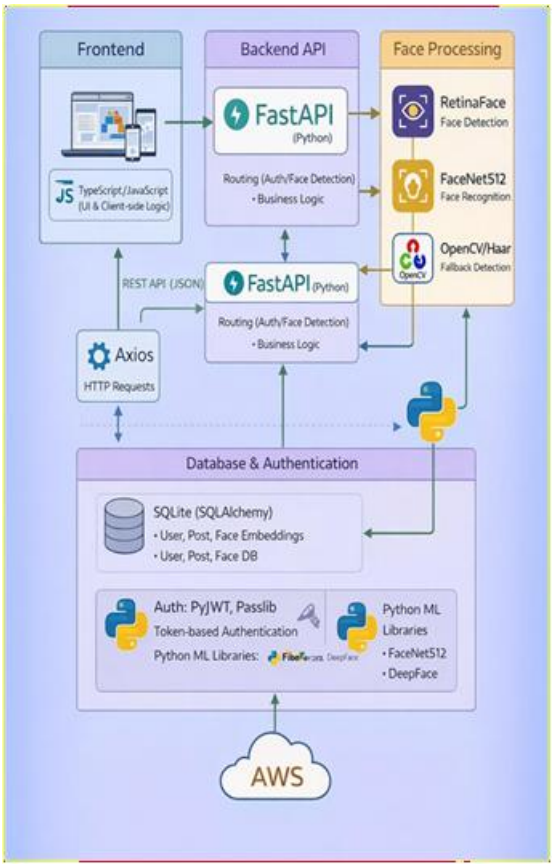

Fig. 1 System Working Architecture

The architecture of the proposed Face Recognition Based Image Permission System consists of multiple modules that work together to process images and control sharing permissions.

Frontend:

The frontend is developed using TypeScript/JavaScript and provides the user interface where users can upload images and interact with the system.

Backend API:

The backend is implemented using FastAPI (Python) which handles routing, authentication, and system business logic.

Face Processing Module:

The system performs face detection and recognition using Retina Face for face detection, FaceNet512 for recognition, and OpenCV/Haar as a fallback detection method.

Processing Layer:

The FastAPI processing layer manages authentication and face detection requests received from the frontend.

Database:

The system uses SQLite with SQL Alchemy to store user data, posts, and facial embedding.

Authentication:

Security is provided using PyJWT and Passlib, enabling token-based authentication.

Python ML Libraries:

Machine learning libraries such as FaceNet512 and DeepFace are used for facial feature extraction and comparison.

Deployment:

The system can be deployed on cloud platforms such as AWS for scalable online operation.

IX. RESULT AND DISCUSSION

Face recognition-based image permission system created as social media web application.

Following output screen shots shows how the application works successfully.

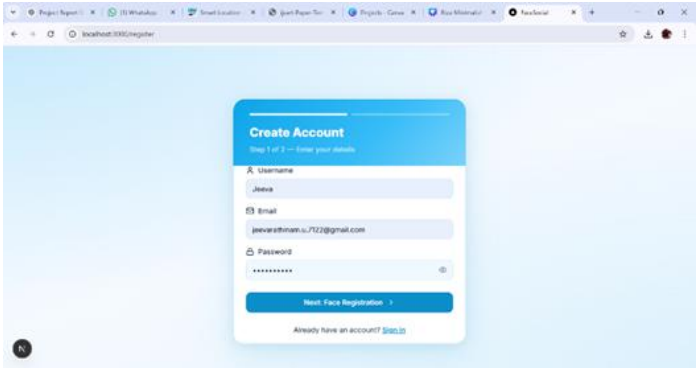

Fig. 2 User A Create Account

User A Create account in this app using his User name, Mail ID and Password

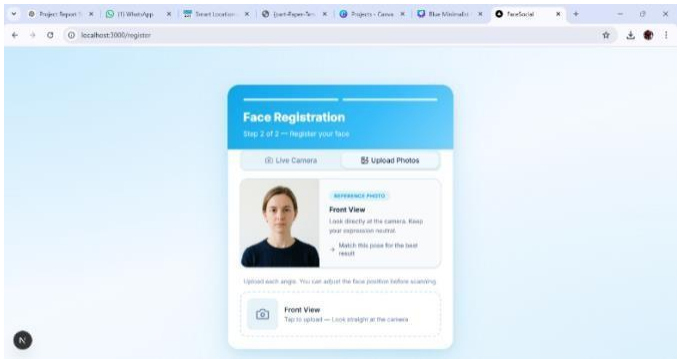

Fig. 3 User A Register his Face

In this page user A upload his face photos to register in this app.

