iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49584

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Secure Identification at Your Fingertips: Building a Face Recognition System with Google Colab

Harsh R. Mishra[1], Shivang Vadgama[2], Hardik Pandya[3]
Computer Engineering, B.H. Gardi College of Engineering & Technology, Rajkot, India

Abstract: The term "security" refers to the measures taken to ensure protection against harm. A security system is the result of measures taken to secure something through a system. There are various types of security systems available today, and ongoing research is being conducted in this field.
The purpose of this research paper is to develop a face recognition system to enhance security, with the aim of making it more reliable and secure than existing systems. This will be achieved through the use of Google Colaboratory (Colab) for face recognition, which will enable the system to accurately identify individuals based on their facial features. The system will automatically distinguish between real and fake samples to prevent unauthorized access attempts. If a fake access attempt is detected, the system will display a message indicating that the user is unauthorized. The proposed method aims to improve accuracy, efficiency, clarity, and security, ultimately enhancing the overall security of the system.
Keywords: Face Recognition, Google Colab, Machine Learning, Python, Human Images

I. INTRODUCTION

Face recognition is the most common research area of person identification. Face recognition is a method for identifying individuals using their face. Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it to learn for themselves. The process of learning begins with observations or data, such as examples, direct experience, or instruction, in order to look for patterns in data and make better decisions in the future based on the examples that we provide. The primary aim is to allow the computers to learn automatically without human intervention or assistance and adjust actions accordingly [1].

Deep learning is a subset of machine learning in artificial intelligence that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Deep learning is a technique used to generate face detection and recognize it for real or fake by using profile images and determining the differences between them [1].

Deep networks have the ability of learning from unstructured or unlabeled raw data. It works like the human brain where “Neuron” indicates a mathematical function that collects and classifies information according to specific architecture. In a neural network each node in the layer of interconnected nodes is a perceptron. The signal produced by multiple linear regressions into an activation function is fed by the perceptron. Neural network mainly comprised of three layers. These are, Input Layer: Takes primary data through corresponding layers for further analysis, then Hidden Layers: It’s the intermediate layer where every computation is done and activation function provides the output and Output Layer: It’s the last layer that brings out the information learned by the network [2].

To enhance the security we are building a Face Recognition System using Machine Learning Technology with Python as programming language in Google Colab IDE. The system is precise generating results above 95% as precision for the data sets trained in the model. A detailed explanation of the precision is mentioned in the research paper.

A. Objectives of Study

The primary goal of this research is to develop a software model that can accurately and efficiently identify and differentiate between authentic and manipulated facial images created by experts. Alongside this overarching aim, several other objectives have been established, including the rapid detection of fraudulent facial images, ensuring high accuracy and validation rates for both training and testing datasets, minimizing the expenses and time required for repetitive image analysis, and implementing an optimal network architecture to obtain optimal results. Furthermore, the study seeks to train the model with a large dataset of genuine and fabricated human faces to achieve maximum precision in the final outcome.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

II. DATA PREPROCESSING

Data preprocessing is an important step in preparing raw data for machine learning or data mining algorithms. Prior to application of these algorithms, it is essential to check the quality of data for correctness, completeness, and accuracy. Data preprocessing involves removal of incorrect, incomplete, and inaccurate data from datasets and replacement of missing values. Subsequently, preprocessed data were fed into a Convolutional Neural Network (CNN) for training purposes. The training process was conducted using the CNN model and the resulting model was saved for testing purposes. The trained model enabled classification of users' faces in real-time [3].

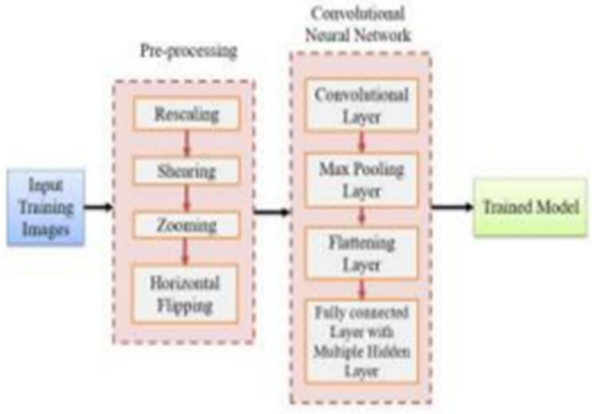


Fig. 1. Flowchart for Data Processing with Convolutional Neural Network [3]

III. EXPLANATION OF PROPOSED SYSTEM

Get ready to meet the future of person identification! Our proposed method is a cutting-edge Face Model-based system that revolutionizes the way we identify individuals. In this section, we dive deep into the details of this innovative system.

