IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307036|

Identification of Face Spoofing Using Deep Learning Technique

Akshatha G R

PG Student, Department of Master of Computer Applications, PES Institute Technology and Management, Shivamogga, Karnataka, India

ABSTRACT: The project aims to develop a robust face recognition and anti-spoofing system integrated within a graphical user interface (GUI) using Python's tkinter framework. The system utilizes the MiniFastnet algorithm variants (V1, V2, V1SE, and V2SE) for face recognition and leverages anti-spoofing models from the Silent-FaceAnti-Spoofing repository to enhance security against facial spoof attacks. The GUI allows users to perform actions such as logging in, logging out, and registering new users through a webcam interface. Key functionalities include real-time face detection and recognition using OpenCV and face_recognition libraries, which enable the system to match detected faces with stored facial embeddings. Upon successful recognition, users are logged in with their respective names and timestamps recorded in a `log.csv` file. In cases where no matching face is found, users are prompted to register as new users. The project also incorporates error handling and user feedback mechanisms using tkinter's message box module to notify users of successful logins, unrecognized faces, or spoofing attempts. Additionally, the system ensures data integrity by securely storing facial embeddings in pickle files within a designated database directory. Overall, the project aims to provide a user-friendly and secure authentication solution utilizing advanced face recognition and anti-spoofing techniques, suitable for applications requiring reliable user identification and access control.

KEYWORDS: Image Captioning, Deep Learning, Convolutional Neural Networks, Multimedia Applications.

I. INTRODUCTION

In In the realm of modern security systems, biometric authentication, particularly facial recognition, has emerged as a powerful tool for user identification and access control. This project delves into the development of comprehensive face recognition and anti-spoofing system integrated within a graphical user interface (GUI) using Python's tkinter framework. The primary objective is to create a robust solution capable of accurately recognizing individuals based on their facial features while mitigating risks associated with facial spoofing attacks. Facial recognition technology leverages advanced algorithms such as MiniFastnet (including variants V1, V2, V1SE, and V2SE) to perform realtime face detection and feature extraction. These algorithms enable the system to match detected faces against stored facial embeddings, ensuring secure authentication of users. Concurrently, anti-spoofing models sourced from the Silent-Face-Anti-Spoofing repository are employed to detect and prevent spoofing attempts by distinguishing between genuine faces and deceptive images or videos. The graphical user interface provides an intuitive platform for users to interact with the system, facilitating actions such as user login, logout, and registration through a webcam interface. Real-time feedback mechanisms and error handling functionalities are integrated using tkinter's messagebox module to notify users of authentication outcomes and potential spoofing incidents. Moreover, the system maintains a log of user activities, recording login and logout timestamps along with user identities in a structured `log.csv` file for audit and security monitoring purposes.

II. RELATED WORK

Here we have selected few key literatures after exhaustive literature survey and listed as below:

1. Sun et al. (2007) [1] introduced a blinking-based live face detection method utilizing conditional random fields. This approach leverages the natural, involuntary blinking of human eyes to distinguish between live faces and static images or videos, providing an effective means to counteract spoofing attempts.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307036|

2. Karson (1983) [2] explored the connection between spontaneous eye-blink rates and dopaminergic systems. This research, while primarily focused on neurological aspects, provides a foundational understanding of the physiological basis for using blink rates in live detection systems.
3. Singh, Joshi, and Nandi (2014) [3] presented a technique for face recognition with liveness detection using both eye and mouth movements. Their approach combines multiple facial movements to enhance the accuracy of live detection. The inclusion of mouth movements alongside eye blinks adds an additional layer of complexity for spoofing attempts, making the system more robust against sophisticated attacks.
4. Killioğlu, Taşkiran, and Kahraman (2017) [4] focused on anti-spoofing in face recognition through pupil tracking. Their method leverages the unique patterns and dynamics of pupil movement, which are difficult to replicate in static images or pre-recorded videos.
5. Dhawanpatil and Joglekar (2018) [5] reviewed the use of Local Binary Pattern (LBP) descriptors in spoof face recognition. LBP descriptors are effective in texture analysis, enabling the detection of subtle differences between live faces and spoofing materials. This technique's strength lies in its ability to capture fine-grained texture details that are often absent in spoofing attempts.
6. Albakri and Alghowinem (2019) [6] investigated the effectiveness of depth data in liveness face authentication using 3D sensor cameras. Depth data provides a three-dimensional view of the face, allowing the system to detect inconsistencies in depth that are characteristic of spoofing artifacts like photos or videos. This approach enhances the robustness of liveness detection by leveraging spatial information that is difficult to fake convincingly.