Fig. 4 User A Registered his face

User A Registered his face's Front, Left and Right-side views successfully.

Like this User B also create an account in this app and using this app

Fig. 5 User B Register his Face

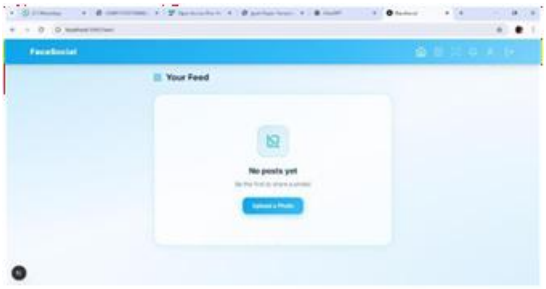

Fig. 6 Home Page

By clicking Upload a Photo users can post the photos from their Gallery

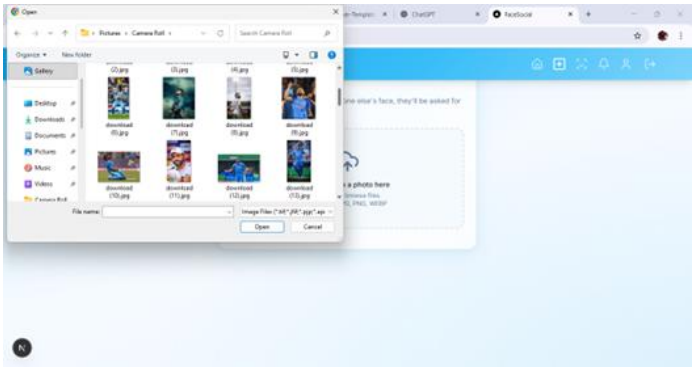

Fig. 7 User B Selecting the photo to post

Fig. 8 User B Upload the photo

In this Picture User B try to upload the photo which contains user A's Face

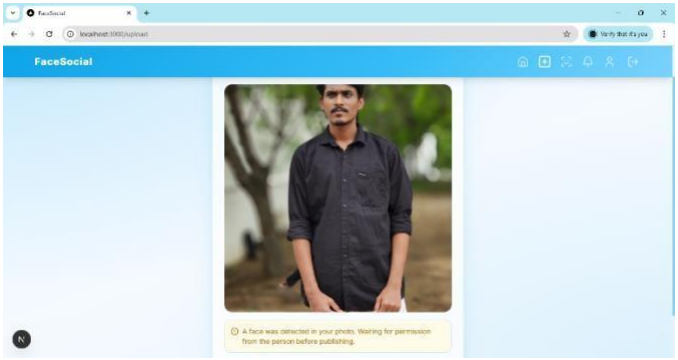

Fig.9 Photo Not Uploaded

The app does not Allow the user to Publish this photo, because it detects the face and recognized the face it's not user B's Face

Fig. 10 Notification for User A

User A received the Permission request from User B to Publish the photo that contains his face.

Fig. 11 Notification for User B

User B received the Reply message from User A, that the User A Denied his Request to post user A's Photo

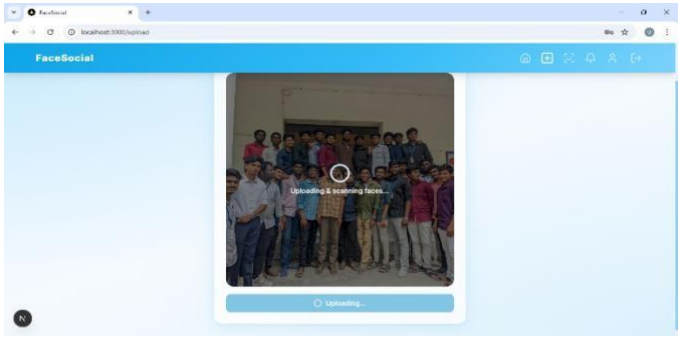

Fig. 12 User C Upload the Group Photo

Now User C try to upload the Group Photo that contains Multiple Persons Face including User A, User B and User C

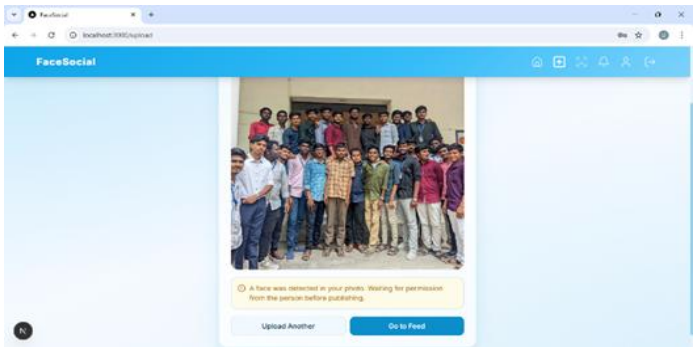

Fig. 13 Uploading Stopped

This app does not allow the User C to upload this Group Photo, because it contains multiple persons Face. here that's not Problem. This app recognized two registered Users Face in this Group photo so it stopped the uploading.