A. Workflow Diagram of Face Recognition System

Figure 2 depicts the workflow diagram of the face recognition model utilized in this study. Following the preprocessing of training data, it is fed into the Deep Learning model for training. The model is trained based on the input data. Once the training process is complete, the testing data is preprocessed and fed into the trained model to predict the person using the learned model and corresponding labels.

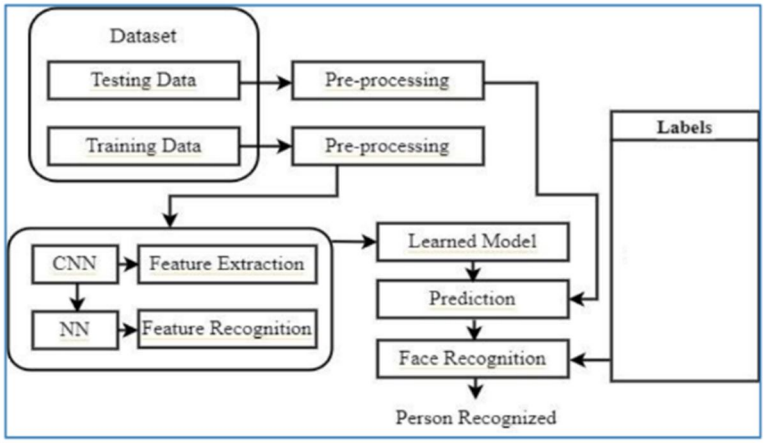


Fig. 2. Workflow Diagram of Face Recognition System [2]

IV. MEATHOIDOLOGY

The proposed methodology for this research entails a systematic approach consisting of several phases. Initially, a dataset was gathered, followed by the identification of tools and programming languages to be utilized. Next, images in the dataset underwent preprocessing to improve their quality. To enhance the dataset's size and variety, data augmentation techniques were employed. Through this comprehensive approach, we aim to develop a highly efficient and accurate face recognition system.

A. Dataset

In the context of the research, a dataset consisting of two authentic human images has been used. These images were captured by a camera and represent two different individuals, who have been assigned the aliases "Person A" and "Person B". The use of pseudonyms is a common practice in research to maintain confidentiality and privacy of the subjects. These images will be utilized to train and test the face recognition system developed in this study.

B. Languages & Tools Used

The programming language utilized for this study was Python, an interpreted, high-level, general-purpose language that was created by Guido van Rossum and initially released in 1991. Python is renowned for its emphasis on code readability, which is achieved through the notable use of significant whitespace in its design philosophy. Furthermore, the language constructs and object-oriented approach of Python strive to aid programmers in writing logical and clear code for projects of varying sizes [1].

Python is dynamically typed and features garbage collection. It offers support for multiple programming paradigms, such as procedural, object-oriented, and functional programming. Python is often described as a "batteries included" language because of its extensive standard library [1].

In this study, various tools were employed, with the most notable being Google Colab for writing Python code, which is a research tool for teaching and exploring deep learning machines. Google Colab, being a free research project, enables the storage and direct access of all notebooks from Google Drive. Google Colab is user-friendly, requires no preparation for use, and is recognized for its performance speed due to its utilization of high-speed GPU processors [1].

C. Image Format

The corpus under examination was procured from a compilation of authentic facial depictions, aimed at discerning the veracity of an image in JPG format, and optimizing the fidelity of the model for the intended outcomes.

V. EXPERIMENTAL RESULTS

The above lines suggest that the section being referred to provides a detailed and thorough investigation of the face recognition system that has been proposed. This examination has been conducted through an experimental approach, which indicates that the proposed system has been tested and evaluated under various conditions to assess its effectiveness and accuracy.

The section in question delves into the intricate nuances of the implementation of the facial model that has been designed as a part of the proposed system. The term 'nuances' implies that the implementation details being discussed are subtle and complex, and require a deeper understanding to comprehend.

