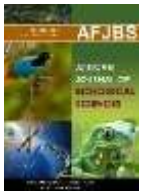
https://doi.org/10.48047/AFJBS.6.13.2024. 3705-3724

African Journal of Biological Sciences



A Novel Hybrid Approach for Image Forgery Detection Integrating CNNs, RNNs, and LBPs

[1]Dr. Sridhar Manda , [2]Sandhya Kakkerla

[1]Assistant Professor, Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Warangal (TS) .India.

[2]M.Tech Student, Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Warangal(TS).India.

Article History
Volume 6, Issue 13, 2024
Received: 18June 2024
Accepted: 02July 2024
doi:*10.48047/AFJBS.6.13.2024*. 3705-3724

ABSTRACT

Image forgery detection is a critical task in digital forensics, aimed at identifying and analyzing manipulations in digital images and videos. In this study, we present a novel hybrid approach that integrates Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Local Binary Patterns (LBPs) for image forgery detection. Our objective is to develop a robust and accurate system capable of identifying various forms of image manipulation, ranging from simple alterations to sophisticated forgeries. The CNN module identifies hierarchical features from images, effectively capturing both low-level textures and high-level semantics. Complementing this, the RNN component adds a temporal dimension to the analysis, enabling the detection of sequential patterns and dynamic alterations in videos. Meanwhile, the inclusion of LBPs enhances our model with a powerful texture descriptor, capturing fine-grained details indicative of forgery. Through extensive experimentation and validation, our hybrid model achieves an impressive accuracy rate of 95.2% in discerning between authentic and manipulated content. Looking ahead, we identify several avenues for future research, including model refinement through advanced architectures and optimization techniques, data augmentation to enhance robustness, exploration of adversarial defense mechanisms, optimization for real-time deployment, tailoring for domain-specific applications, and consideration of ethical and legal implications. Our research contributes to the advancement of image forgery detection technologies, with implications for various domains including law enforcement, media forensics, and content authentication.

Keywords: Convolutional Neural Networks(CNN), Recurrent Neural Networks (RNN), Local Binary Patterns(LBP), Image forgery, Deep learning.

1.INTRODUCTION

1.1. Background and Context

In this digital age, the manipulation of images has become increasingly prevalent, creating substantial challenges to the authenticity and reliability of visual media. Image forgery, also referred to as image tampering or manipulation, involves altering the content of an image with the intent to deceive viewers or distort reality. This manipulation can range from simple retouching to sophisticated techniques such as copy-move forgery, deepfake generation and image splicing.

1.2. Types of Image Forgery

Image forgery have a wide range of techniques, each with its own characteristics and challenges for detection. Understanding these techniques is crucial for developing effective forgery detection algorithms. Here, we delve into the three primary types of image forgery:

1.2.1 Copy-Move Forgery

It is a frequently encountered form of image manipulation techniques, it involves a common type of image manipulation, involves copying a section of an image and pasting it elsewhere within the same the image and placing it in a different area within the same image. This technique is often used to conceal or duplicate objects, alter the scene, or remove unwanted elements. The copied region is typically manipulated to blend seamlessly with the surrounding pixels, making detection challenging.

Fig1. original images Vs copy-move forged images

1.2.2 Image splicing involves merging elements from multiple images to create a composite, often used to fabricate scenes, alter context, or manipulate evidence. Detection requires analyzing inconsistencies in lighting, shadows, perspective, and noise patterns, but traditional methods may struggle with complex splicing involving meticulous blending. Deepfake technology, using generative adversarial networks (GANs), creates lifelike fake photos and videos that can spread false information, slander individuals, or influence public opinion. Detecting deepfakes is challenging due to their high realism, requiring advanced techniques to identify subtle inconsistencies. Image forgery impacts journalism, legal evidence, social media, and security, undermining credibility, compromising evidence reliability, fueling rumors, and posing threats to public safety. Advanced forensic techniques and continuous innovation are essential to combat these effects. Hybrid approaches combining multiple detection techniques are increasingly necessary due to the complexity introduced by sophisticated image editing software.