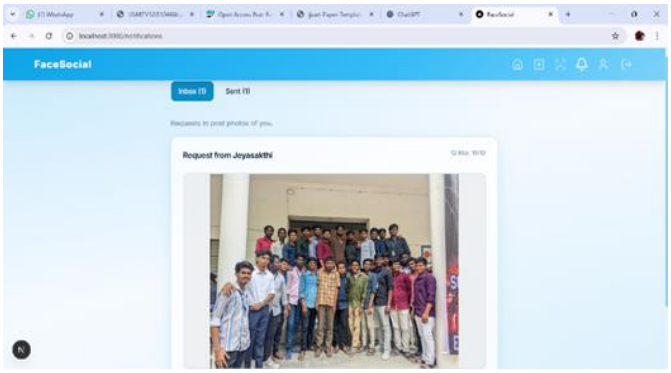

Fig. 14 Notification for User A

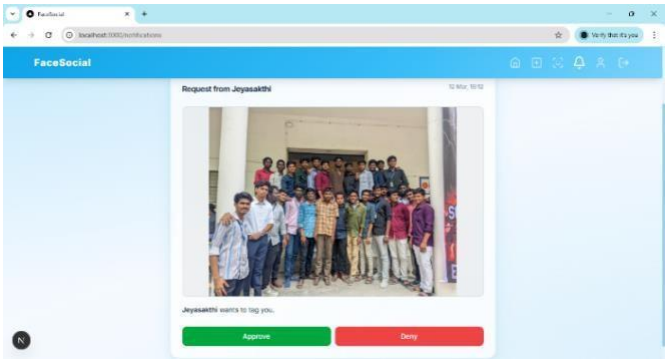

Fig. 15 Notification for User B

User a and User B Received the Permission request from user C.

Fig. 16 Notification for User C from User A

Fig. 17 Notification for User C from User B

Above the two pictures shows the Request Approved Notification from User A and User B

Fig. 18 Image in Feed

User A and User B allowed to publish the post so this photo is published and it will be appeared in everyone's Feed

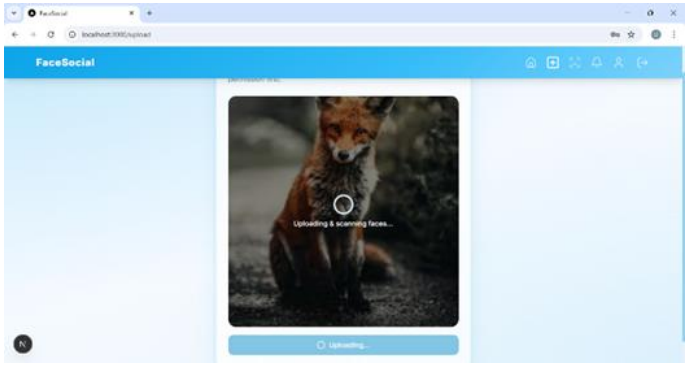

Fig. 19 User C Upload the Photo

User C try to upload this photo it does not contains any human face.

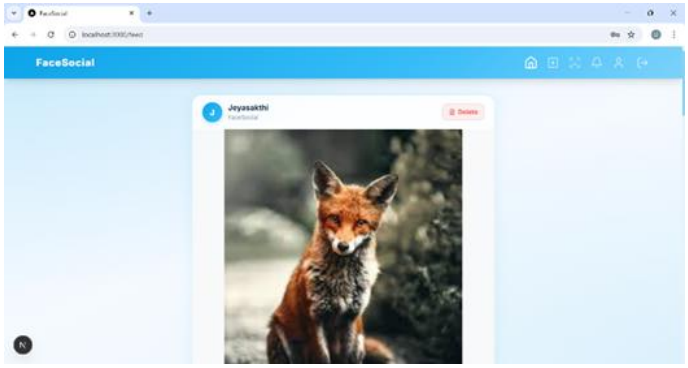

Fig. 20 Uploaded Successfully

This photo uploaded Successfully without any restriction, because it does not Contains any Human Face

