iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51468

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 V May 2023- Available at www.ijraset.com

Disguised Face Recognition using Deep Learning

S Pratheek[1], Sachin Manjunath[2], Saikiran M[3], Manoj Kumar[4], Darshan L M[5]
[1, 2, 3, 4]*Student*, [5]Associate Professor, *Dept. of Computer Science and Engineering, Reva University, Bengaluru, India*

Abstract: ***The accuracy of facial recognition has significantly improved thanks to deep learning-based methods. However, several factors including facial ageing, disguises, and position fluctuations impair the efficiency of automatic face recognition algorithms. Disguises are commonly utilized to conceal one's identity or assume the identity of someone else by intentionally or unintentionally altering one's facial features. Here, we intend to make use of the Disguised Faces in the Wild (DFW) small-scale training data. Deep Convolutional Neural Networks(DCNNs) will be trained for general face recognition. The IIIIT-D testing data set will be used for model evaluation because it exhibits greater performance. The IIIT-D testing dataset is used to gauge the effectiveness of the model's performance when applied to faces that have been deliberately disguised. The performance of the results is encouraging and suggests that DCNNs have a chance of successfully recognizing disguised faces.***
Keywords: CNN, DCNN, VGG16, IIITD-DFD, Disguied face recognition, face recognition

I. INTRODUCTION

Face recognition is a prominent area within the field of computer vision that has garnered significant research attention in recent years. Deep Convolutional Neural Networks (CNNs) have emerged as a powerful tool for accurately detecting and recognizing faces. Researchers have made notable advancements, achieving high levels of accuracy in face recognition tasks using CNN-based approaches. However, it is important to note that a number of difficulties and variables, such facial ageing, plastic surgery, and facial camouflage, hamper the performance due to the extensive deployment of face recognition applications, particularly for security. These variances are loopholes that are used to impersonate other people’s identities. Hence Disguised Facial Recognitions needs to be researched on.

Deep learning disguised face recognition is a technique that uses deep neural networks to identify faces even when they are partially covered or disguised. This can be useful in situations where people may try to conceal their identity, such as security and surveillance systems. There are several approaches to using deep learning to implement disguised face recognition, but one common method involves training a deep neural network on a dataset of both disguised and undisguised face images. The network learns to extract features that are resistant to variations in facial appearance caused by masks, glasses, or hats. These characteristics can then be used to identify faces that are partially obscured or disguised.



Fig.1. Using disguise accessories, the same person can appear in different ways. The images depict the subject present in the dataset, in various disguises.[1]

By overcoming problems with illumination, posture, and age, recent developments in the field of face detection and recognition have attempted to establish a solid system. Because of this, modern surveillance systems mainly rely on these methods to verify their users. Despite the promising results, some people have found ways to get around this layer of security by using accessories including glasses, wigs, scarves, caps, beards, masks, and other objects that impede recognition and interfere with the mechanisms.[2]

The four-stage process used by the suggested approach to recognize people uses facial feature points. In the first stage, 15 facial characteristic points are used to calculate the likelihood that the said individual is actually that person and not a forger. The sale of electronic products is referred to as "electronic commerce". Based on previously accessible or acquired visuals of various persons, a face recognition algorithm is utilized to identify the person.

©IJRASET: All Rights are Reserved

In this scenario, the obscured and less accurately detectable facial points are discarded, and instead, corresponding key points are generated in the fourth phase. To accurately reconstruct the intruder's image, these spots must be statistically positioned. In order to determine the possibility that an image of an intruder obtained with obfuscation matches someone in the dataset, the classification step is performed after regeneration and the new face points are compared to the previously stored ones.

Since convolutional neural networks have shown results that are comparable to those of manual procedures used by true professionals, they are widely used in deep learning. Through a succession of model architectural changes, deep learning approaches, like CNN, mechanically acquire photographic data in order to identify complicated properties. The figure illustrates the CNN branch of AI. Deep learning methods like CNN are part of the machine learning branch of artificial intelligence (AI). CNNs are reliable, simple to train, and low in complexity as the network picks up new skills during the tuning process. There are many different factors. The overall architecture of CNN consists of an input layer, hidden layers linked to various image filtration systems, feed-forward network layers where the image filtration are displayed upon the input picture, and a result layer where the feature will be recovered.