III. PROBLEM STATEMENT

The project addresses the challenge of developing an effective face recognition and anti-spoofing system to enhance security and reliability in user authentication processes. Traditional authentication methods, such as passwords or PINs, are susceptible to vulnerabilities like theft or misuse. Facial recognition offers a promising alternative by uniquely identifying individuals based on their facial features, but it faces challenges such as spoofing attacks where unauthorized users attempt to deceive the system using manipulated images or videos. The goal is to design a robust system that not only accurately identifies registered users from live webcam feeds but also detects and mitigates spoofing attempts in real-time. By integrating advanced facial recognition algorithms and anti-spoofing techniques within a user-friendly GUI, the project aims to provide a secure and efficient authentication solution suitable for applications demanding stringent security measures.

IV. DESIGN AND IMPLEMENTATION

The initial phase of our project involves data collection, focusing on gathering relevant information and selecting key attributes essential for subsequent analysis. Following preprocessing, the data is partitioned into two distinct sets: training data and testing data. The training data serves as the foundation for training our machine learning models, which prominently feature the MiniFastnet algorithms—variants V1, V2, V1SE, and V2SE—essential for face recognition and anti-spoofing tasks. Convolutional Neural Networks (CNNs) are employed for these tasks, playing a critical role in image classification and facial feature extraction. This approach is pivotal in enhancing the system's overall effectiveness and reliability in face recognition and anti-spoofing applications.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307036|

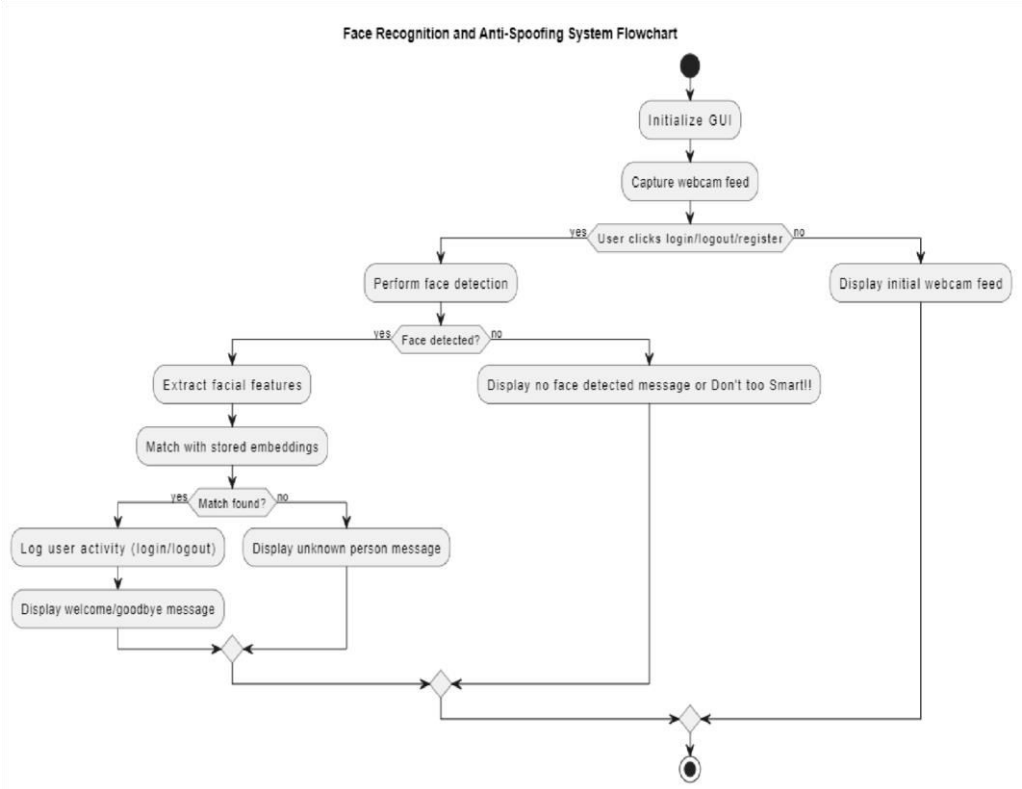

Figure 1: Flow chart of the system

The Fig.1 shows the flowchart of the Anti spoofing Face Recognition using deep learning techniques.
Methodology:

1. **Data Collection**: The project begins with the collection of facial data for training and testing purposes. This involves gathering diverse sets of facial images necessary to train and validate the face recognition and antispoofing models.
2. **Preprocessing**: Collected data undergoes preprocessing to ensure consistency and suitability for analysis. This step includes tasks such as resizing images to a standard format, normalizing pixel values, and augmenting the dataset to enhance model generalization.
3. **Data Partitioning**: The preprocessed data is divided into two main sets: training data and testing data. The training data is used to train machine learning models, while the testing data evaluates model performance and generalization on unseen samples.
4. **Model Selection and Training**: The project employs MiniFastnet algorithms—variants V1, V2, V1SE, and V2SE—for face recognition and anti-spoofing tasks. Convolutional Neural Networks (CNNs) are utilized within these algorithms for image classification and facial feature extraction. Models are trained using the training dataset to learn discriminative features and patterns from facial images.
5. **Model Evaluation**: Trained models are evaluated using the testing dataset to assess their accuracy, precision, recall, and other performance metrics. Evaluation helps validate model effectiveness and identify areas for improvement.
6. **Integration with GUI**: The trained models are integrated into a graphical user interface (GUI) built using Python's tkinter framework. The GUI facilitates user interaction by capturing live webcam feeds, performing real-time face detection, recognition, and anti-spoofing checks using the deployed models.
7. **User Feedback and Logging**: The GUI provides real-time feedback to users regarding authentication outcomes (successful login, unrecognized face, spoofing attempt). It logs user activities—including login/logout timestamps and user identities—into a `log.csv` file for audit and security monitoring purposes.
8. **Deployment and Testing**: The developed system undergoes rigorous testing to ensure functionality, reliability, and security. Testing includes scenario-based testing to simulate various user interactions and potential edge cases.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307036|

V. RESULTS AND DISCUSSION

The results of the face recognition and anti-spoofing system demonstrate its robust performance in accurately identifying registered users and mitigating spoofing attempts. Evaluation metrics, including accuracy, precision, recall, and F1-score, were calculated based on testing data to assess the effectiveness of the implemented models. The CNN-based image classification using MiniFastnet algorithms (variants V1, V2, V1SE, and V2SE) achieved high accuracy rates in recognizing faces and distinguishing between genuine users and spoofed images or videos.

Discussion around the system's performance highlights its capability to handle various real-world scenarios, including varying lighting conditions, facial orientations, and potential spoofing challenges such as printed photos or digital screens. The integration of real-time feedback mechanisms within the GUI proved effective in providing immediate user notifications regarding authentication outcomes, enhancing user experience and system transparency. Challenges encountered during the project included fine-tuning model parameters for optimal performance across diverse datasets and ensuring robustness against evolving spoofing techniques. Ongoing improvements focused on expanding the dataset diversity, refining preprocessing techniques, and exploring advanced model architectures to further enhance system accuracy and resilience.