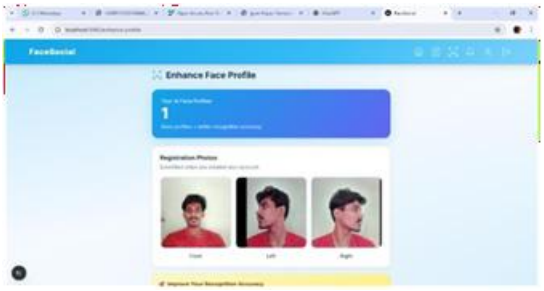

Fig. 21 User A's Registered Face

This are the different side faces of user A. User can see their faces which he used to register in the app

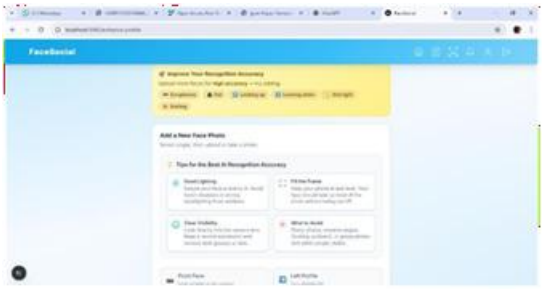

Fig.22 Increase Accuracy

This Shows how to increase the accuracy of face detection and recognition.

Fig. 23 Different Face Photos

User can upload different face photos that isinstructed in this image to improve the accuracy of face detection and recognition.

The proposed system successfully detects faces in uploaded images and compares them with stored user data. The system sends permission requests to identified users and restricts image publication until approval is granted.

Experimental results show that the system can accurately detect faces and provide reliable permission control, thereby improving privacy protection in social media environments.

X. ADVANTAGES

- Prevents unauthorized image sharing
- Enhances user privacy protection
- Provides automated permission control
- Reduces misuse of personal photos
- Improves trust in social media platforms

XI. CONCLUSION

This paper presented a **Secure Image Publishing System Using Facial Identity Verification** to enhance privacy protection on social media platforms. The system detects faces in uploaded images and verifies the identity of individuals using face recognition techniques. If a recognized person appears in the image, the system requests permission before allowing the image to be published.

The proposed system integrates technologies such as **FastAPI, Next.js, OpenCV, and FaceNet512** to perform face detection and recognition efficiently. By introducing a permission-based mechanism, the system helps prevent unauthorized image sharing and protects user privacy.

Overall, the system demonstrates how combining Secure Image Publishing System Using Facial Identity Verification can improve security and provide better privacy management in digital environments.

REFERENCES

[1] Alhayani, Bilal Salih Abed and Rane, Prof. Milind, "Face Recognition System by Image Processing". International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 5, Issue 5, May (2014), pp. 80-90

[2] Divyarajsinh N. Parmar, Brijesh B. Mehta,"Face Recognition Methods & Applications". International Journal of Computer Technology & Applications, Vol 4 (1), pp. 84-86, Jan-Feb 2013

[3] Faizan Ahmad, Aaima Najam, Zeeshan Ahmed. "Image-based Face Detection and Recognition: "State of the Art"". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012 ISSN (Online): 1694-0814

[4] Eimad Abusham, Basil Ibrahim, Kashif Zia and Muhammad Rehman. "Facial Image Encryption for Secure Face Recognition System". MDPI – Multidisciplinary Digital Publishing Institute, Vol. 12, Issue 3, 3 February 2023

[5] P. Venkatesh, Pramod Sreedharan. "Face Recognition Based Security System". 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)

[6] Eimad Abusham, Basil Ibrahim, Kashif Zia and Muhammad Rehman. "Facial Image Encryption for Secure Face Recognition System". 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). 24-28 June 2024

[7] Guanhao Yang; Wei Feng; Jintao Jin; Qujiang Lei; Xiuhao Li; Guangchao Gui; Weijun Wang. "Face Mask Recognition System with YOLOV5 Based on Image Recognition". 2020 IEEE 6th International Conference on Computer and Communications (ICCC), 11-14 December 2020

[8] Xingyuan Wang & Ziyu Leng. "Image encryption algorithm based on face recognition, facial features recognition and bionic sequence". Published in Springer Nature, Volume 83, pages 31603–31627. 18 September 2023

[9] Amal Almansour, Ghada Alsaeedi, Haifaa Almazroui, Huda Almuflehi. "I-Privacy Photo: Face Recognition and Filtering". ICCDA '20: Proceedings of the 2020 4th International Conference on Compute and Data Analysis. 17 April 2020

[10] Maliha Khan, Sudesha Chakraborty, Shaveta Khepra, Rani Astya. "Face Detection and Recognition Using OpenCV". 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)**.** 18-19 October 2019