II. LITRATURE SURVEY

Kaipeng Zhang et al. [3] conducted a study on the application of Deep Convolutional Neural Networks (DCNN) for face recognition in the presence of disguises. The researchers developed a novel approach that involved utilizing a Wselect transformation matrix to alter masked faces and employing two DCNNs to extract universal face identity attributes. Initially, the researchers trained the DCNNs on a large dataset for general face recognition. They then calculated the transformation matrix to adapt the model for disguised face recognition. The reported accuracy of this model was 0.8571.

The paper titled "Disguised Facial Recognition Using Neural Networks" was authored by Saumya, Kumaar Ravi Vishwanath, M. Omar S. N. Majeed, Abrar Abhinandan Dogra, and others in 2018. The study introduces a real-time deep neural network architecture for verifying masked faces. The proposed model comprises two neural networks: a convolutional neural network (CNN) that predicts 20 significant facial points in the image, and a classification neural network that utilizes the angles and ratios derived from the predicted points to identify the subject. The accuracy rates for prediction and classification are reported as 67.4% and 74.8%, respectively, and the performance of the model is compared to state-of-the-art techniques.

In their 2018 research paper titled "Face Verification with Disguise Variations using Deep Disguise Recognizer," Naman Kohli, Daksha Yadav, and Afzel Noore introduced a novel approach to address the challenges of face verification in the presence of disguises. Several factors, including facial ageing, disguises, and position variations, limit the effectiveness of the automatic face recognition algorithms that are now in use. By making purposeful or unintended changes to the way one looks, disguises are used to hide one's identity or to pass for another person. In this study, we employ a transfer learning technique based on deep learning for face verification with disguise adjustments. For the purpose of learning the innate face [5] representations, we use a residual Inception network structure with the central loss. To mitigate the impact of facial disguises, researchers have developed the Inception-ResNet model, which is trained using a large database of faces through inductive transfer learning.

Jiankang Deng and his colleagues [6] conducted research using the ArcFace algorithm, known for its high accuracy rate of 98.66%, to recognize disguised faces. They evaluated the verification accuracy of different models, including the recommended ArcFace, and presented the results in a table. Among the models, the DFW2018 winner called MiRA-Face achieved the highest accuracy of 90.65% and 80.56% at 1% and 0.1% false acceptance rates (FARs) respectively, for the obfuscation task on the validation dataset. The ArcFace algorithm outperformed all other algorithms with a margin of at least 4.43% for the GAR (Genuine Acceptance Rate) at 1% FAR and at least 11.64% for the GAR at 0.1% FAR.

Amarjot Singh [7] conducted a study called "The Space Fusion" where they created a dataset of disguised faces. The dataset was divided into two categories: basic disguised faces and complex disguised faces. Each category consisted of 1000 training photos, 500 validation photos, and 500 test shots. The network was trained for 90 iterations with a batch size of 20. For each input image, a random sub-picture at the 248th position was selected. The selected patch was then subjected to random transformations such as flipping, rotation between -40 and 40 degrees, and resizing to 256x256. The output heat map size was set to 64x64, and the Gaussian variance was set to 1.5. The initial learning rate is adjusted from 105 to 106 after 20 iterations. The momentum is set to 0.9. The accuracy of key-point detection in the simple background dataset was found to be approximately 85%, while in the complex background dataset, it was around 74%. Additionally, the accuracy of both datasets tends to improve as the pixel distance from the ground truth decreases.

The components of this paper are as follows: The second section contains resources and instructions for gathering datasets, pre-processing them, and creating and refining deep learning models. The results of the experimental setting are discussed and explained in Part Three, and then Part Four concludes.

III. MATERIALS AND METHODS

Data collecting, pre-processing, which includes actions like shrinking the knee images, and noise reduction are the three steps of the proposed system, which is shown in Fig. 3. Following the extraction and classification of features, a convolutional neural network is used.