A. Face Dataset

The customized facial dataset at our disposal comprises a total of four images featuring two distinct individuals, namely Person A and Person B. The dataset in question has been meticulously curated to showcase the captured photographs and their corresponding generated outputs, each presented in a side-by-side format. The precision of the generated outputs is of paramount importance, and as such, great care has been taken to ensure their accuracy.

Fig. 3. Sample Image of Face Dataset of Person A

Fig. 4. Sample Image of Face Dataset of Person B

B. Classification Report of Face Recognition Model

The statement refers to the results obtained from an empirical study, which reveals that Person A has obtained a higher precision value of 98.38%, while Person B has achieved a precision value of 96.95%. These precision values indicate the accuracy of the facial recognition model, as they represent the proportion of correctly identified faces out of all the faces analyzed.

However, it is crucial to note that the precision value is not solely dependent on the facial recognition model itself but is also influenced by various external factors. These factors may include adequate lighting that should be directed towards the face, ensuring an optimal head posture, and other related factors that could affect the quality of facial recognition.

In conclusion, the precision value is a vital measure of the efficiency and effectiveness of a constructed facial recognition model, and its accuracy is dependent on various factors. Therefore, these findings have significant implications for researchers, policymakers, and practitioners in the field of facial recognition technology

Table. 1. Classification Report of Face Recognition Model

Sr. No	Labels	Precision Value
1	Person A	98.38%
2	Person B	96.95%

VI. FUTURE WORK

For future work, we propose the integration of a face recognition model with an authentication system based on fingerprint technology. This approach will address the limitations of facial recognition technology and fingerprint authentication, respectively, and provide a more reliable and accurate method for identity verification.

Facial recognition technology is susceptible to errors when dealing with variations in facial features, such as lighting, facial expression, or occlusion. Similarly, fingerprint authentication may not be effective when dealing with damaged or dirty fingers or other physical deformities. Therefore, combining both technologies can overcome these limitations and provide a more robust and reliable identity verification system. The proposed integration of the face recognition model with fingerprint authentication will require significant technical expertise and development effort. However, the potential benefits of this system in terms of improved security and accuracy for identity verification are substantial and could have significant implications for various domains such as law enforcement, banking, healthcare, and more. The integration of the existing facial recognition model with a cloud-based system consisting of a face recognition algorithm and a TCP/IP client. The cloud-based system will receive a smaller image size, as opposed to the entire image, which will then be processed using a facial recognition algorithm [4].

By using this approach, the system's efficiency and performance will be enhanced, resulting in a faster and more accurate facial recognition process. Additionally, the smaller image size will require less bandwidth and energy for communication between the client and the cloud-based system, resulting in a more cost-effective and energy-efficient solution [4].

In conclusion, the integration of a face recognition model with fingerprint authentication technology represents a promising avenue for future research and development. This approach could address the limitations of both technologies and provide a more accurate and reliable identity verification system. Further research is necessary to investigate the technical feasibility and potential benefits of this approach in real-world scenarios.

VII. CONCLUSION

In conclusion, the development of a face recognition system using machine learning technology in Google Colab IDE has been described in this research paper. The system has been designed to enhance security by providing an accurate and efficient means of personal identification. The system utilizes a dataset consisting of two distinct human images that have been pre-processed using techniques such as zooming, shearing, rescaling, and horizontal flipping.

The proposed method offers several advantages over existing face recognition systems, including improved accuracy, efficiency, clarity, and security. The system is designed to automatically distinguish between legitimate and fake samples, and it generates a message for any unauthorized access attempt.

The study also highlights the importance of data preprocessing in machine learning applications. The quality of the data is critical for the success of machine learning algorithms, and preprocessing techniques such as removing incorrect, incomplete, and inaccurate data, and replacing missing values can significantly improve the accuracy and reliability of the system.

Overall, the proposed face recognition system offers a promising solution for enhancing security in various applications, including access control, surveillance, and identity verification. Further research can be conducted to improve the system's performance by using more extensive and diverse datasets and exploring advanced deep learning techniques.