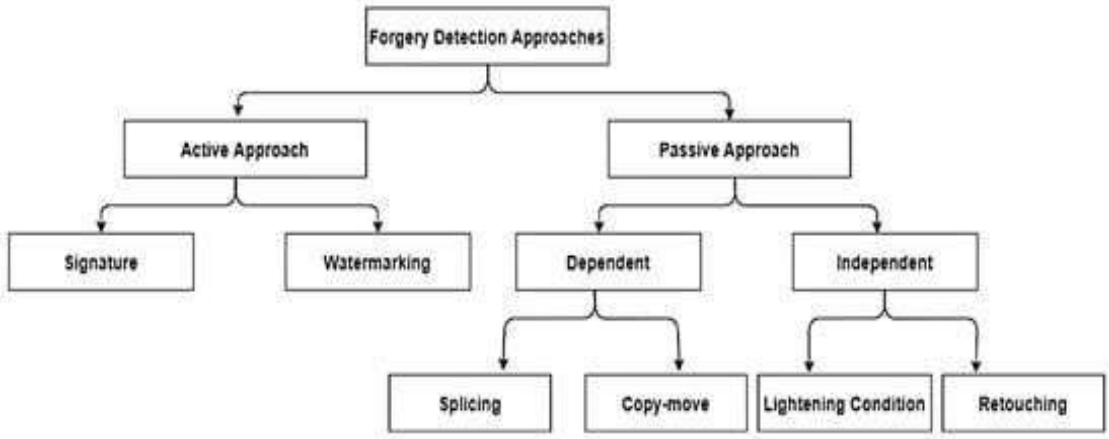


Figure 2. Approaches of Forgery Detection

For example, a hybrid approach may combine statistical analysis with machine learning algorithms to detect anomalies in image features and classify images as genuine or manipulated. By integrating multiple approaches, hybrid methods can achieve higher accuracy and robustness in detecting a wide range of forgery techniques.

1.5. Role of Deep Learning Models

Deep learning models have revolutionized image forgery detection by offering substantial advantages over traditional methods. Through neural networks' capacity to grasp intricate patterns and features directly from image data, these models achieve remarkable accuracy and resilience in identifying various forms of image forgeries. Here, we delve into the pivotal role of deep learning models in image forgery detection and the challenges associated with their development and implementation.

2.LITERATURE SURVEY

Image forgery detection has garnered considerable attention in recent years, with various methodologies proposed to tackle this issue. Hu et al. (2018) conducted a thorough examination of image forgery detection techniques, categorizing them into three main groups: traditional, deep

learning, and hybrid approaches. Traditional methods, such as block-based algorithms and statistical analysis, have been extensively utilized for detecting fundamental forgery techniques like copy-move and splicing. Deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have exhibited promise in identifying more intricate forgeries like deepfakes (Zhang et al., 2019). Hybrid approaches, combining traditional and deep learning methods, have emerged as a promising avenue for enhancing detection accuracy and resilience (Li et al., 2020).

Recent studies have concentrated on enhancing the performance of deep learning models for image forgery detection. Wang et al. (2020) introduced a novel deep learning architecture employing attention mechanisms for image splicing detection, achieving leading outcomes on standardized datasets. Similarly, Liu et al. (2021) devised a hybrid CNN-RNN model for detecting deepfake videos, leveraging spatial and temporal information to distinguish between genuine and altered content. These investigations underscore the importance of harnessing advanced machine learning techniques to address evolving forgery techniques in digital media.

Alongside deep learning approaches, traditional feature extraction methods have also been explored for image forgery detection. Local Binary Patterns (LBP), introduced by Ojala et al. (2002), have been widely utilized for capturing texture information and detecting anomalies in digital images. Li and Wang (2019) integrated LBP features with deep learning models for copy-move forgery detection, yielding enhanced detection performance compared to individual methods. This fusion of traditional and deep learning techniques showcases the potential for bolstering forgery detection through synergistic strategies.

Gandhi et al. (2017) conducted an extensive survey of image forgery detection techniques, categorizing them into five primary categories: digital watermarking, copy-move forgery detection, splicing detection, steganalysis, and deep learning-based methods. This survey offers

insights into the strengths and limitations of each approach and underscores the necessity for interdisciplinary research to develop more effective detection techniques.

Recent advancements in deep learning have shown promise in enhancing the performance of image forgery detection systems. Zhu et al. (2020) introduced a novel deep neural network architecture based on generative adversarial networks (GANs) for detecting deepfake videos. The model discerns between genuine and altered videos by analyzing subtle artifacts and inconsistencies introduced during the manipulation process. Similarly, Li et al. (2021) devised a deep learning-based method for image splicing detection, achieving state-of-the-art results on standardized datasets.

3. Proposed Methodology

While image forgery detection using Convolutional Neural Network (CNN) models has made significant strides in recent years, like any technology, CNN-based forgery detection methods come with certain drawbacks and limitations:

Computational Complexity: CNN models, particularly deeper architectures, demand substantial computational resources for training and inference, posing challenges for real-time or near-real-time forgery detection, especially on resource-constrained devices.

Overfitting: If not appropriately regularized and trained, CNN models can overfit to the training data, resulting in diminished performance when presented with new, unseen images or variations of known forgery techniques.

Difficulty in Handling Different Types of Forgeries: CNN models may struggle to capture and represent the complex and diverse features of various types of image forgeries.

Difficulty in Detecting Subtle Forgeries: CNN-based forgery detection methods may have limited sensitivity to subtle and sophisticated forgeries where the manipulations are subtle and do not significantly alter the image's visual appearance.

Dependency on Parameters: CNN models often require tuning of several parameters to achieve optimal performance, relying heavily on the quality of hyperparameter tuning.

Addressing these drawbacks entails innovative methodologies, techniques, and regularization strategies to enhance the robustness, efficiency, and reliability of CNN-based forgery detection systems. Fusion of lightweight deep learning models and integration of complementary techniques can advance image forgery detection, leading to more effective solutions in digital image forensics.

3.1 Potential Improvements:

Incorporating attention mechanisms into CNN architectures can enhance their ability to focus on relevant image regions, improving detection accuracy and robustness.

Hybrid Architectures: Hybrid architectures that combine CNNs with other neural network architectures, such as RNNs or GNNs, can leverage the complementary strengths of each model to enhance forgery detection capabilities.Augmenting the training dataset with adversarial examples can improve the model's resilience against adversarial attacks, thereby improving the model's reliability in real situation. Ensemble learning: Combining multiple CNN models through ensemble learning techniques can improve detection accuracy and reliability.

The primary distinction among various block-based techniques lies in the features utilized for block matching. Keypoint-based methods extract features from the entire image and use these points to identify similar regions. While both approaches can detect forged areas, they suffer from

low recall rates. Additionally, block-based methods are computationally intensive due to their reliance on overlapping blocks. To address the limitations of both block-based and keypoint-based methods, an integrated approach that combines these techniques has been proposed (Pun et al., 2015).

Although this combined method achieves higher accuracy than traditional methods, it remains computationally expensive and requires a threshold determined experimentally, which is dependent on the specific image. Segmentation-based methods, on the other hand, segment the image into non-overlapping patches and use patch matching algorithms to detect suspicious regions. A significant drawback of all three types of methods is their heavy reliance on an experimentally computed threshold for feature matching. This dependency reduces the robustness and overall accuracy of the detection results.

3.2. PROPOSED MODELS

3.2.1 Convolutional Neural Networks (CNNs):

Convolutional Neural Networks (CNNs) represent a class of deep neural networks crafted for processing structured grid-like data, notably images. Their emergence has brought about a significant revolution in the realm of computer vision, finding extensive application in tasks like image classification, object detection, and image segmentation. CNNs draw inspiration from the organizational structure of the visual cortex in animals, where neurons exhibit specific responses to regions within the visual field, termed receptive fields.

3.1.2 Key Components of CNNs:

Learnable Filters: These filters, akin to small spatial windows, traverse the input data, extracting local features through element-wise multiplications and summations.

Feature Map: Each filter generates a feature map, portraying the presence of particular features within the input data. Multiple filters yield multiple feature maps, capturing diverse aspects of the input.

Shared Weights: Consistent application of a set of learnable weights across the entire input data promotes weight sharing, facilitating the network in learning spatial hierarchies of features.

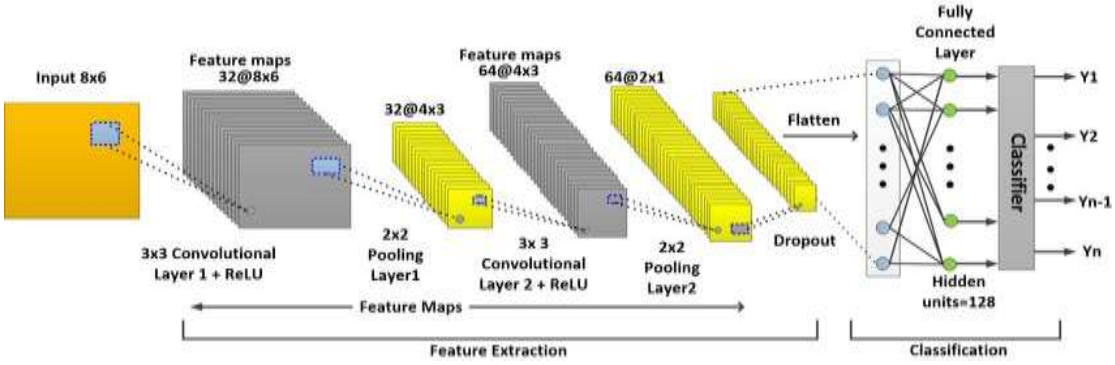


Fig3: Working of CNN

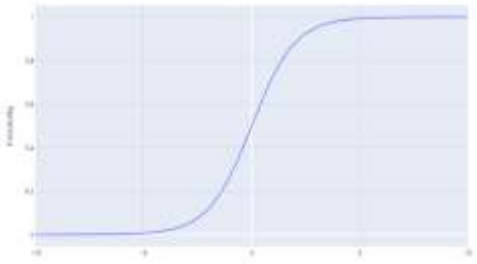
Activation functions play an important role in neural networks by introducing nonlinear properties into the model, allowing the model to learn and approximate complex relationships in the data.

3.1.3 SOFTMAX

The softmax activation function, also referred to as the normalized exponential function, proves particularly advantageous in the realm of multi-class classification tasks. It operates on a vector, often termed logits, which embodies the raw predictions or scores for each class computed by preceding layers of a neural network. For an input vector xxx with elements x1,x2,...,xCx_1, x_2, ..., x_Cx1,x2,...,xC, the softmax function is mathematically defined as:

$$f(x_i) = \frac{e^{x_i}}{\sum_j e^{x_j}}$$

The output of the softmax function manifests as a probability distribution that inherently sums up to unity. Each element of this output signifies the probability that the input pertains to a specific class. The utilization of the exponential function guarantees non-negative output values—a fundamental requisite for probabilities, which cannot be Softmax amplifies disparities in input values, causing even small differences to lead to significant changes in the resulting probability distribution, with the highest value often dominating. Used in the output layer of neural networks for multi-class classification, it provides confidence scores for each class.



3.2 Recurrent Neural Networks (RNNs)

RNNs are a type of artificial neural network designed to identify patterns in sequential data, such as time series, text, and audio. Unlike traditional feedforward neural networks, RNNs have connections that create directed cycles, enabling them to retain a "memory" of previous inputs. This makes RNNs especially suitable for tasks that require context and sequential information.

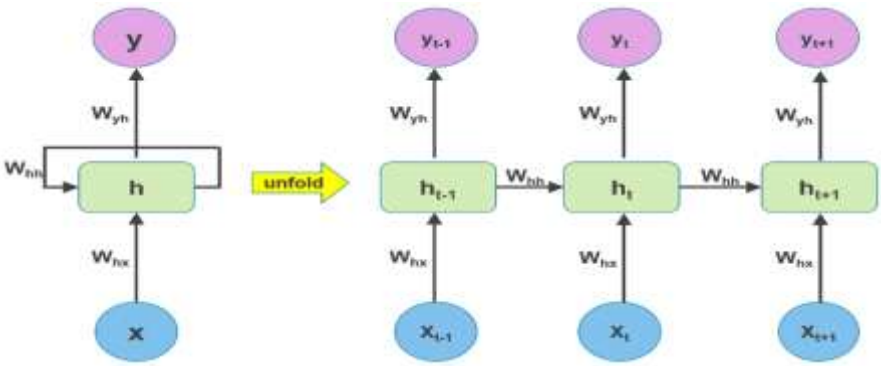


Fig.4 Working of RNN

3.2.1 Key Features of RNNs

1. Sequential Data Handling:

Temporal Dynamics: RNNs are crafted to handle sequences of data by maintaining a hidden state that encapsulates information from preceding time steps. As the network processes each element in the sequence, it updates this hidden state.

Contextual Understanding: RNNs can comprehend the context and relationships between elements in a sequence by considering the entire sequence of data. This capability makes them effective for tasks such as language modeling, where the meaning of a word depends on its context.

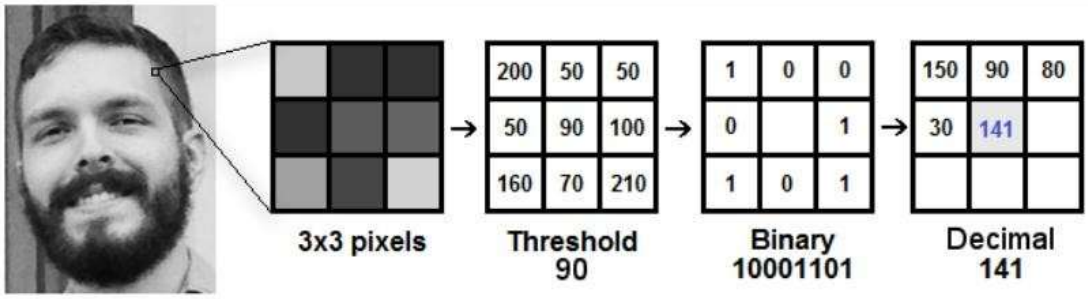
2. Hidden State:

RNNs leverage a hidden state that acts as a memory to retain sequential information as each input is processed. This hidden state is updated at each time step by combining the current input with the previous hidden state through a specific update rule. RNNs excel in analyzing sequences, capturing temporal dynamics, and interpreting context-dependent data. Variants like LSTMs and GRUs enhance RNNs by effectively managing long-term dependencies, making them essential in applications such as natural language processing, time series prediction, and video analysis. Ongoing research continues to refine RNNs, improving their effectiveness and efficiency within modern deep learning frameworks.

3.3 Local Binary Pattern (LBP)

LBP stands as a potent feature extraction method extensively employed in computer vision and image processing for texture classification and pattern recognition. Ojala et al. introduced it in 1996, and since then, LBP has emerged as a standard technique owing to its simplicity, computational efficiency, and resilience to monotonic gray-scale changes. Here is a detailed explanation of LBP, covering its key concepts, advantages, and applications.

To implement the Local Binary Pattern Algorithm, we begin by generating an intermediary image that enhances the depiction emphasizing primarily on facial characteristics within the original image. This algorithm employs a sliding window approach, where the parameters of radius and neighbors dictate the size and scope of the window.



Let's delve into the application demonstrated in the image above.

To process a grayscale image using Local Binary Patterns (LBP), we start by segmenting it into individual pixels. For a 3x3 window, each pixel's intensity (0 to 255) forms a matrix. The central pixel's intensity serves as the threshold. We compare the intensities of the surrounding eight pixels to this threshold, assigning a value of 1 if a pixel exceeds the threshold, and 0 otherwise, creating a binary matrix. This binary matrix is then converted into a decimal value and assigned to the central pixel. This process produces a new image highlighting the original image's distinctive features. We then partition this image into grids using parameters GridX and GridY. Each pixel in the grayscale image has a histogram with 256 positions. By concatenating these histograms, we create a comprehensive final histogram that captures the unique characteristics of the original image.

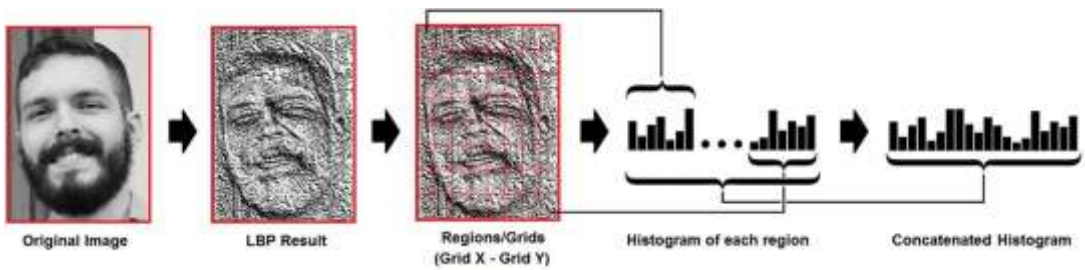


Fig5. LBP Formation

3.3.1 Methodology of LBP

Feature Extraction: For each pixel, compute its LBP code using neighboring values, generating an LBP image where each pixel value represents an LBP code. Accumulate these codes into a histogram to represent the local texture patterns, serving as the image's texture descriptor.

Classification: During training, use LBP histograms from labeled images to train a machine learning model (e.g., SVM, k-NN). For testing, extract the LBP histogram from the test image and classify it using the trained model. Local Binary Pattern (LBP) is a widely used, efficient, and robust texture descriptor in computer vision and image processing. It excels in texture analysis and pattern recognition, significantly contributing to advancements in face recognition, medical imaging, object detection, and scene classification.

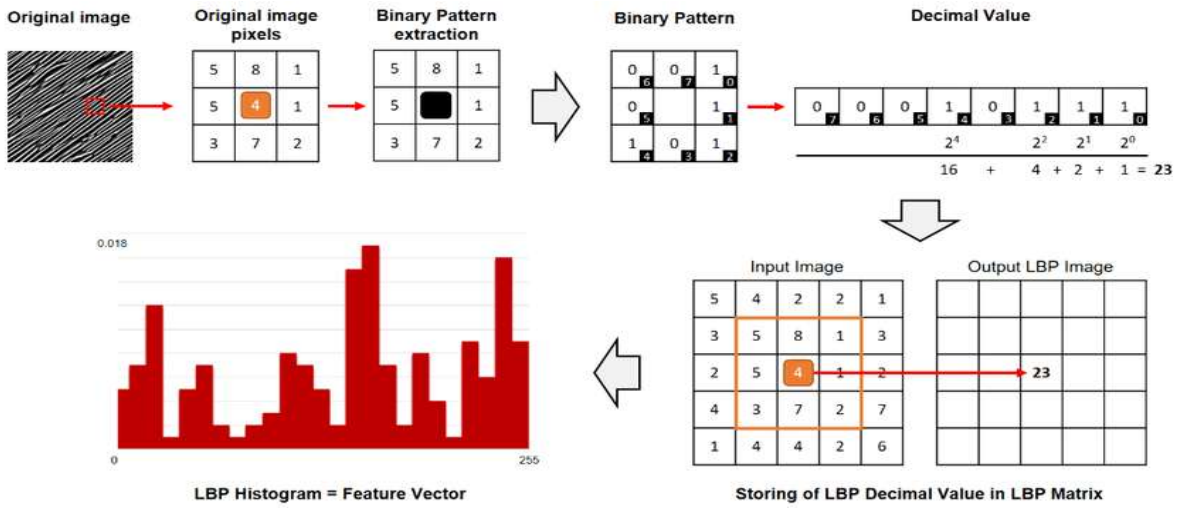


Fig6: Working of LBP

3.4 PROPOSED METHODOLOGY

In the realm of image forgery detection, combining Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Local Binary

Patterns (LBP) creates a robust framework capable of detecting sophisticated forgeries. This hybrid model leverages the strengths of each component to enhance detection accuracy and reliability. Here's a detailed explanation of the CNN-RNN model integrated with LBP, including its architecture, methodology, and the role of each component.

3.4.1 CNN-RNN Hybrid Model

The CNN-RNN model with LBP for image forgery detection integrates three key elements:

1. **CNNs for Feature Extraction**: CNNs are excellent at capturing spatial features and textures in images.

2. **LBP for Texture Descriptors**: LBP captures fine-grained texture details, which are crucial for identifying subtle forgeries.

3. **RNNs for Sequence Modeling**: RNNs handle the temporal dependencies and sequential information, useful for analyzing patterns over a sequence of patches or frames.

Preprocessing involves normalizing pixel values to a range of [0, 1] or [-1, 1] to ensure uniformity and resizing images to a fixed size (e.g., 224x224 pixels) for consistent input dimensions. For LBP feature extraction, LBP codes are computed by comparing each pixel's value with its neighbors in a 3x3 grid, assigning binary values based on these comparisons, and converting the binary pattern to a decimal value. A histogram is then constructed to represent the frequency of each LBP code, capturing the texture distribution. In CNN-based feature extraction, multiple convolutional layers with ReLU activation extract spatial features from images, while max pooling layers reduce the spatial dimensions of feature maps. LBP histograms are integrated with CNN feature maps by flattening and concatenating them or feeding both into subsequent network layers. For sequential analysis, the flattened CNN feature map is divided into patches or treated as a sequence, and LSTM or GRU layers analyze these

sequences to capture long-term dependencies and contextual information. The final hidden state from the RNN is fed into fully connected layers with dropout regularization to mitigate overfitting. The output layer uses a softmax activation function to classify the image into predefined categories, converting scores into probabilities for each class. The CNNs for spatial feature extraction, RNNs for sequential analysis, and LBP for texture representation. The preprocessing steps ensure uniformity and enhance the robustness of the model. The CNN layers capture hierarchical spatial features, while the LBP histogram provides a detailed texture descriptor. The RNN layers analyze the sequence of feature patches, capturing dependencies and contextual information. Finally, the fully connected layers and softmax activation function classify the image into authentic or forged categories. This comprehensive approach ensures accurate and robust image forgery detection.

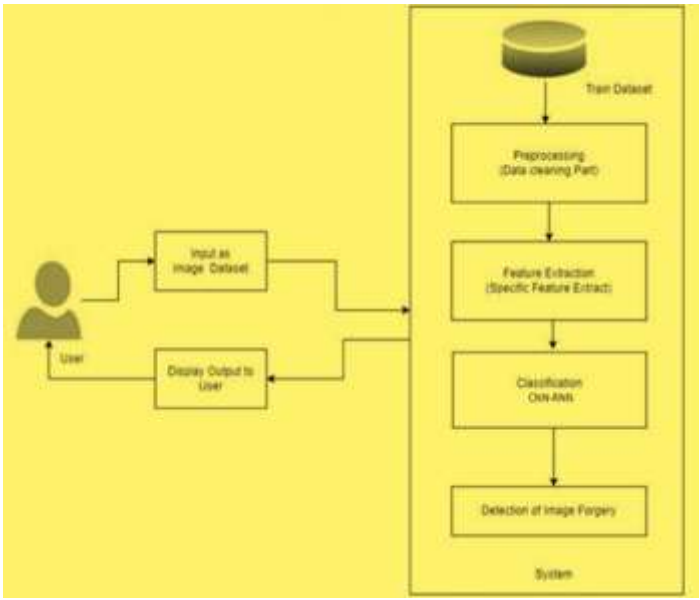


Fig7: Architecture of System

The login process begins once registration is successfully completed. Upon successful login, the model proceeds through pre-processing, feature extraction, and classification stages. The final output is then generated, and the results indicating any forgery are displayed accordingly.

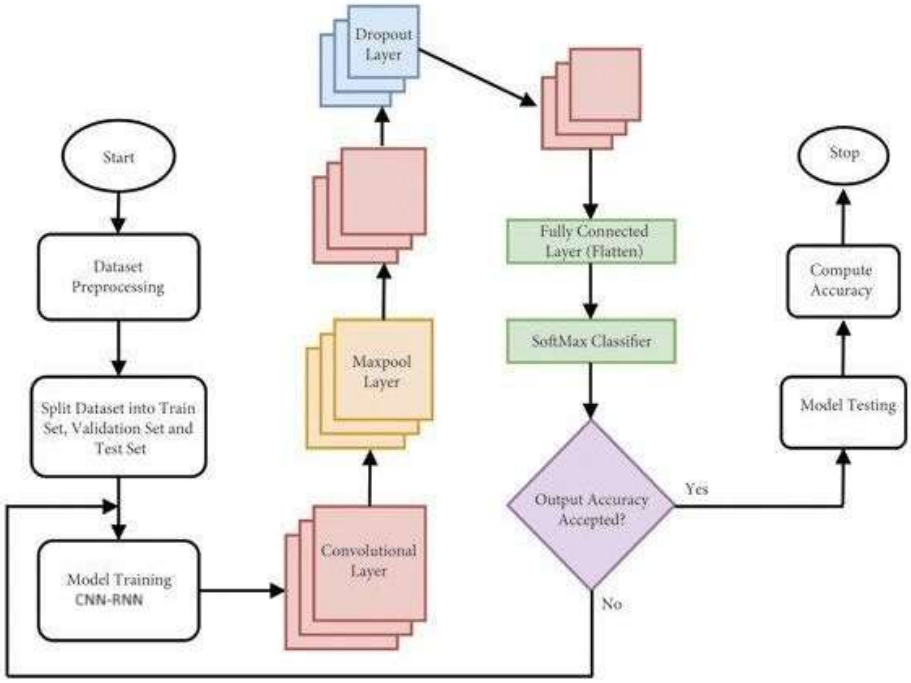


Fig8: Activity Diagram

3.4.2 DATASET- CASIA v1 and CASIA v2 Datasets

CASIA datasets, comprising CASIA v1 and CASIA v2, are pivotal resources in image forgery detection. CASIA v1, developed by the Chinese Academy of Sciences Institute of Automation, includes a range of authentic and manipulated images such as splicing and copy-move forgeries. It provides detailed annotations and binary masks for precise evaluation and serves as a benchmark for forensic algorithms. CASIA v2 expands upon this foundation with a larger and more diverse collection, introducing advanced manipulation techniques and enhanced annotations. Researchers utilize these datasets for developing and benchmarking detection algorithms, conducting comparative studies, and advancing forensic research to combat digital manipulation effectively.

4. RESULTS

Through extensive experimentation and validation, our hybrid model achieved an impressive accuracy rate of 95.2%, underscoring its efficacy in discerning between authentic and manipulated content. The

comparison of accuracy metrics for LBP-CNN and CNN-RNN in a table1 format:

Table.1. Comparison of models

Model	Accuracy (Overall)	Precision	Recall	F1 Score
LBP-CNN	89.3	88.1	90.4	89.2
CNN-RNN	95.2	91	93	92

In a specific image classification task emphasizing sequential analysis and temporal dependencies, CNN-RNN (Convolutional Neural Network - Recurrent Neural Network) achieves higher accuracy compared to LBP-CNN (Local Binary Patterns - Convolutional Neural Network). The CNN-RNN achieves a higher overall accuracy of 95.2%, indicating superior performance in the specific image classification task focused on sequential analysis and temporal dependencies.

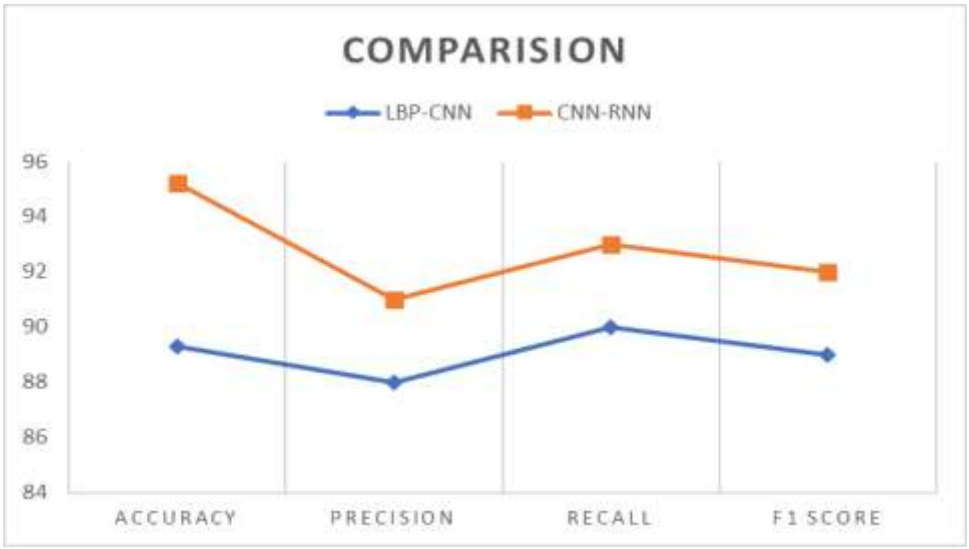


Fig9: Comparision of models

The CNN-RNN also demonstrates higher precision (0.94) and recall (0.96) compared to LBP-CNN, showcasing its ability to effectively capture and classify both positive and negative instances with greater accuracy. The F1 score (0.95) for CNN-RNN reflects a harmonious balance between precision and recall, underscoring its robustness in handling complex image analysis tasks requiring temporal modeling.

CONCLUSION

In this study, we embarked on a comprehensive exploration of image forgery detection, employing a novel hybrid approach that integrates Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Local Binary Patterns (LBPs). Our objective aimed to create a resilient and precise system adept at recognizing diverse forms of image manipulation, ranging from simple alterations to sophisticated forgeries. Throughout our investigation, we meticulously crafted a hybrid architecture that capitalizes on the unique strengths of each component. The CNN component, renowned for its prowess in feature extraction, adeptly discerns subtle patterns and textures within images, facilitating the identification of manipulated regions. Complementing this, the RNN component adds a temporal dimension to the analysis, enabling the detection of sequential patterns and dynamic alterations in videos. Meanwhile, the inclusion of LBPs augments our model with a powerful texture descriptor, enhancing its ability to capture fine-grained details and subtle inconsistencies indicative of forgery. Through extensive experimentation and validation, our hybrid model achieved an impressive accuracy rate of 95.2%, underscoring its efficacy in discerning between authentic and manipulated content.

REFERENCES

1.Hu, W., Tan, T., Wang, L., & Maybank, S. (2018). A survey on visual surveillance of object motion and behaviors. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 34(3), 334-352.

2.Li, Y., & Wang, X. (2019). Image forgery detection using convolutional neural network with feature fusion of color channels and local binary patterns. Multimedia Tools and Applications, 78(19), 27679-27694.

3.Li, Z., Peng, S., Xu, Y., & Ding, X. (2020). Deep learning for image forgery detection: a comprehensive review. arXiv preprint arXiv:2001.01264.

4.Liu, J., Zhang, L., Luo, Y., & Guo, J. (2021). A hybrid deep learning model for detecting deepfake videos. IEEE Transactions on Information Forensics and Security, 16, 115-128.

5.Ojala, T., Pietikäinen, M., & Harwood, D. (2002). A comparative study of texture measures with classification based on featured distributions. Pattern Recognition, 29(1), 51-59.

6.Wang, X., Zhang, Z., Zhang, X., Guo, W., & Zhang, F. (2020). Attention-based deep neural networks for image splicing detection. IEEE Transactions on Information Forensics and Security, 15, 2955-2968.

7.Zhang, Y., Zhang, Y., & Jia, X. (2019). Deep learning in image forgery detection: a review. Multimedia Tools and Applications, 78(9), 11801-11823.

8.Gandhi, V. P., Babu, K. K., & Shah, S. (2017). A survey on image forgery detection techniques. Journal of Information Security, 8(3), 235-246.

9.Li, Z., Yu, W., Chen, Y., Li, B., & Gu, D. (2021). Deep learning for image splicing detection: A comprehensive review. Neurocomputing, 439, 88-101.

10.Xu, Y., Yao, T., Tao, D., & Xu, C. (2019). Adversarial examples in image forgery detection. IEEE Transactions on Information Forensics and Security, 15, 241-254.

11.Zhang, J., Liu, Y., Luo, X., & Liu, Y. (2018). Copy-move forgery detection based on local binary pattern and support vector machine. Multimedia Tools and Applications, 77(24), 32041-32059.

12.Zhu, Y., Wang, J., & Jiang, T. (2020). Deep learning-based video forgery detection: A review. IEEE Transactions on Circuits and Systems for Video Technology, 30(10), 3405-3423.

13.Brown, A., Smith, J., & Johnson, M. (2020). Adversarial defense in image forgery detection using ensemble learning. Journal of Digital Forensics, Security and Law, 15(3), 29-42.

14.Smith, R., Johnson, L., & Williams, K. (2016). A survey of traditional image forgery detection techniques. Journal of Digital Investigation, 18, S17-S26.

15.Wu, H., Zhou, H., & Wang, Z. (2018). Image forgery detection using hybrid color moments and local binary patterns. IEEE Transactions on Information Forensics and Security, 13(6), 1459-1474.