A. Dataset Details

We have utilised the IIITD-DFD, a collection of pictures with disguised faces, to assess how well the model for identifying hidden faces works. The database's disguise variations are divided into the following categories. Without hiding neutral picture variations in hairstyles: various wig designs and colours, Beard and moustache variations include diverse beard and moustache styles, variations brought induced by glasses: sunglasses, Cap and hat variations include several types of caps, turbans, bandanas, and veils (also known as hijabs, which cover the hair). mask-related variation: single-use doctor's mask, and A variety of variations: a collection of accessories for disguise. This contains 15,690 images.This image has 75 classes. Each class contains 8–10 photos that include both neutral and hidden faces. The initial dataset, which consists of 15,690 images in the ratio of 80:10:10, is divided into the training dataset, validation dataset, and testing dataset, yielding 9382 images for training, 3105 images for validation, and 3203 images for testing. The dataset is also divided into the ratios of 70:15:15 and 60:20:20 for additional analysis.

The effectiveness of our approach has been assessed using a challenging custom dataset. The dataset includes a variety of simple, semi-complex, and complex images, with background noise being the determining factor in complexity. The complexity of this noise has not been changed to promote algorithmic accuracy rather, it has been left alone to increase system robustness. This enables our algorithm to learn and operate well in adverse circumstances that may affect the orientation of faces or other factors. A total of 15,690 photos of 75 different subjects, shot in various lighting settings, make up our dataset. The training dataset has 9382 photos, while the validation dataset contains 3105 images and training dataset contains 3203.



Fig.2. Sample Images

Learning from start to finish can be highly valuable in addressing the challenge of identifying individuals in various disguises. By training a model to detect and extract 20 facial key points from a person's face, regardless of whether they are wearing a disguise, the model becomes more resilient. This approach involves using a single image of an undisguised face to capture the relative distances and angles of facial features. The training process involves using a dataset of 9,382 images with input sizes of 224 x 224, validation on 3,105 images, and testing on 3,203 previously unseen images. To enhance visual interpretation, the predicted facial coordinates are overlaid on the input images.

B. Pre-Processing

Data preprocessing is an essential step in deep learning workflows to ensure that the data is in a format that the network can understand. This process involves modifying the data to improve its compatibility with the model and enhance desired features while reducing any artifacts that could negatively impact the network's performance.

One common example of data preprocessing is resizing image inputs to match the required dimensions of the network's image input layer. This step ensures that all images are uniform in size before being fed into the model. Additionally, other transformations such as cropping, rotation, or normalization can be applied to further enhance the data.

Preprocessing the data can also optimize the training and inference process. For instance, when using convolutional neural networks (CNNs), the fully connected layers typically require input data in arrays of the same size. By resizing or reshaping the images to a consistent size, the model can efficiently process the data.

Furthermore, scaling down large input images can significantly reduce the training time without sacrificing the model's performance. This approach is particularly beneficial when dealing with computationally intensive deep learning models that require extensive processing power.

By appropriately preprocessing the data, deep learning models can train more efficiently, make accurate predictions, and achieve better overall performance. It is an essential step in preparing the data for successful model training and inference.

C. VGG16 Deep Learning Model

The VGG16 model is a convolutional neural network (CNN) developed by the Visual Geometry Group at the University of Oxford. It is widely used for image classification tasks and has become a benchmark in the field of deep learning. The model consists of 16 layers, including 13 convolutional layers and 3 fully connected layers. It gained recognition for its simplicity and impressive performance in various image recognition challenges, notably winning the ImageNet Large Scale Visual Recognition Challenge in 2014.

One of the notable features of VGG16 is its use of 3x3 convolutional filters throughout the network. This design choice allows the model to capture more detailed information from input images, enabling better discrimination between different classes. Additionally, VGG16 incorporates max pooling layers to reduce the spatial dimensions of feature maps, leading to more efficient computation.

Due to its success and well-established architecture, VGG16 serves as a reference model for many deep learning applications. Its impact extends beyond image classification, as it has also influenced the development of other CNN architectures. Overall, VGG16 has significantly contributed to the advancement of computer vision and continues to be utilized in various domains and applications.

