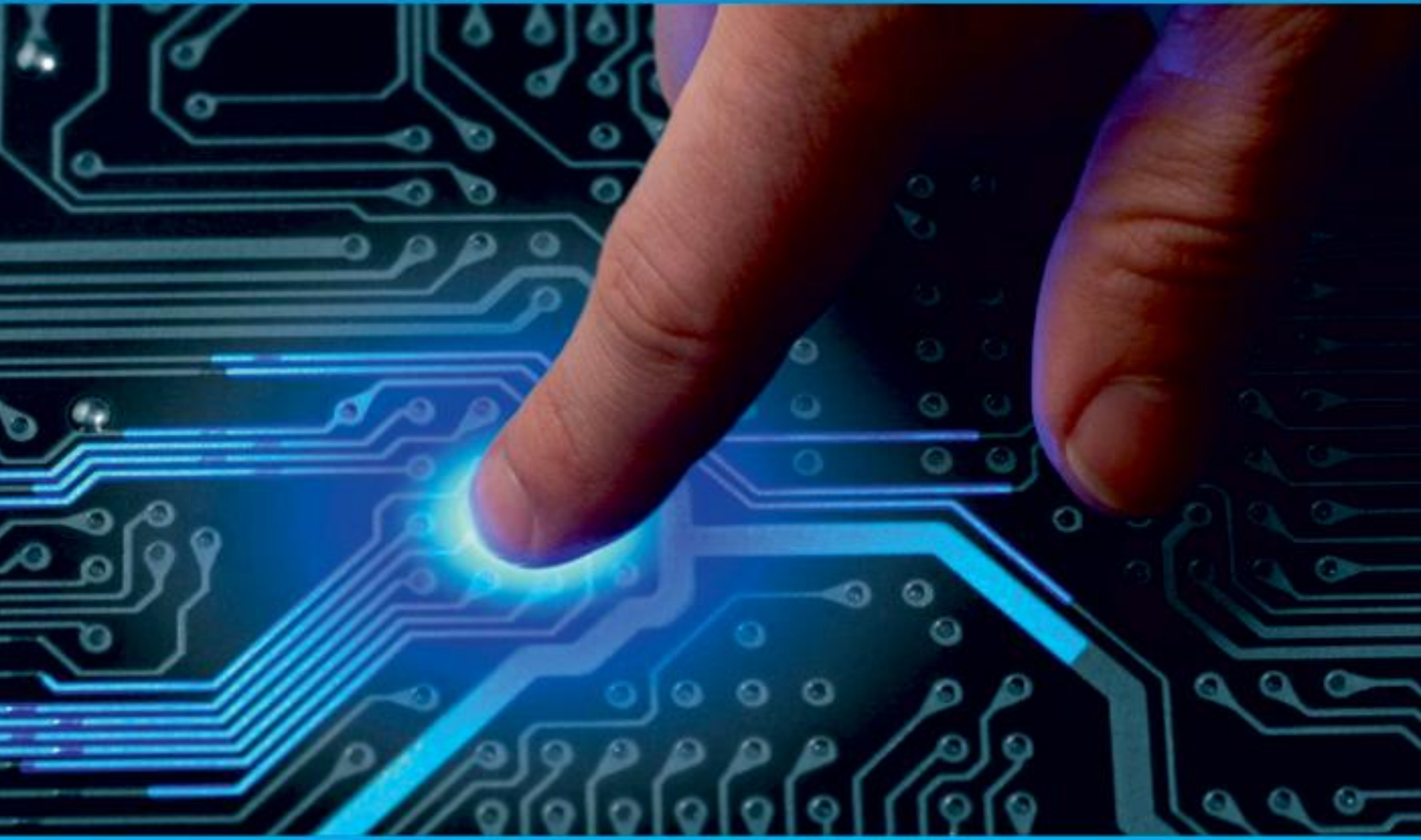
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205239 |