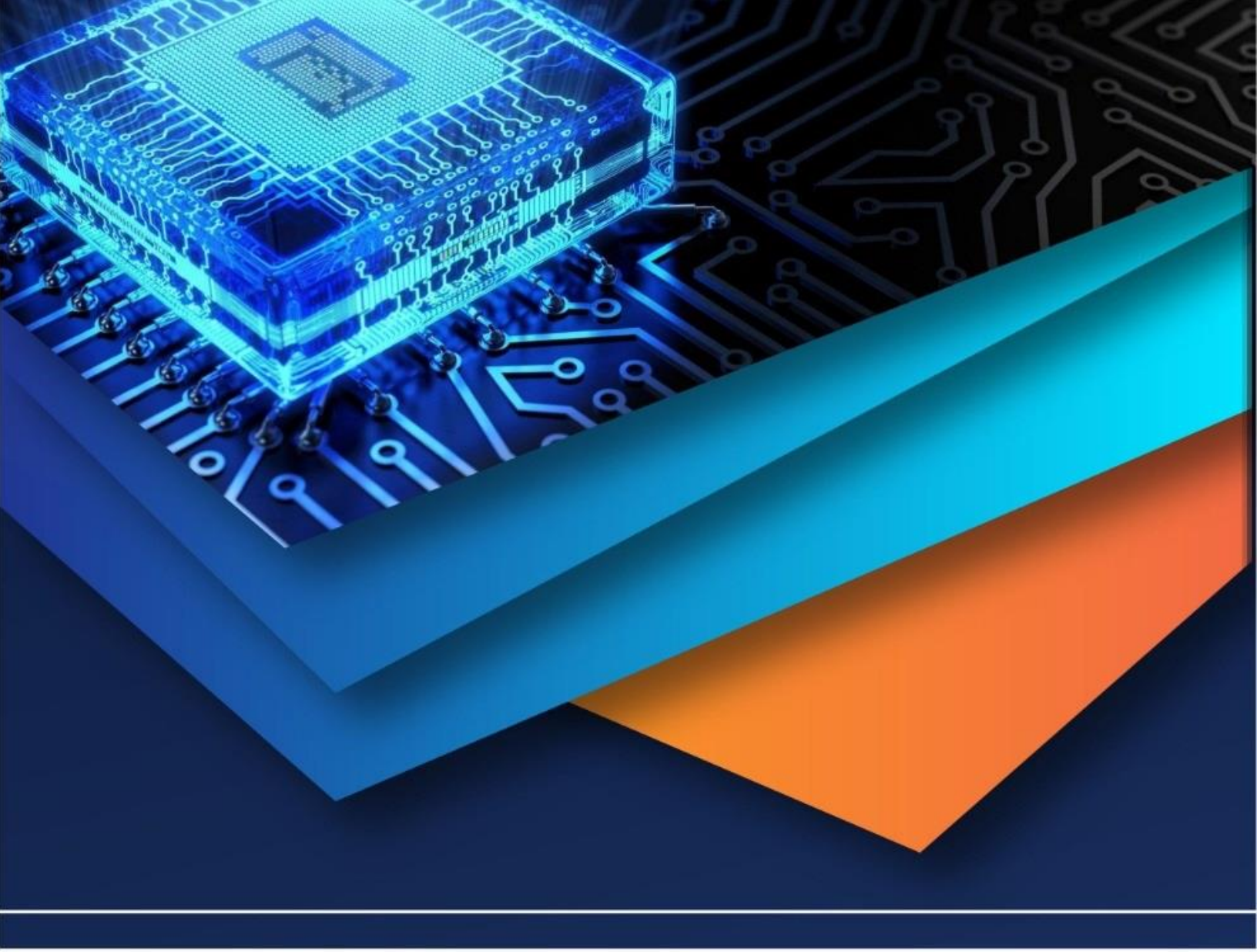
REFERENCES

[1] Deshmukh, A. and Wankhade, S.B. (1970) Deepfake detection approaches using Deep Learning: A Systematic Review, SpringerLink. Springer Singapore. Available at: https://link.springer.com/chapter/10.1007/978-981-15-7421-4_27.

[2] Face and hand gesture recognition based person identification system ... (no date). Available at: https://www.researchgate.net/publication/359615125_Face_and_Hand_Gesture_Recognition_Based_Person_Identification_System_using_Convolutional_Neural_Network.

[3] Card-less ATM transaction using biometric and face recognition– a review (no date). Available at: https://www.researchgate.net/publication/343346935_Card-Less_ATM_Transaction_using_Biometric_and_Face_Recognition-_A_Review.

[4] Oroceo, P.P. et al. (2022) Optimizing face recognition inference with a collaborative edge–cloud network, MDPI. Multidisciplinary Digital Publishing Institute. Available at: https://www.mdpi.com/1424-8220/22/21/8371.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY