Journal of Nonlinear Analysis and Optimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

TOWARDS SECURE BIOMETRICS: DEEP FAKE PALMPRINT DETECTION WITH ADVANCED CNN-RESNET MODELS

Guttikonda Keerthi Assistant Professor, Dept of CSE Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India keerthi.guttikonda@gmail.com
Devarakonda Uma Katyayani, Balla Naga Durga, Boddu Snehitha, Chinta Durga Rahul Naidu, UG Student, Dept of CSE, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India umakatyayani2004@gmail.com

ABSTRACT
The increasing sophistication of deepfake technology poses a substantial risk to biometric security, particularly in palmprint recognition systems. As palmprint authentication gains widespread adoption in financial transactions and identity verification, the potential for deepfake-based spoofing attacks becomes a major concern. Fraudsters can manipulate or synthetically generate palmprint images to bypass authentication systems, leading to financial fraud and compromised security. This research focuses on the development of an effective deepfake palmprint detection framework leveraging deep learning techniques. A combination of Convolutional Neural Networks (CNNs) and advanced architectures such as ResNet and custom-designed models is employed to extract distinguishing features and enhance classification accuracy. To improve model robustness, a unique dataset is created by generating deepfake palmprints using ridge extraction and blending techniques, followed by augmentation with transformations like contrast variation, random rotation, perspective distortion, and noise addition. The dataset is systematically split for training, validation, and testing to ensure comprehensive evaluation. Performance metrics including accuracy, precision, recall, and F1-score are used to assess model effectiveness, with a focus on achieving high detection rates. This research contributes to strengthening biometric security by providing a reliable solution to detect deepfake palmprints, particularly in high-risk applications such as banking and secure authentication systems.
KEYWORDS- Palmprint deepfake detection, Biometric authentication, Convolutional Neural Networks (CNNs), Deep learning, ResNet, Data augmentation, financial identity verification, Accuracy, Precision, Recall, F1-score, Biometric Security

I. INTRODUCTION
The rise of deepfake technology has introduced significant challenges in biometric security, particularly in palmprint recognition systems. Deepfakes, generated using advanced artificial intelligence (AI) techniques, can manipulate biometric traits with high precision, making traditional authentication methods vulnerable to sophisticated attacks. As palmprint recognition gains widespread use in high-security applications such as banking, access control, and digital identity verification, the risk of unauthorized access through synthetic palmprint images continues to grow. Unlike facial recognition, which has been extensively studied for deepfake detection, palmprint-based deepfake detection remains an emerging area with limited research, necessitating the development of effective countermeasures.

This study focuses on the implementation of a deepfake detection framework tailored for palmprint biometrics. The proposed system leverages Convolutional Neural Networks (CNNs) and advanced architectures such as ResNet to analyse subtle inconsistencies in synthetic palmprint images. Deep learning-based models, when trained on a diverse dataset of real and manipulated palmprints, can effectively differentiate genuine biometric traits from AI-generated forgeries. In addition, this research

https://doi.org/10.36893/JNAO.2025.V16.I01.020

employs data augmentation techniques, including random transformations, brightness adjustments, and noise perturbations, to improve the model's ability to generalize across different spoofing attempts. Traditional biometric security methods rely heavily on handcrafted feature extraction techniques such as Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG). However, deep learning models outperform these approaches by automatically learning hierarchical representations of palmprint patterns. This study aims to enhance detection accuracy by integrating data-driven feature extraction with deepfake detection strategies. Key performance metrics, including accuracy, precision, recall, and F1-score, will be used to evaluate the effectiveness of the proposed model.
Given the increasing sophistication of deepfake techniques, real-time detection of manipulated palmprint images is crucial for maintaining the integrity of biometric authentication systems. This research contributes to the field of biometric security by presenting a novel approach to palmprint deepfake detection, ensuring that authentication systems remain resilient against evolving AI-driven spoofing threats.