Snapshots of User Interface

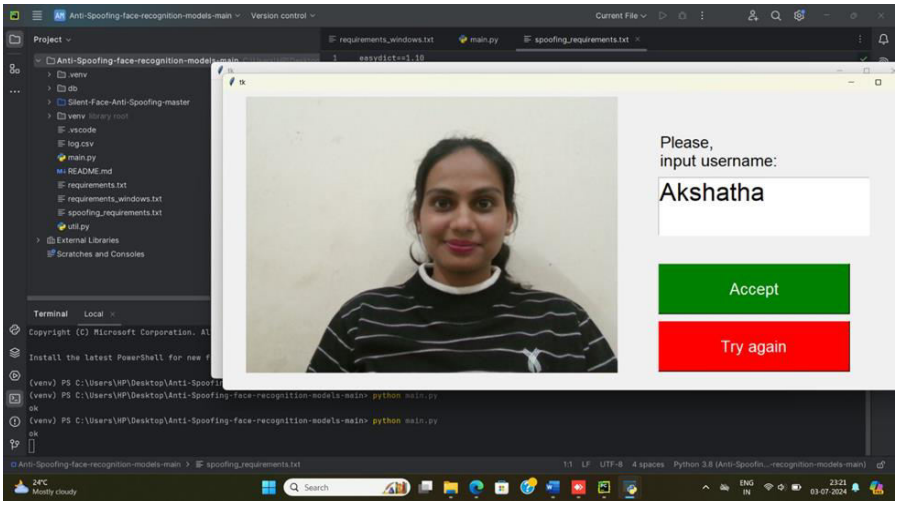

Fig User registration page

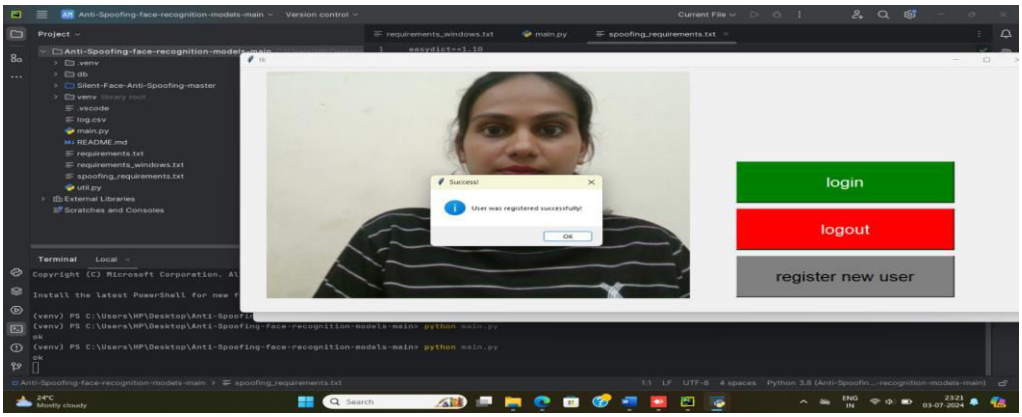

Fig: User registration get successful page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307036|