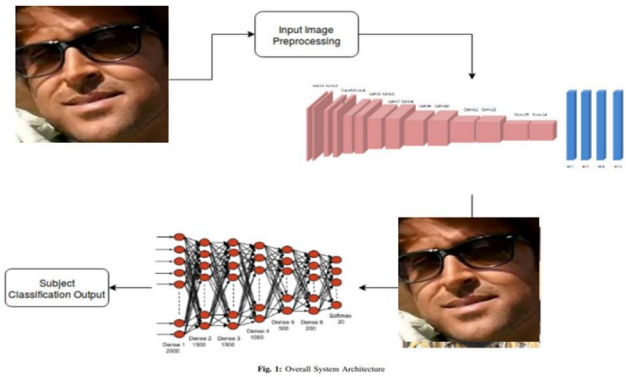


Fig.3. Proposed system Architecture

D. Proposed System

In order to extract key elements from facial photos for training a linear neural network, the suggested method employs a convolutional neural network model. The proposed disguised face recognition system is being developed using four modules: dataset preparation, disguised face detection, feature extraction, and classification.

E. Dataflow Diagram

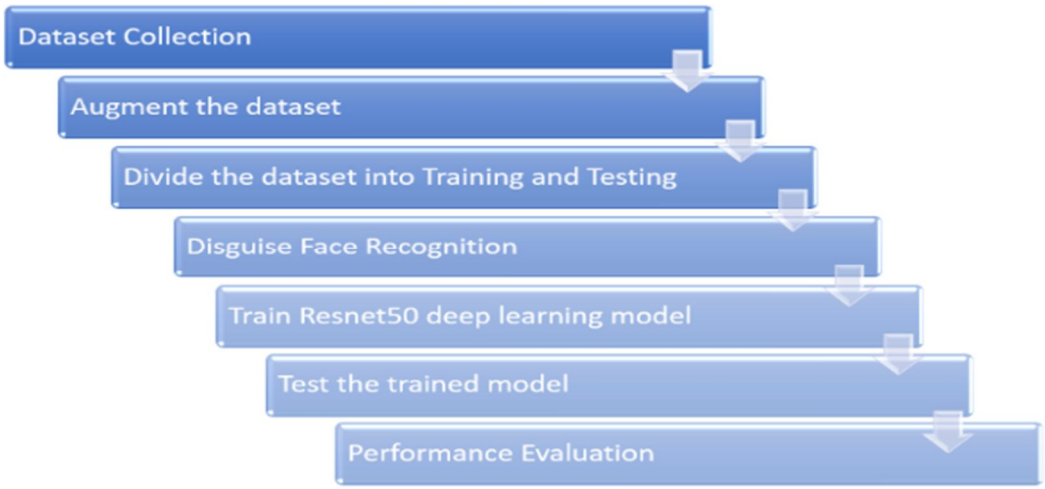


Fig.4. Dataflow Diagram

IV. RESULTS AND DISCUSSIONS

On evaluation of the results provided by the trained model we are able to find that the proposed model for disguised faces recognition has high degree of reliability by achieving high accuracy score. The experiment had multiple model trained on same dataset with varying train test validation ratio. The consolidated results of the experiment is provided below.

Test Dataset	Split ratio		
	80:10:10	75:15:15	60:20:20
IIITD-DFD	100	99.57	98.65

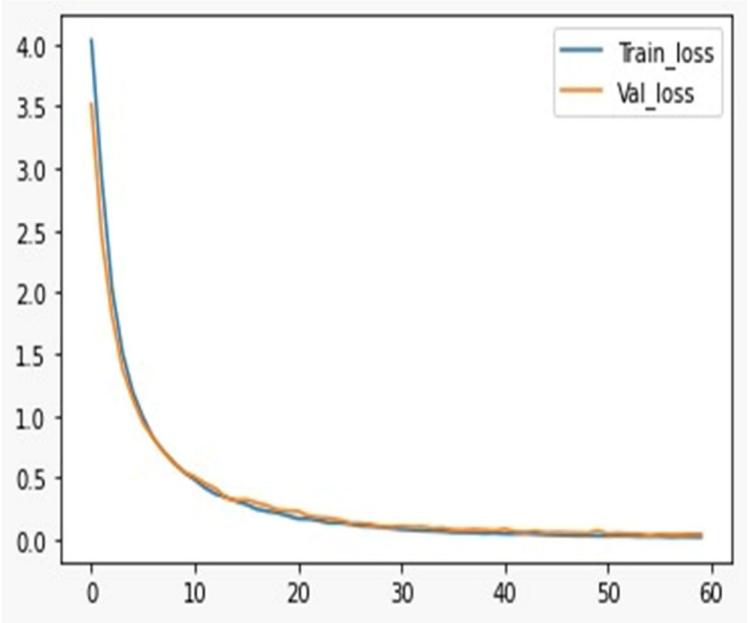


Fig.5(a). Training Loss and Validation Loss shown by the model trained on image dataset split in the ratio of 80:10:10