Image Forgery and Face Detection Using Convolutional Neural Network

Akshath S, Anandu G, Lijin S George, Mahadevan T. R, Shahida. M, Dr. Smitha C Thomas

U.G. Student, Department of CSE, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, India

U.G. Student, Department of CSE, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, India

U.G. Student, Department of CSE, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, India

U.G. Student, Department of CSE, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, India

Assistant Professor, Department of CSE, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, India

Associate Professor, Department of CSE, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, India

ABSTRACT: This research explores cutting-edge advancements in image recognition and face recognition technologies. The focus on image forgery detection involves deploying various pre-processing techniques and a fundamental Convolutional Neural Network (CNN) model. Evaluation on the practical CASIA V2.0 dataset ensures real-world relevance. Additionally, the study integrates transfer learning by fine-tuning pre-trained models from ImageNet, showcasing adaptability to diverse tasks. Shifting to face recognition, the research emphasizes faces as unique identifiers. The two-phase authentication process involves rapid face detection and subsequent individual recognition. Introducing Eigenface and Fisherface methods, the study employs Principal Component Analysis (PCA) for facial feature dimensional space reduction. A notable aspect is the integration of digital image processing to craft an advanced face recognition system. This interdisciplinary approach combines digital image processing techniques with biometric principles for refined feature extraction. The research anticipates challenges, acknowledges the significance of a practical dataset, and concludes with a forward-looking perspective, hinting at potential future directions. In summary, this research blends innovative methodologies to tackle image forgery detection and advance face recognition technologies for robust identity authentication.

KEYWORDS: Convolutional Neural Network, Image Processing, Digital Image Processing, Casia V2.0. Image Forgery, Face Detection.

I. INTRODUCTION

A. IMAGE FORGERY

Detecting image forgery has become increasingly essential in today's digital age where images and videos can be easily manipulated using sophisticated editing tools. The widespread dissemination of digital content, coupled with the ease of tampering, raises concerns about the authenticity of visual information. In response to this challenge, our paper proposes a comprehensive approach to image forgery detection, leveraging the advancements in deep convolutional neural networks (CNNs). our research focuses on two key aspects: the exploration of different preprocessing methods in conjunction with CNN architectures and the evaluation of transfer learning techniques, specifically through fine-tuning pre-trained models on ImageNet. This dual-pronged strategy aims to enhance the accuracy and robustness of image forgery detection by combining the strengths of both foundational CNN structures and the knowledge transfer capabilities of pre-trained models.

B. FACE DETECTION

One of the sub divided image frame makes one class i.e. the one consisting the faces in the image, which marks the first step towards the process of face detection[2][9]. It is inconvenient because in spite of the congruity exist among faces but several factors like age, skin color and facial expression can vary considerably. Then this problem is furthermore intricate by the arrival of factors like environment factors affecting light, risk of imitation and also probability of limited obstruction in image. The face detection system that can easily recognize any face from a given image that too under any circumstance with any kind of lighting environment is thus considered as the finest face detection system.The function of the face detection system can be further bifurcated into two phases. Phase one consists of classification, in which the system based on the input that was in the form of some random images and if the face is present in the image the output comes in the form of yes or no. Face localization is the second phase in which for a given input image it shows a bounding box which comprise the dimensions of exact location of the face in the image.

II. RELATED WORK

The survey explores different approaches for image forgery and face detection.

A. Face Detection and Recognition System using Digital Image Processing.
The development of a Face Detection and Recognition System using Digital Image Processing involves a comprehensive approach. From detecting facial features using algorithms like Haar cascades to employing sophisticated face recognition techniques, digital image processing plays a vital role in enhancing accuracy and efficiency. Despite existing challenges, ongoing research and technological advancements are continuously improving the robustness of these systems, making them integral in various domains.