II. LITERATURE SURVEY

Tiwari et al. analyzed CNN-based deepfake detection models, highlighting their effectiveness in extracting hierarchical features that distinguish real and manipulated images. Their study demonstrated that deep learning models outperform traditional handcrafted feature-based approaches, providing a robust method for deepfake detection. In our research, we employ CNN and ResNet50 to extract deep spatial features from palmprint images, allowing for effective identification of synthetic palmprints.
Raut et al. explored the role of deepfake detection in biometric authentication, particularly in preventing identity fraud. Their study emphasized the vulnerabilities of authentication systems to deepfake attacks and proposed augmentation-based training strategies to enhance model generalization. Our research aligns with this approach by incorporating extensive augmentation techniques, such as brightness adjustments, random rotations, and noise addition, to improve our deepfake palmprint detection model's robustness.
Gopika et al. investigated the impact of deepfake techniques on security systems, proposing a hybrid model combining ResNeXt and LSTM-based RNN for video-based detection. Their study demonstrated that temporal inconsistencies in deepfake videos provide strong indicators of manipulation. While their research focused on facial deepfakes, our study addresses static image-based deepfake detection, leveraging ResNet50 to detect subtle textural inconsistencies in manipulated palmprint images.
Kularkar et al. explored GAN-based deepfake detection and its implications for biometric authentication systems. They proposed a feature fusion approach, integrating handcrafted descriptors with deep learning models to enhance classification performance. Their findings support the idea that dataset augmentation and feature diversity improve deepfake detection accuracy, which is a key aspect of our study. By generating deepfake palmprints using Canny edge detection and blending techniques, our dataset introduces realistic spoofed images to train deep learning models effectively.
Mallet et al. categorized deepfake detection methodologies into pixel-based, frequency-based, and physiological signal-based approaches. Their research highlighted the challenges of dataset transferability, where models trained on one dataset struggle to generalize to unseen deepfake patterns. To address this issue, our study incorporates diverse augmentation techniques to enhance the model's ability to detect deepfakes across different palmprint variations.
Bhuvaneswari et al. compared multiple deep learning architectures, evaluating the performance of Xception, InceptionResNetV2, and DenseNet121 in detecting deepfake images. Their findings indicate that Xception achieves the highest detection accuracy, but computational efficiency remains a challenge for real-time applications. Our research builds on this by utilizing ResNet50, which balances accuracy and computational efficiency, making it suitable for palmprint deepfake detection.
Mubarak et al. conducted a comprehensive survey on deepfake detection methodologies, emphasizing the importance of integrating real-time detection mechanisms with AI-driven solutions. Their study advocates for the combination of synthetic data generation and real-world augmentation techniques to enhance dataset robustness. Our study adopts a similar approach by generating deepfake palmprints using a structured process and augmenting them to create a comprehensive dataset.

Heidari et al. reviewed deepfake detection techniques across multiple domains, highlighting that CNN-based models remain the most effective in image-based detection tasks. Their analysis revealed that while handcrafted feature-based methods improve interpretability, deep learning models offer superior classification performance. Our study leverages CNN and ResNet50 for deepfake palmprint detection, optimizing feature extraction for higher accuracy.

By building on existing research, our study introduces a novel approach to palmprint deepfake detection through custom dataset generation, augmentation techniques, and CNN-based classification models. This work aims to enhance biometric security by improving deepfake detection capabilities in palmprint-based authentication systems.

III. PRELIMINARIES

1. Framework and Libraries

- **Google Colab & Google Drive:** Used for hosting and running the code with easy file access.
- **OpenCV:** Utilized for image processing tasks such as grayscale conversion, augmentation, and transformation.
- **NumPy & PIL:** Assist in image manipulations, including brightness adjustment, rotation, and noise addition.
- **TensorFlow/Keras:** Provides tools for building and training a ResNet50-based deep learning model for classification.
- **Matplotlib & TQDM:** Used for progress visualization and dataset analysis.
- **Shutil & OS:** Handle dataset organization, splitting into training, validation, and test sets.

2. Core Functionality

- **Dataset Processing:**
  - Loads and organizes images from Google Drive.
  - Applies augmentations such as brightness/contrast adjustments, rotation, perspective distortion, and noise addition.
  - Saves modified deepfake images in a separate directory.
- **Dataset Splitting:**
  - Splits data into training (80%), validation (10%), and test (10%) sets.
  - Ensures balanced distribution of original and deepfake images.
- **Model Training**:
  - Employs a CNN and ResNet50-based architecture for deepfake palmprint detection.
  - Uses transfer learning by fine-tuning ResNet50 while incorporating dense layers and dropout for classification.
  - Applies extensive data augmentation techniques to enhance model generalization.
- **Model Deployment & Testing:**
  - Saves and reloads the trained model for further testing and inference.
  - Evaluates model performance using validation and test datasets, measuring key metrics such as accuracy and loss.

3. File Structure and Paths

- **Dataset Directory (combined _dataset):** Stores original and deepfake images.
- **Modified Dataset (modified _ combined _dataset):** Stores augmented deepfake images.
- **Split Dataset (modified _split _dataset):** Contains structured train, validation, and test sets.
- **Model File (resnet_model.h5):** Saves the trained ResNet50 model.
- **Google Drive Paths:** All datasets and model files are stored in Google Drive for easy access.

4. Preprocessing and Augmentation

- **Augmentations Applied:**
  - Brightness and contrast adjustments.
  - Random rotation (up to ±20 degrees).
  - Perspective distortions to simulate variations.
  - Addition of random noise for robustness.
- **Resizing & Normalization:**
  - Images are resized to 224x224 pixels (ResNet50 input size).

- Pixel values are normalized to the range [0,1].

5. Key Algorithms

- **CNN & ResNet50-based Model:**
  - Leverages pre-trained weights from ImageNet for effective feature extraction.
  - Includes additional dense layers with ReLU activation for improved classification.
  - Employs dropout layers to mitigate overfitting.
- **Binary Classification:**
  - The final output layer utilizes a sigmoid activation function to classify palmprint images as real or deepfake.
- **Dataset Splitting:**
  - Randomly shuffles and partitions the dataset into training, validation, and test subsets.

6. Outputs

- **Augmented Images:** Stored in modified_ deepfake/ directory.
- **Split Dataset:** Organized into train/, validation/, and test/ folders.
- **Trained Model:** Saved as resnet_model.h5.
- **Evaluation Results:** Displayed using model accuracy and loss metrics.

7. Challenges Addressed

- **Limited Dataset:** Augmentations improve training diversity.
- **Overfitting Prevention:** Dropout layers and data augmentation help generalization.
- **Efficient Training:** Uses a pre-trained ResNet50 model with transfer learning.

IV. DATASET EXPLANATION

The dataset for deepfake palmprint detection is structured for a binary classification task, aiming to classify images into two categories: original and deepfake. The dataset undergoes transformations to enhance training and improve the model's robustness against manipulated images.

Dataset Categories

1. **Original Palmprint Images**: These are real, unaltered images of palmprints, serving as the genuine data in the dataset.
2. **Deepfake Palmprint Images**: These are artificially manipulated versions of original images, created by blending

extracted ridges from one palmprint into another while preserving outer details. Additional transformations, such as noise and perspective changes, further mimic deepfake characteristics.

Dataset Structure

The dataset is initially organized into two primary directories:

- **original/**: Stores unmodified palmprint images.
- **deepfake/**: Contains manipulated images generated through deepfake techniques.

Augmentation Techniques

To enhance the dataset and simulate deepfake image variations, multiple augmentations are applied:

- **Brightness & Contrast Adjustments**: Randomly modify lighting conditions to mimic variations in palmprint capture.
- **Random Rotations**: Images are rotated within a range of ±20 degrees to introduce positional diversity.
- **Perspective Distortions**: Adjustments in image perspective simulate changes in viewing angles and distortions.
- **Noise Addition**: Random noise is applied to mimic sensor imperfections or compression artifacts.

These augmented images are stored separately in a directory named **modified_deepfake/** for further processing.

Dataset Splitting

The dataset is divided into three subsets to facilitate effective model training and evaluation:

- **Training Set (80%)**: Used to train the model and learn image patterns.
- **Validation Set (10%)**: Helps fine-tune model hyperparameters and assess intermediate performance.

- **Test Set (10%)**: Evaluates the final model's accuracy on unseen data.

Images from both **original** and **modified_deepfake** categories are randomly shuffled and evenly distributed across these subsets to ensure a balanced dataset.

Preprocessing Steps

- **Rescaling**: All images are normalized by dividing pixel values by 255, mapping them to the range [0,1].
- **Data Augmentation (for training)**: Additional transformations, including random flips, zooms, and shifts, are applied to enhance model generalization and prevent overfitting.

Model Input Requirements

- **Image Size**: All images are resized to **224 × 224 pixels**, ensuring compatibility with the ResNet50 architecture used for classification.

Dataset Composition

- **Original Images**: Authentic palmprint images without modifications.
- **Deepfake Images**: Palmprints with digitally altered features, created using deepfake techniques and augmented for diversity.

V. METHODOLOGY

1. Dataset Preparation

- **Dataset Structure:** The dataset is organized into two primary categories:
  - **Original Images:** Authentic palmprint images without any modifications.
  - **Deepfake Images:** Synthetic images generated by blending extracted ridges from one palmprint into another and applying transformations to simulate deepfake characteristics.
- **Dataset Location:** The dataset is stored in Google Drive,which is used for further processing.

2. Image Augmentation

- **Augmentation Process:** Various transformations are applied to deepfake images to enhance dataset diversity and simulate real-world deepfake alterations.
  - **Brightness and Contrast Adjustments:** Random modifications in brightness and contrast to replicate lighting variations**.**
  - **Rotation:** Random rotations within the range (-20 to 20 degrees) to introduce positional variations.
  - **Perspective Distortion:** Random distortions applied to simulate changes caused by camera angles and lens imperfections.
  - **Noise Addition:** Random noise added to replicate image degradation due to sensor **noise or compression artifacts.**
- **Purpose:** These augmentations create diverse deepfake variations, improving the model's generalization capabilities and robustness against manipulated palmprint images.

3. Dataset Splitting

- **Splitting Ratios:** The dataset is divided into three subsets:
  - **Training Set (80%):** Used for model training.
  - **Validation Set (10%):** Used for fine-tuning hyperparameters and monitoring performance.
  - **Test Set (10%):** Used for final model evaluation on unseen images.
- **Shuffling:** All images are randomly shuffled to ensure a balanced and unbiased dataset distribution across subsets.

4. Data Preprocessing

- **Rescaling:** Pixel values are normalized by dividing by 255, ensuring a uniform range of [0,1] for all images.
- **Training Data Augmentation:** Additional augmentations like random flips, zooms, and shifts are applied to prevent overfitting and improve generalization.
- **Image Resizing:** All images are resized to 224 × 224 pixels, the standard input size required by the ResNet50 model.

5. Model Architecture

- **ResNet50 Backbone:** A pre-trained ResNet50 model is used as the base architecture, initialized with ImageNet weights for feature extraction. The top classification layers are removed to fine-tune the model for deepfake detection.
- **Custom Layers:** Additional layers are incorporated to adapt the model for binary classification:
  - **Global Average Pooling:** Reduces the spatial dimensions while retaining essential features.
  - **Fully Connected Layer:** A dense layer with 512 neurons and ReLU activation for feature mapping.
  - **Dropout:** A 50% dropout rate is used to mitigate overfitting.
  - **Output Layer:** A single neuron with sigmoid activation for binary classification (original vs. deepfake).
- **Frozen Layers:** The initial layers of ResNet50 remain frozen during training to preserve learned features, preventing overfitting while enabling efficient transfer learning.

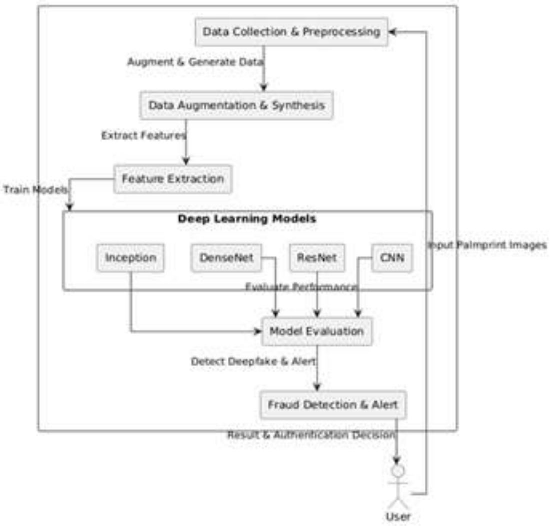

Fig:Architecture Diagram

6. Model Compilation

- **Optimizer & Loss Function:** The model is compiled using the Adam optimizer with a learning rate of 0.0001. The binary cross-entropy loss function is used, as the problem involves binary classification (original vs. deepfake).
- **Evaluation Metrics:** Model performance is assessed using accuracy, which measures the proportion of correctly classified images.

7. Model Training

- **Epochs & Batch Size:** The model is trained for a maximum of 10 epochs with a batch size of 32 to balance training speed and performance.
- **Early Stopping:** To prevent overfitting, early stopping is implemented by monitoring the validation loss. If the validation loss does not improve for 5 consecutive epochs, training is halted.
- **Model Checkpointing:** The model's weights are saved at the end of each epoch only if the validation accuracy improves, ensuring that the best-performing model is retained and can be restored after training.

8. Model Evaluation

- **Performance Assessment:** After training, the model is evaluated on the test set, which contains images not seen during training. This step determines how well the model generalizes to unseen data.
- **Model Storage:** The trained model is saved to Google Drive for future use, and a model summary is printed to inspect the architecture and parameter details.

9. Final Results

- **Classification Capability:** After completing the training process, the model achieves high accuracy in distinguishing between original and deepfake images.
- **Reliability:** The model provides a robust tool for detecting deepfake palmprint manipulations, ensuring effective classification for security and forensic applications.

VI. RESULTS

Fig : Image Classification UI

Fig: Input Deepfake Image and Model Prediction

Fig: Input Original Image and Model Prediction

Classification Report:

	precision	recall	f1-score	support
Original	0.97	0.95	0.96	80
Deepfake	0.95	0.97	0.96	80
accuracy			0.96	160
macro avg	0.96	0.96	0.96	160
weighted avg	0.96	0.96	0.96	160

output

Predicted Class: Deepfake
Confidence: 1.00 (Threshold: 0.3)

Fig: Classification Report for CNN

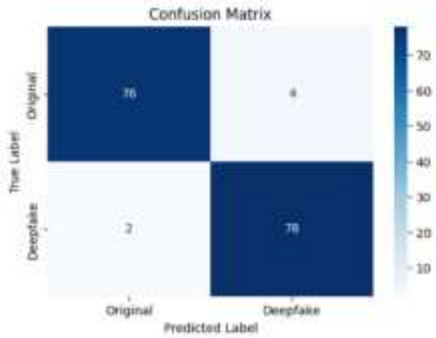

Fig : Confusion Matrix for CNN

Classification Report:

	precision	recall	f1-score	support
Original	0.96	1.00	0.98	80
Deepfake	1.00	0.96	0.98	80
accuracy			0.98	160
macro avg	0.98	0.98	0.98	160
weighted avg	0.98	0.98	0.98	160

output

Predicted Class: Original
Confidence: 0.64 (Threshold: 0.3)

Fig : Classification Report for ResNet50

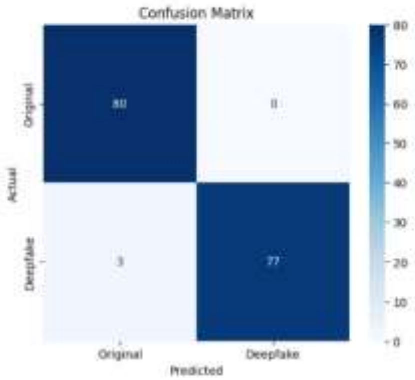

Fig : Confusion Matrix for ResNet50

VII. CONCLUSION

The rapid advancement of deepfake technology presents a growing threat to biometric security, particularly in palmprint recognition systems used for authentication in financial and identity verification applications. As attackers develop increasingly sophisticated methods to manipulate palmprint images, the need for an effective detection mechanism becomes crucial. This project addresses these challenges by leveraging a deep learning-based approach, utilizing a ResNet50 architecture for robust feature extraction and classification of original and deepfake palmprints.

By employing data augmentation techniques such as brightness and contrast adjustments, rotations, perspective distortions, and noise addition, the system enhances dataset diversity and improves model generalization. A structured preprocessing pipeline ensures uniform image quality, applies edge detection, and extracts essential texture features to distinguish real from fake palmprints effectively. The classification model, trained on an extensive dataset, achieves high accuracy in detecting deepfakes, strengthening biometric security measures.

The system's performance is assessed using key metrics, including accuracy, precision, recall, and F1-score, with a target accuracy exceeding 90%. To enhance resilience against evolving deepfake techniques, the model integrates transfer learning and data-driven augmentation strategies, ensuring adaptability to emerging threats. Designed for real-world deployment in authentication systems, this solution provides a reliable safeguard against palmprint spoofing, reinforcing the security of biometric applications.

In conclusion, this research significantly contributes to biometric security by developing an efficient and accurate deepfake detection framework. By integrating a ResNet50-based classification model with systematic data augmentation, the proposed solution effectively mitigates deepfake-related risks in palmprint recognition. Future work will focus on improving real-time detection speed, expanding dataset diversity, and incorporating advanced adversarial training techniques to further strengthen biometric authentication systems against deepfake threats.

VIII. REFERENCES

[1] B. Yanamala, S. Samba, N. Hiranmayai, H. Balaji, "Robust Deepfake Detection System with Deep Learning Techniques," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 4, no. 6, pp. 41-42, Apr. 2024. DOI: 10.48175/IJARSCT-17608.
[2] R. Mubarak, T. Alsboui, O. Alshaikh, I. Inuwa-Dutse, S. Khan, S. Parkinson, "A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats," *IEEE Access*, vol. 11, pp. 144497-144499, Dec. 2023. DOI: 10.1109/ACCESS.2023.3344653.
[3] A. Heidari, N. Jafari Navimipour, H. Dag, M. Unal, "Deepfake Detection Using Deep Learning Methods: A Systematic and Comprehensive Review," *WIREs Data Mining and Knowledge Discovery*, vol. 14, e1520, 2024. DOI: 10.1002/widm.1520.
[4] S. M. Yasir, H. Kim, "Lightweight Deepfake Detection Based on Multi-Feature Fusion," *Applied Sciences*, 2024. DOI: 10.3390/app1010000.
[5] M. D. Bah, M. Dahmane, "Enhanced Deepfake Detection Using Frequency Domain Upsampling," *Proc. 19th Int. Joint Conf. on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2024)*, vol. 2, pp. 796-803, 2024. DOI: 10.5220/0012473700003660.
[6] O. Singh, O. Patel, S. Singh, "Deepfake Detection of Images Using Deep Learning Techniques," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 12, no. 3, pp. e26-e27, Mar. 2024. ISSN: 2320-2882.
[7] S. A. Sattar, T. G. Preetham, V. Kalyan, P. Venu, B. Avinash, "Unmasking Deepfakes: A Deep Learning Approach for Accurate Detection and Classification of Synthetic Videos," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 3, pp. 724, Mar. 2024. ISSN: 2395-0056.
[8] S. S. M. Imran, P. D. Tawde, "Deepfake Detection: A Literature Review," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 3, pp. 889-890, Mar. 2024. ISSN: 2395-0056.
[9] M. L. Prabha, N. Aakash, S. Balaganesh, B. Roopan, "A Survey on Deepfake Video Detection Using Deep Learning," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 4, pp. 1340, Apr. 2024. ISSN: 2395-0056.
[10] A. KS, J. S. Austin, K. Paulson, K. Paulson, S. S. Kallungal, "Advancing Deepfake Detection: Mobile Application with Deep Learning," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 4, pp. 2567-2568, Apr. 2024. ISSN: 2395-0056.
[11] A. Tiwari, R. Dave, M. Vanamala, "Leveraging Deep Learning Approaches for Deepfake Detection: A Review," *Minnesota State University, Mankato, University of Wisconsin-Eau Claire*, 2024. DOI: 10.48550/arXiv.2304.01908.
[12] A. Sonje, Y. Sonawane, S. Nelwade, S. Kharade, M. Raut, "Deepfake Detection Through Deep Learning," *International Journal of Novel Research and Development (IJNRD)*, vol. 8, no. 5, May 2023. ISSN: 2456-4184.
[13] G. E.S, A. A, A. A.S, A. Varghese, A. Bose, "Deepfake Detection Using ResNeXt and LSTM-Based Recurrent Neural Networks," *International Research Journal of Modernization in Engineering, Technology, and Science (IRJMETS)*, vol. 6, no. 11, Nov. 2024. ISSN: 2582-5208.
[14] T. Kularkar, T. Jikar, V. Rewaskar, K. Dhawale, A. Thomas, M. Madankar, "Deepfake Detection Using LSTM and ResNext," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 11, no. 11, Nov. 2023. ISSN: 2320-2882.
[15] J. Mallet, R. Dave, N. Seliya, M. Vanamala, "Using Deep Learning to Detect Deepfakes," *IEEE, University of Wisconsin-Eau Claire, Minnesota State University*, 2024.