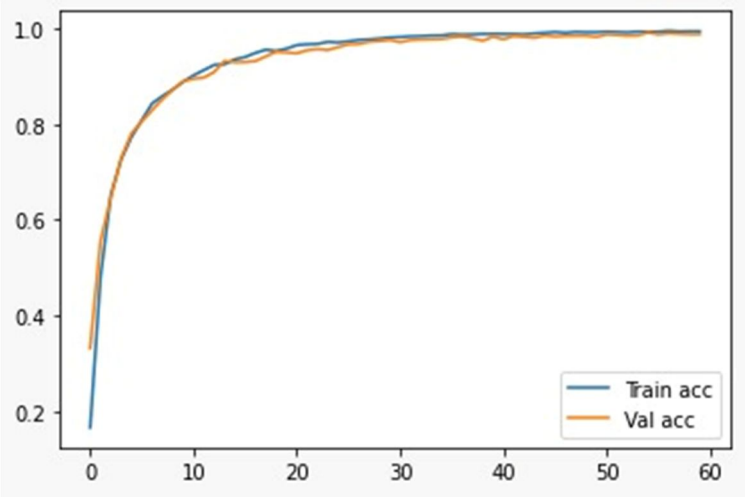


Fig.5(b). Training Accuracy and Validation Accuracy shown by the model trained on image dataset split in the ratio of 80:10:10

V. CONCLUSION

It has been proposed to use VGG16 to recognize disguised faces. Our suggested models produced incredibly pleasant results that were extremely precise.

Our model, which made use of the IIITD-DFD dataset, has multiple model that has been divided different training, testing and validation dataset. The model with dataset split ratio of 80:10:10 achieving accuracy of 100%. The model with dataset split ratio of 70:15:15 it as the accuracy of 99.57% and finally the model with dataset split ratio of 60:20:20 as the accuracy of 98.65%. Each of the model had a very low loss percentages. These experimental models demonstrates the deep learning applied to disguised faces and it has the potential to highly helpful in applications such as Face ID validation, Security surveillance.