B. Deep residual learning for image recognition.
Deep residual learning, particularly through the ResNet architecture, has significantly advanced image recognition capabilities. By introducing residual connections, these models effectively address the challenges associated with training very deep neural networks, leading to improved accuracy and performance on image recognition tasks.

C. A Review of Face Recognition Technology.
The future of face recognition technology holds promise and challenges alike. Ongoing research aims to improve accuracy, address biases, and enhance the adaptability of systems to diverse demographics. As the technology becomes more prevalent, there is a growing need for comprehensive regulations and standards to guide its ethical use. Continued collaboration between technologists, policymakers, and ethicists is essential to shape the future of face recognition technology in a manner that aligns with societal values and respects individual rights.

D. Comparison of support vector machine and softmax classifiers incomputer vision.
SVM might be sensitive to imbalanced datasets, whereas Softmax can handle class imbalances more naturally, especially when using appropriate loss functions. In computer vision, the choice between SVM and Softmax depends on the specific task, the nature of the data, and whether it's a binary or multi-class problem. Both classifiers have been successfully applied in various computer vision applications.

E. An efficient weak sharpening detection method for image forensics.
Continued research in weak sharpening detection could involve exploring deep learning models tailored for this specific task, considering advancements in neural network architectures and training strategies. Additionally, collaboration with forensic experts and integration into comprehensive image analysis tools could enhance practical usability. In summary, an efficient weak sharpening detection method for image forensics requires a thoughtful combination of frequency domain analysis, gradient evaluation, contrast assessment, noise analysis.

III. METHODOLOGY

A. Existing System
Due to the availability of deep networks, progress has been made in the field of image recognition. Images and videos are spreading very conveniently and with the availability of strong editing tools the tampering of digital content become easy. To detect such scams, It proposed techniques. In our paper, I proposed two important aspects of employing deep convolutional neural networks to image forgery detection. It first explore and examine different preprocessing method along with convolutional neural networks (CNN) architecture. Later It evaluated the different transfer learning for pre-trained ImageNet(via-fine-tuning) and implement it over our dataset CASIA V2.0.

B. Proposed System
In the ever-expanding landscape of biometric security, the amalgamation of Face Detection and Recognition Systems with cutting-edge technologies has emerged as a frontier in ensuring robust authentication processes. At the core of this innovation lies Digital Image Processing, a field that has played a transformative role in refining the accuracy and efficiency of these systems. Face Detection, the initial phase in this multifaceted process, involves rapidly identifying and localizing faces within an image. The intricate interplay of algorithms and techniques within Digital Image Processing ensures not only the quick detection of faces but also the adaptability to varying conditions such as lighting and pose.

In essence, the synthesis of Face Detection and Recognition Systems with Digital Image Processing, bolstered by the capabilities of Deep Neural Networks for Image Forgery Detection, represents a pinnacle in biometric security. This multidimensional approach not only ensures the swift and accurate identification of individuals but also serves as a formidable barrier against the increasing sophistication of fraudulent activities in the digital realm. As technology continues to advance, the convergence of these methodologies paves the way for a future where secure and reliable biometric authentication becomes not just a necessity but a cornerstone in safeguarding digital identities.

IV. SYSTEM DESIGN

Designing a system for image forgery detection and face detection using convolutional neural networks (CNNs) involves several steps.

A. Data collection and Pre Processing
For face detection, you may need datasets containing images with and without faces. Preprocess the images, which may include resizing, normalization, and augmentation to increase the diversity of the dataset.

B. Model Architecture
Design separate CNN architectures for image forgery detection and face detection. For image forgery detection, a CNN model with multiple convolutional layers followed by pooling layers and fully connected layers can be used. You can consider architectures like ResNet, VGG, or custom architectures.

C. Training
Train the forgery detection model on the dataset of authentic and forged images. Use techniques like cross-validation and data augmentation to improve the model's generalization. Fine-tune pre-trained face detection models on face datasets to detect faces accurately.

D. User Interface
Develop a user-friendly interface for users to interact with the system. This interface should provide feedback on whether the image contains a forgery and if faces are detected, along with any relevant metadata.

E. Security and Privacy
Implement security measures to protect sensitive data, especially if the images being processed contain personal information. Ensure compliance with data protection regulations such as GDPR or HIPAA.

V. PREPROCESSING PHASE

In the preprocessing phase of image forgery and face detection using convolutional neural networks (CNNs), the goal is to prepare the input images in a format suitable for the subsequent stages of the system.

Image Forgery Detection

A. Image Loading:
Load the images from the dataset into memory.

B. Resizing:
Resize the images to a consistent size. CNNs typically require fixed-size input images, so resizing ensures uniformity.

C. Normalization:
Normalize the pixel values of the images. This usually involves scaling the pixel values to be within a certain range (e.g., [0, 1] or [-1, 1]).

D. Data Augmentation
Apply data augmentation techniques to increase the diversity of the dataset. Techniques such as rotation, translation, scaling, flipping, and adding noise can be used to generate additional training samples.

E. Label Encoding:
Encode the labels of the images. For image forgery detection, labels may indicate whether an image is authentic or forged.

Face Detection

A. Image Loading:
Load the images containing faces into memory.

B. Resizing:
Resize the images to a fixed size suitable for face detection. The size should be compatible with the input size expected by the face detection model.

C. Normalization:
Normalize the pixel values of the images, similar to the forgery detection preprocessing step.

D. Data Augmentation:
Apply any specific preprocessing steps required for face detection. For example, converting the image to grayscale, enhancing contrast, or applying histogram equalization can improve face detection accuracy.

E. Bounding Box Annotation:
Annotate the bounding boxes around the faces in the images. This step is necessary for training supervised face detection models.

VI. PROPOSED APPROACH

A. CNN Architecture
A Convolutional Neural Network (CNN) comprises layers designed for extracting and learning features from input data, commonly used for image recognition. The architecture typically includes convolutional layers, applying filters to detect patterns, followed by pooling layers, reducing spatial dimensions while retaining important information. Additional layers like fully connected layers interpret features and classify them. CNNs leverage techniques like dropout to prevent overfitting and activation functions like ReLU to introduce non-linearity.

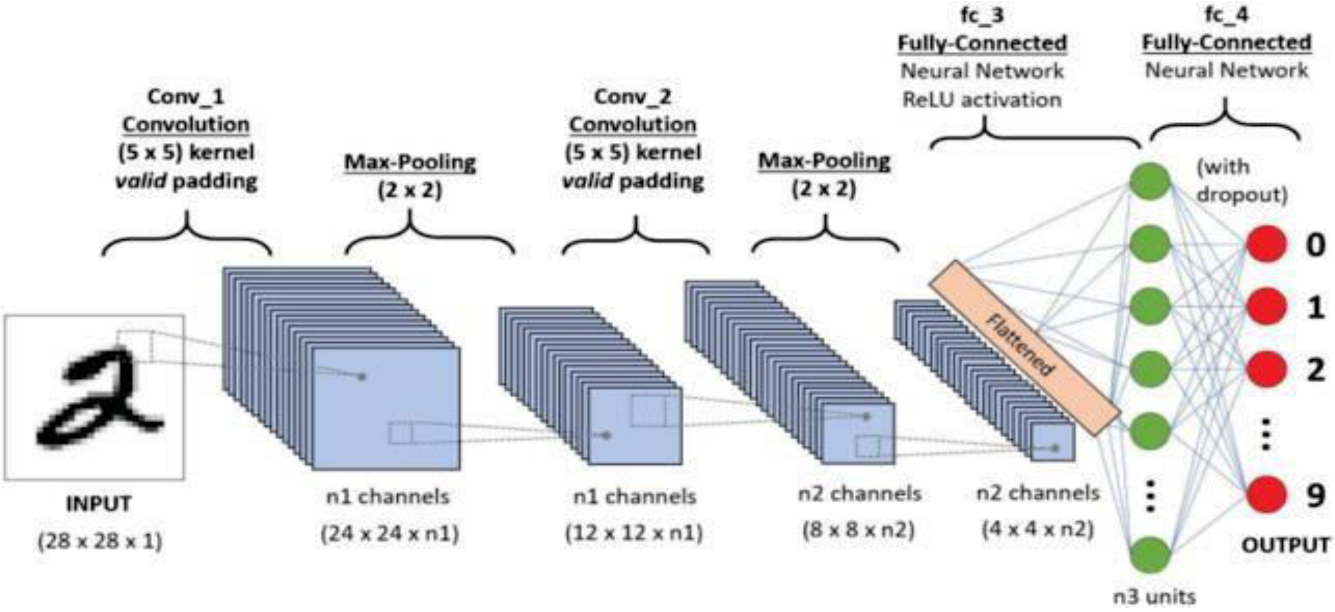


Fig 1. Architecture of Convolution neural network

Testing for image forgery involves various techniques to detect alterations or manipulations in images.Check the metadata of the image for any inconsistencies or alterations. Look for discrepancies in timestamps, camera information, or software used for editing.ELA helps detect areas of an image that have different compression levels, indicating potential areas of manipulation. Analyze individual pixel values to identify areas that have been altered. Sudden changes in pixel values or patterns may indicate tampering.Compare the content of the image with known reference images or databases to identify any plagiarized or manipulated content.Utilize deep learning algorithms trained to detect image forgeries. Convolutional Neural Networks (CNNs) can be trained on large datasets of authentic and manipulated images to identify forged content.Use reverse image search engines to check if the image has been previously published elsewhere on the internet, which can help identify if it's original or manipulated.

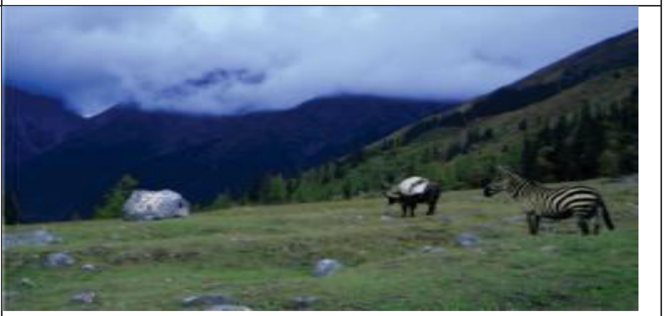
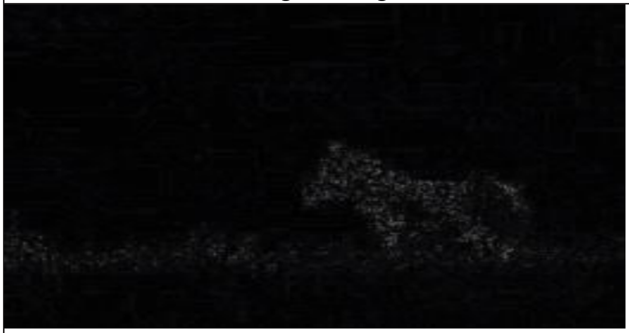
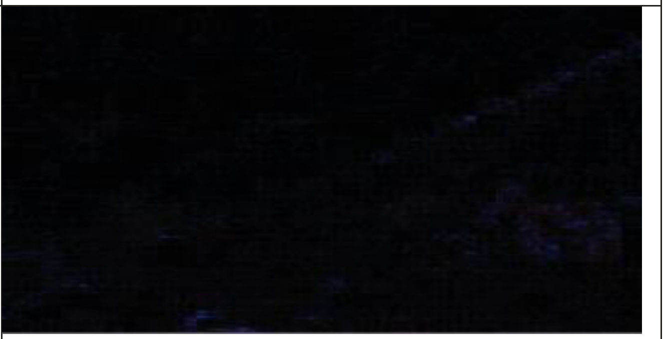
Original Image	Tampered Image
 Original image	 Tampered image
 ELA operated original image	 ELA operated Tampered image

Fig 2. Theoratical and Tampered Images

System testing for face detection begins with defining test cases that cover different aspects of the system's functionality. This includes testing for detecting faces in different lighting conditions, with various facial expressions, and from different angles. Test cases should also include scenarios involving multiple faces, occlusions, and varying distances from the camera.Additionally, system testing evaluates the speed and efficiency of the face detection algorithm.

Geometric:
This approach mainly deals with the spatial correlation uniting the profile (i.e. face) features, also we can simply that dimensional layout of the facial attributes. Some of the main geometrical attributes of a human face are nose, eyes and the mouth. Based on these attributes firstly the face is categorized and then based on these attributes respective spatial intervals and the respective associated gradients are estimated, thereby advancing the process of face recognition.

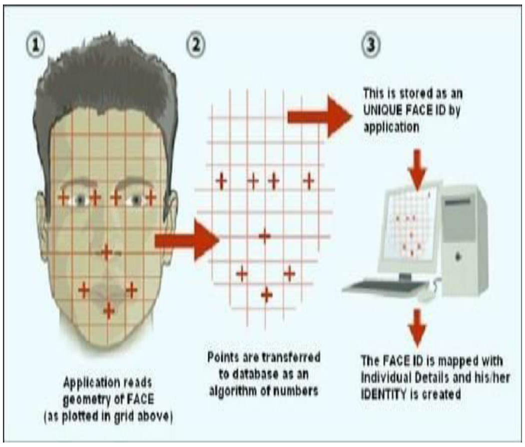

1
2
3
This is stored as an UNIQUE FACE ID by application
Application reads geometry of FACE (as plotted in grid above)
Points are transferred to database as an algorithm of numbers
The FACE ID is mapped with Individual Details and his/her IDENTITY is created

Fig 3. Geometric Approach

Photometric stereo:

It is a methodology of computer vision technology which mainly recuperates the structure of an underlying object from the images that were shot in varying circumstances that were affected by the lighting environment An arrangement of the surface standards shown by the slope chart that finally elucidate the retrieved entity’s configuration.

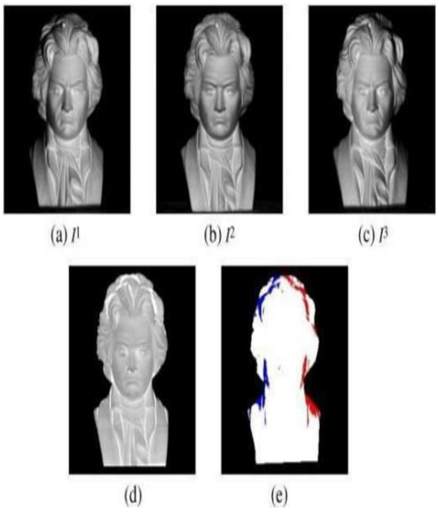


Fig 4. Photometric Sterio Image

Eigen Face Method (EFM):

Kohonen took the initiative of implementing the Eigen vectors for the problem of face recognition, by making use of simple neural network; for recognizing a human face in aligned and normalized position. Further advancement in this was done by Kirby and Sirovich by making use of Linear Encoding. A vector of size m*n represent the images and then the mean square error is minimized.

| DOI: 10.15680/IJIRCCE.2024.1205239 |

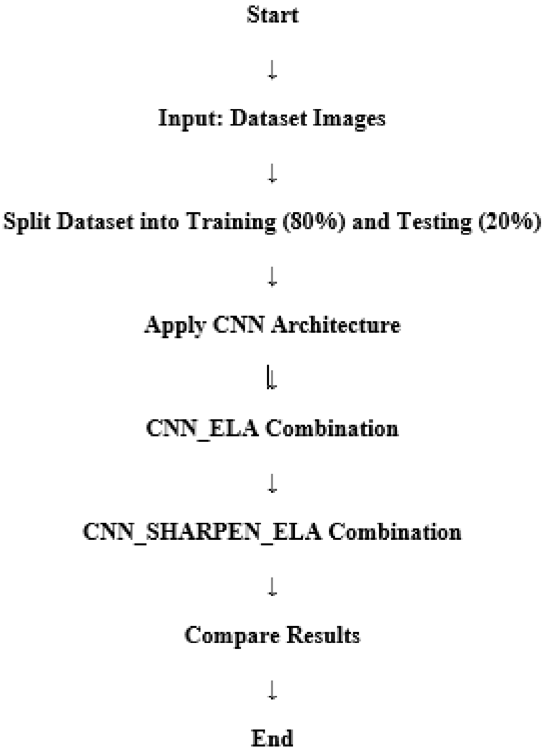


Fig 5. Data Flow Diagram

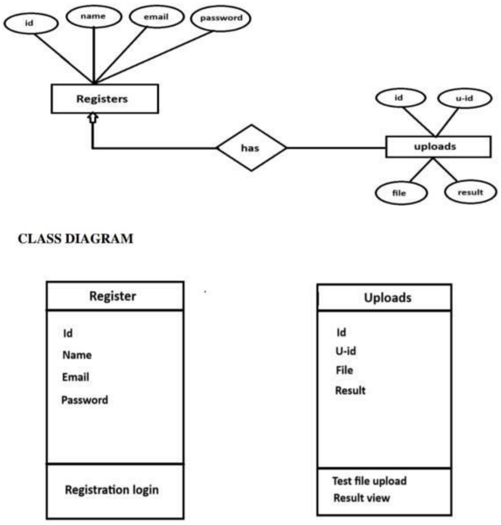


Fig 5. Entity Relationship Diagram

VII. EXPERIEMENTAL RESULTS

A. IMAGE FORGERY

The output result of image forgery detection using a CNN typically involves predicting whether a given image is authentic or contains some form of forgery. Here's how the output result might look.Image forgery detection using Convolutional Neural Networks (CNNs) is a crucial application of deep learning in digital forensics. The output result of such a system encompasses various aspects, including predictions, confidence scores, evaluation metrics, visualization, and error analysis.

After training on a dataset containing both authentic and forged images, the CNN is capable of classifying unseen images into one of two categories: authentic or forged. Each image inputted into the model yields a prediction, indicating the model's belief regarding the image's authenticity. This prediction serves as the foundation of the output result.Accompanying the prediction, the model generates confidence scores for each class.

B. FACE DETECTION

Face detection using Convolutional Neural Networks (CNNs) is a fundamental task in computer vision with various applications, including facial recognition, surveillance, and image analysis. The output result of a CNN-based face detection system encompasses several key aspects, including detection accuracy, bounding box localization, computational efficiency, and real-world applicability.At its core, the output result of face detection using CNNs revolves around accurately identifying the presence and location of faces within an image. The CNN is trained on a diverse dataset containing images with annotated bounding boxes around faces. During inference, the model processes an input image and generates bounding boxes around detected faces, along with confidence scores indicating the likelihood of each detection being a true positive.

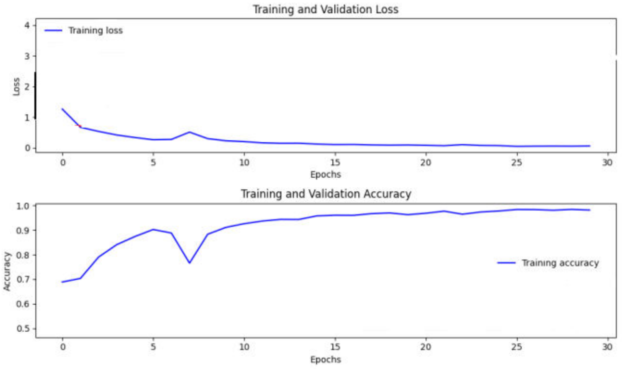


Fig 6. Training and Validation Accuracy

VIII. CONCLUSION AND FUTURE SCOPE

Certainly! In conclusion, the abstract encapsulates a dynamic exploration into the realm of image forgery detection, leveraging the advancements in deep convolutional neural networks. The acknowledgment of the ubiquity of digital content and the accessibility of powerful editing tools sets the stage for the paper's significance in addressing the consequential issue of content tampering. The dual-pronged approach proposed within the research is commendable. The meticulous examination of various pre-processing methods, coupled with diverse CNN architectures, reflects a commitment to a robust foundation for image analysis. The authors' emphasis on understanding the nuances of these techniques lays a solid groundwork for the subsequent evaluation of transfer learning. The second proposal delves into the realm of transfer learning, specifically employing pre-trained ImageNet models through fine-tuning. This strategic decision aligns with the contemporary trend of harnessing the knowledge embedded in broader datasets.

Future Scope is current approach can convert it from web applications to Android or ios app and also windows or any other os supporting app. It can expand as a cyber security network that can find deep fake vedios and forged vedios which can remove it easily.

REFERENCES

1. T. J De Carvalho, C. Riess, E. Angelopoulou, H. Pedrini And De Rezende Rocha, "Exposing Digital Image Forgeries By Illumination Color Classification," In Ieee Transactions On Information ForensicsAnd Security, vol. 8, no. 7, pp.1182- 1194,July2013,doi: 10.1109/TIFS.2013. 2265677.
2. J. Ouyang, Y. Liu and M. Liao, "Copy-move forgery detection based on deep learning," 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), 2017.

3. pp. 1-5, doi: 10.1109/CISP-BMEI.2017.8301940.
4. Nilsback,Maria-Elena, and Andrew Zisserman. "Automated flower classification over a large number of
5. classes.In 2008 Sixth Indian Conference on Computer Vision, Graphics & Image Processing, pp. 722- 729. IEEE, 2008.
6. Schaefer, Gerald, and Michal Stich. "UCID: An uncompressed color image database." In Storage and Retrieval Methods and Applications for Multimedia 2004, vol. 5307, pp. 472-480. International Society for Optics and Photonics, 2003.
7. Christlein, Vincent, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou. "An evaluation of popular copy-move forgery detection approaches." IEEE Transactions on information forensics and security 7, no. 6 (2012): 1841-1854.
8. Z. J. Barad and M. M. Goswami, "Image Forgery Detection using Deep Learning: A Survey," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 571-576, doi: 10.1109/ICACCS48705.2020.907440.
9. A comprehensive guide to convolutional neural network [Online],Available:https://towardsdatascience.com/a-comprehensive- guide-toconvolutional-neural-networks-the-eli5-way-3bd2b1164a53
10. https://www.engpaper.com/face-recognition-2018.htm
11. Manoharan, Samuel. "Image Detection, Classification and Recognition for Leak Detection in Automobiles." Journal of Innovative Image Processing (JIIP)1,no.02(2019):6170.https://www.semanticscholar.org/paper/Face-Detection-usin
12. g-Digital-Image-Processing-Jindal-Gup
13. ta/a0a9390e14beb38c504473c3adc857f8faeaebd2https://www.researchgate.net/publication/266873152. An application of Face recognition system using image processing and neural networks.
14. https://www.researchgate.net/publication/228963208 A MATLAB based Face Recognition System using Image Proessing and Neural Networks
15. https://www.researchgate.net/publication/228963208 A MATLAB based Face Recognition System using Image Proessing and Neural Networks
16. http://www.ijesi.org/papers/Vol(7)i4/Version-5/C0704051728.pdf

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details