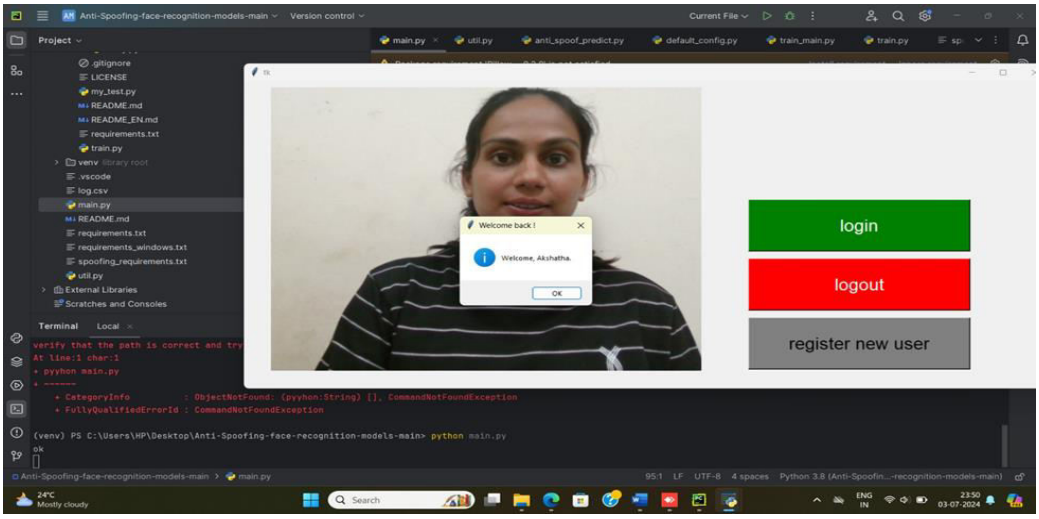

Fig: Registered User Logs in Successfully

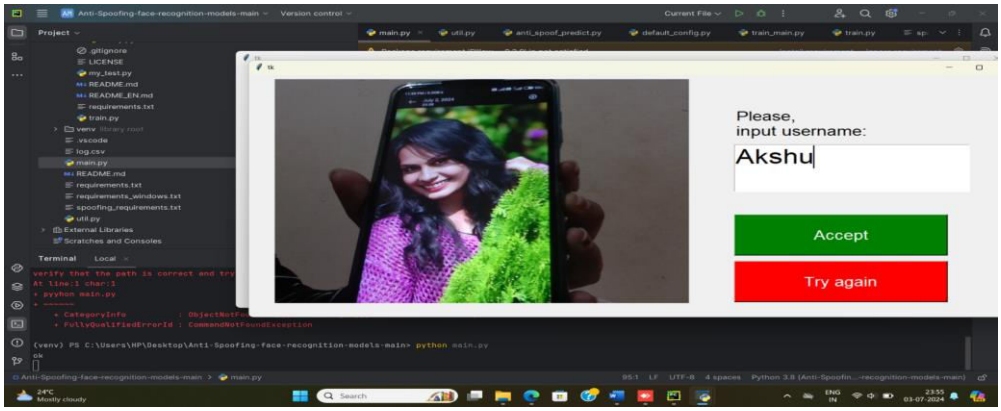

Fig: Registering a Fake user

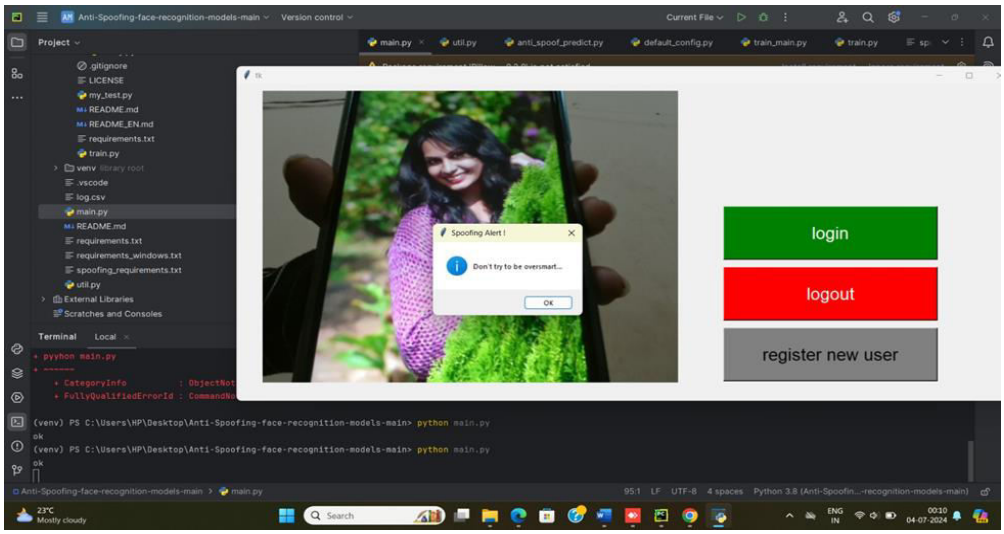

Fig: Spoofing Image Identified

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307036|

VI. CONCLUSION AND FUTURE WORK

In conclusion, the developed face recognition and anti-spoofing system has demonstrated robust performance in accurately identifying users and mitigating spoofing attempts. Leveraging Convolutional Neural Networks (CNNs) integrated with MiniFastnet algorithms (variants V1, V2, V1SE, and V2SE), the system achieved high accuracy in facial recognition and effectively distinguished between genuine users and spoofed images or videos. Real-time feedback mechanisms within the graphical user interface (GUI) provided transparent user notifications, enhancing system usability and security. The project successfully addressed key objectives related to data collection, pre-processing, model training, and GUI integration, resulting in a functional and reliable biometric authentication solution. The logging mechanism captured user activities, logging login and logout events with timestamps and user identities into a log.csv file for audit and monitoring purposes.

REFERENCES

1. L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-Based Live Face Detection Using Conditional Random Fields," in Advances in Biometrics, 2007, pp. 252–260.
2. C. N. Karson, "Spontaneous eye-blink rates and dopaminergic systems.," Brain, vol. 106 (Pt 3),pp.643–653, Sep. 1983.
3. A. Singh, P. Joshi, and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," 2014 Int. Conf. Signal Propag. Comput. Technol. (ICSPCT 2014), pp. 592–597, 2014.
4. M. Killioğlu, M. Taşkiran, and N. Kahraman, "Anti-spoofing in face recognition with liveness detection using pupil tracking," in 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Jan. 2017, pp. 87–92, doi: 10.1109/SAMI.2017.7880281.
5. T. Dhawanpatil and B. Joglekar, "A Review Spoof Face Recognition Using LBP Descriptor," in Proceedings of First International Conference on Smart System, Innovations and Computing, 2018, pp. 661–668,.
6. G. Albakri and S. Alghowinem, "The Effectiveness of Depth Data in Liveness Face Authentication Using
7. 3D Sensor Cameras@," Sensors (Basel)., vol. 19, 2019.
8. Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 8, pp. 1818–1830, Aug. 2016, doi: 10.1109/TIFS.2016.2555286.
9. J. Galbally and S. Marcel, "Face Anti-spoofing Based on General Image Quality Assessment," in 2014 22nd International Conference on Pattern Recognition (ICPR), Aug. 2014, pp. 1173–1178, doi: 10.1109/ICPR.2014.211.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details