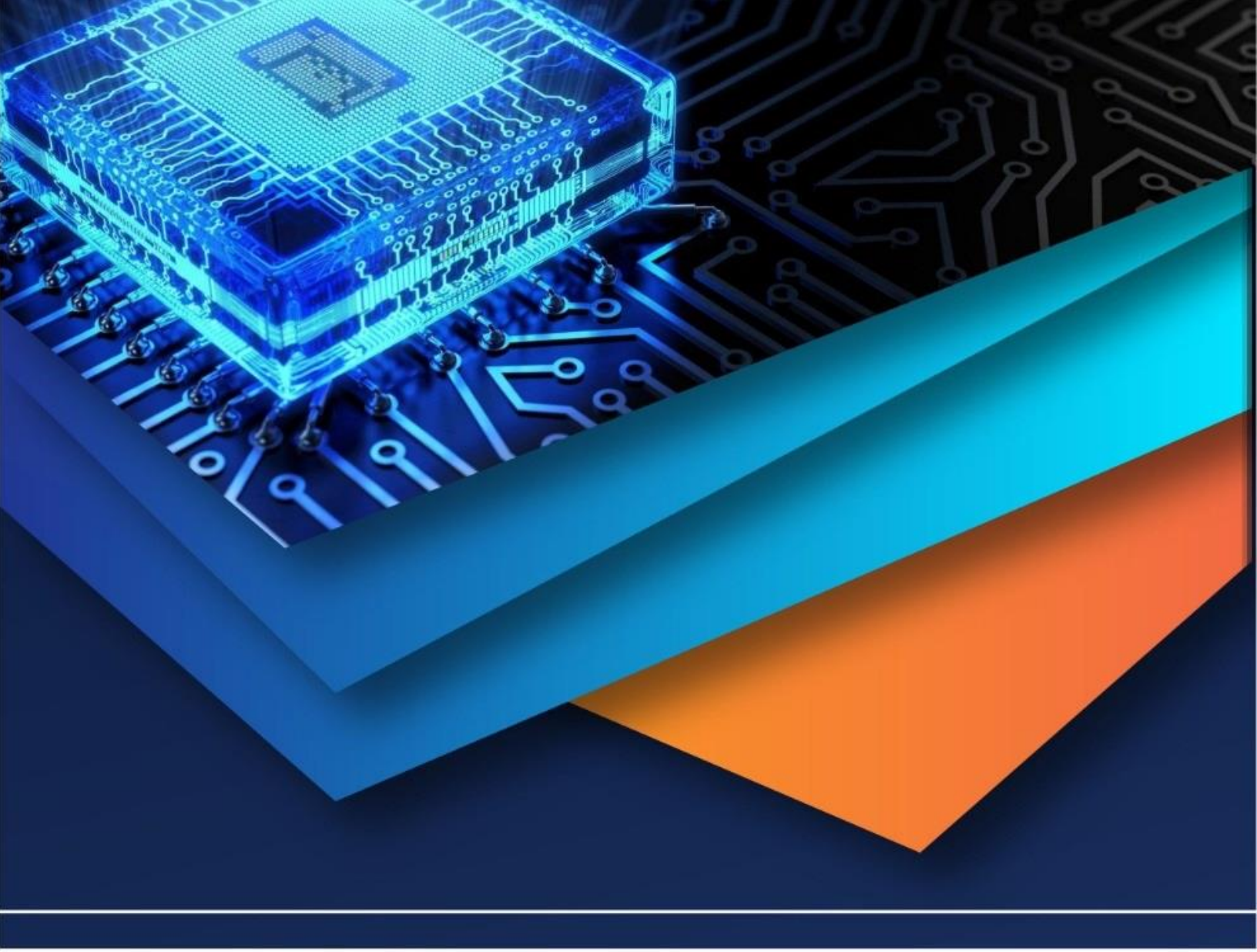
VI. ACKNOWLEDGEMENT

We want to express our appreciation to Reva University for providing us with the resources we required to complete this study. We really appreciate Prof. Darshan L M's guidance, assistance, and support throughout the research process. His extensive knowledge and skill were essential in directing our research and assisting us in achieving our goals.

We express our sincere gratitude to our friends for their invaluable encouragement and support throughout our research endeavor. Their unwavering assistance has played a vital role in enabling us to remain dedicated and focused on the successful completion of this project.

REFERENCES

[1] Tejas I. Dhamecha, Aastha Nigam, Richa Singh, and Mayank Vatsa IIIT Delhi, India
[2] Jay Mehta, Shreya Talati, Shivani Upadhyay, Sharada Valiveti, Gaurang Raval, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Sarkhej Gandhinagar Highway, Chharodi, Ahmedabad, Gujarat, 382481, India
[3] Kaipeng Zhang Ya-Liang Chang Winston Hsu National Taiwan University, Taipei, Taiwan kpzhang@cmlab.csie.ntu.edu.tw, {b03901014, whsu}@ntu.edu.tw
[4] Saumya Kumaar Ravi M. Vishwanath S. N. Omkar Abrar Majeed Abhinandan Dogra, 2018.
[5] Naman Kohli, Daksha Yadav, and Afzel Noore, 2018.
[6] Jiankang Deng, Stefanos Zafeiriou Imperial College&FaceSoft UK. ArcFace for Disguised Face Recognition
[7] Amarjot Singh, Devendra Patil, G Meghana Reddy, SN Omkar. Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network
[8] Amarjot Singh, Devendra Patil, G Meghana Reddy, SN Omkar. Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network
[9] Javier Hernandez, Javier Galbally , Julian Fierrez , Rudolf Haraksim , Laurent Beslay . FaceQnet: Quality Assessment for Face Recognition based on Deep Learning
[10] Omkar M. Parkhi Andrea Vedaldi Andrew Zisserman. Deep Face Recognition



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)