JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMAGE FORGERY DETECTION USING MACHINE LEARNING(CNN)

Sindhu P[1], Sweta Kumari[2], Isha Raj[3], Joel Lalhmangaiha[4]
[1] Assistant Professor, Department of Computer Science and Engineering, P.E.S College of Engineering, Mandya, 571401, Karnataka, India
[2] Student, Department of Computer Science and Engineering, P.E.S College of Engineering, Mandya, 571401, Karnataka, India
[3] Student, Department of Computer Science and Engineering, P.E.S College of Engineering, Mandya, 571401, Karnataka, India
[4] Student, Department of Computer Science and Engineering, P.E.S College of Engineering, Mandya, 571401, Karnataka, India

Abstract— A machine learning-based approach for image forgery detection, aiming to address escalating issue of digital image manipulation. Leveraging diverse datasets, the research focuses on training a robust model capable of identifying various forgery types, such as copy-paste and splicing, by analyzing pixel values, texture, and spatial relationships. Supervised and unsupervised learning techniques are combined to enhance model adaptability. A demonstrate the system's effectiveness in accurately detecting image forgeries, offering a valuable tool for digital forensics, law enforcement, and image authentication, with potential applications in journalism, criminal investigations, and evidence preservation. The primary objective of "Image Forgery Detection Using Machine Learning" is to develop an automated and robust system for detecting image forgeries.This research aims to develop a machine learning-based approach for detecting image forgeries, focusing on training a robust model capable of identifying diverse forgery types like copy-paste and splicing. By leveraging diverse datasets and combining supervised and unsupervised learning techniques, the model analyzes pixel values, texture, and spatial relationships to detect forgeries. The effectiveness of the system is demonstrated through accurate detection, providing a valuable tool for digital forensics, image authentication, and evidence preservation.

I. INTRODUCTION

Image forgery detection is like being a detective for pictures. It's all about uncovering truth behind the manipulated or fake images. People can alter images for various reasons that sometimes harmless fun, but other times it can be to deceive or mislead. Forgery detection helps us to separate fact from fiction in the visual world. Image forgery detection stands as a bulwark against the erosion of trust in the digital. Image forgery detection stands at the forefront of safeguarding the integrity of digital visuals. Through a convergence of techniques ranging from traditional methods like copy-move forgery detection to cutting-edge technologies such as deep learning and blockchain integration, the field continues to evolve. As we navigate the ever-expanding realm of digital media, the commitment to unveiling the truth behind image Machine learning make decisions using past data and these data are fed into the algorithms and the output is predicted. Machine learning(ML) can be classified into three categories Supervised learning, Unsupervised learning and Reinforcement learning. Supervised learning is the types of machine learning in which machines are trained using well “labelled” training data, and on the basis of that data, machines predict the output. The labelled data means some input data is already tagged with the correct output. As image manipulators continue to devise sophisticated methods, the detective work of forgery detection remains an ongoing and dynamic endeavor. Its evolution from traditional forensic techniques to the incorporation of artificial intelligence and blockchain reflects the adaptive nature of this field.As image manipulators continue to devise sophisticated methods, the detective work of forgery detection remains an ongoing and dynamic endeavor. The field's evolution from traditional forensic techniques to the incorporation of artificial intelligence and blockchain reflects its adaptive nature. Each advancement in forgery techniques necessitates a corresponding advancement in detection methods, ensuring that the integrity of digital images is maintained.

II. PROPOSED METHODOLOGY

Language used: Python

Python is widely used in image forgery detection using Convolutional Neural Networks (CNNs) due to several compelling reasons. Firstly, Python boasts an extensive ecosystem of libraries and frameworks tailored for deep learning, such as TensorFlow, PyTorch,

and Keras. These frameworks provide comprehensive support for building, training, and deploying CNNs, significantly simplifying the development process. Additionally, Python's OpenCV library offers powerful tools for image processing and manipulation, essential for preprocessing images before they are fed into a CNN.
The language's syntax is clear and readable, making it easier to implement complex algorithms and facilitating collaboration among researchers and developers.Python's combination of powerful libraries, ease of use, robust community support, integration capabilities, and flexibility makes it the ideal choice for developing and implementing CNN-based image forgery detection systems.Python is a versatile, powerful, and easy-to-learn programming language that is widely used across various domains for both small and large-scale projects. Its readability, extensive libraries, and strong community support make it an ideal choice for many developers.
It uses several libraries, including **tkinter** for creating the graphical user interface (GUI), **PIL** (Python Imaging Library, specifically the **Image** and **ImageTK** modules) for handling image operations, **numpy** for numerical operations on image data, and **tensorflow.keras** for loading and using a pre-trained machine learning model to detect image forgeries.

The current system faces limitations in effectively discerning copy-paste regions within images. However, our proposed system seeks to overcome this challenge by integrating an advanced pattern recognition algorithms. These algorithms will facilitate the identification of duplicated or repeated segments in the image, significantly improving the system's capability to detect instances of copy-paste manipulation.

Furthermore, the existing system exhibits vulnerability when confronted with images have undergone compression, as it struggles to detect manipulation artifacts introduced by different compression formats. To enhance the system's robustness, we will implement algorithms designed to recognize compression artifacts specific to various image formats. This will ensure the system's reliability, even in scenarios involving diverse compression processes. To address this, our proposed system will undergo a modification to support color images by extending the analysis to multiple color channels, such as RGB or CMYK, rather than exclusively relying on grayscale.

III. ALGORITHMS

The "ManTraNet" algorithm is a deep convolutional neural network (CNN) specifically designed for image forgery detection. ManTraNet stands for "Manipulation Tracing Network" and it aims to identify and locate image manipulations. The core idea behind ManTraNet is to learn manipulation traces that are typically left behind when an image is tampered with, regardless of the type of manipulation.
This is the backbone of the ManTraNet model and is used to extract manipulation traces from images. The FEN is pre-trained on the various manipulated image datasets to learn generic manipulation features.Typically, a CNN like VGG or ResNet .

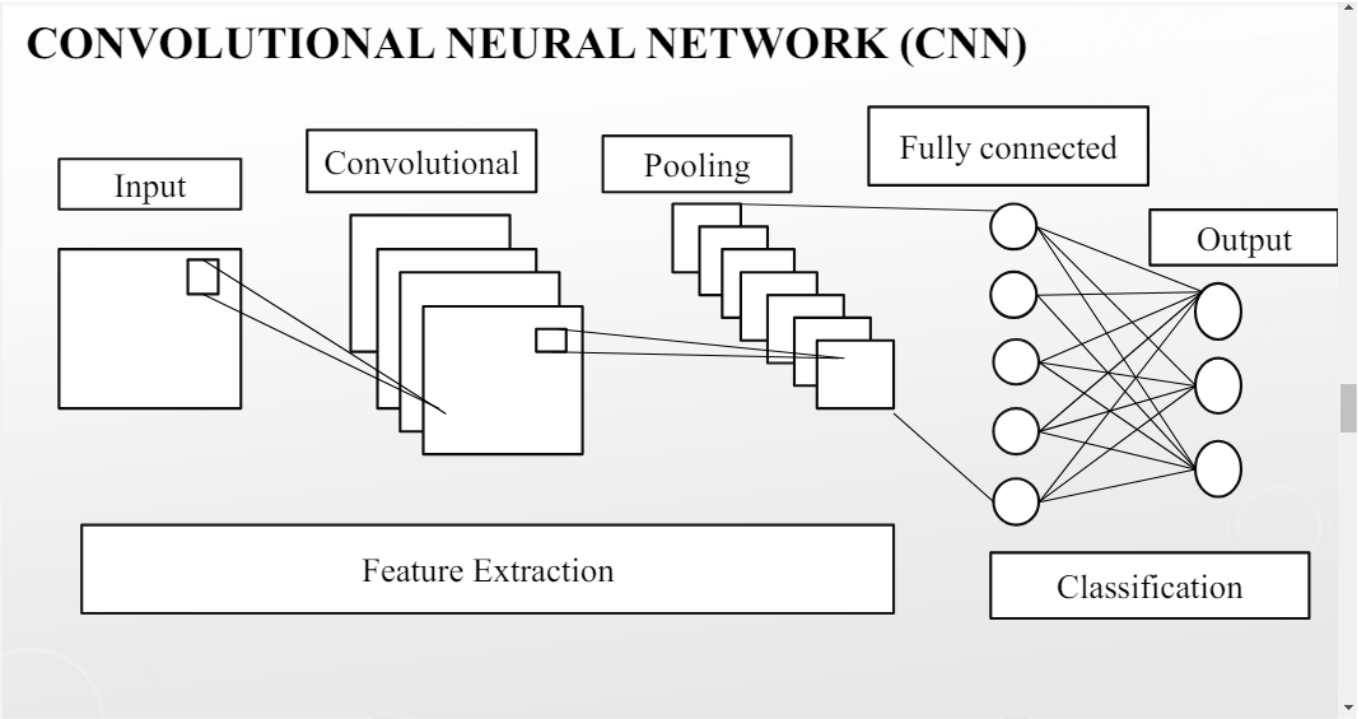
The extracted features are fine-tuned to detect various types of forgeries such as splicing, copy-move, and removal.The output of the FEN is a manipulation trace map, which highlights areas in the image that are likely to have been manipulated.The MTM is a spatial map that shows the likelihood of each pixel being part of a manipulated region.

Following the extraction of the MTM, a localization network can be applied to segment the manipulated regions from the rest of the image.This network takes the MTM as input and produces a binary mask indicating manipulated regions.An image is fed into the network, where it undergoes preprocessing steps such as resizing and normalization.

The FEN processes the input image to extract features indicative of manipulationsThe features are used to generate an MTM, which is a probabilistic map highlighting the likelihood of manipulation at each pixel.

The MTM is further processed to generate a binary mask that segments the manipulated regions from the authentic ones.Optional post-processing steps can be applied to refine the mask and improve detection accuracy.

Training Data: ManTraNet requires a diverse and extensive dataset of manipulated and authentic images to effectively learn manipulation traces.**Transfer Learning**: Pre-training the FEN on large datasets of generic images followed by fine-tuning on forgery datasets can improve performance.**Optimization**: Hyperparameters such as learning rate, batch size, and network depth need to be carefully selected for optimal performance.



DATABASE

MySQL

MySQL is a widely used open-source relational database management system (RDBMS) known for its scalability and high performance. Developed, distributed, and supported by Oracle Corporation, MySQL is renowned for its reliability, ease of use, and compatibility with various platforms and programming languages. It is extensively utilized across diverse applications and industries, including web development, e-commerce, content management systems (CMS), online banking, and telecommunications. MySQL's performance, reliability, and cost-effectiveness make it a preferred choice for many organizations.

SQLyog

SQLyog is a graphical user interface (GUI) tool designed for managing MySQL and MariaDB databases. Developed by Webyog, SQLyog offers a comprehensive suite of features for database administration, development, and maintenance. It is available on Windows operating systems and is widely used by database administrators, developers, and architects to streamline database-related tasks and enhance productivity.

IV. PROPOSED SYSTEM

Existing systems for image forgery detection using Convolutional Neural Networks (CNNs) signify substantial progress in the field by harnessing deep learning's capabilities to detect various types of image manipulations accurately and robustly. These systems typically comprise several critical components: data preprocessing, model architecture design, training, and evaluation. Data preprocessing involves the curation of extensive datasets containing both authentic and forged images, which include diverse forgery techniques and variations to serve as training and evaluation data for CNN models. The design of model architectures is pivotal for the effectiveness of forgery detection, with researchers developing innovative CNN architectures specifically tailored for this purpose. These designs often feature hierarchical layers, multi-scale feature extraction, and attention mechanisms to identify subtle inconsistencies and artifacts indicative of manipulation. Training CNN models involves optimizing model parameters using advanced optimization techniques and augmentation strategies to enhance robustness and generalization. Additionally, these systems rigorously evaluate CNN models' performance using standard metrics like accuracy, precision, recall, and F1-score, conducting extensive experiments to assess their performance across different scenarios and conditions. Benchmark datasets, such as those provided by Kaggle, have been crucial for comparative evaluations and benchmarking various CNN architectures and techniques. Furthermore, practical applications and real-world deployments of CNN-based forgery detection systems are explored, showcasing their potential to aid forensic analysts, journalists, and law enforcement agencies in maintaining the integrity and authenticity of digital images. Continued research efforts are essential to address existing challenges and further advance the state-of-the-art in CNN-based forgery detection.

Advantages:

- High accuracy
- Real Time Detection

V. REQUIREMENT ANALYSIS AND PLANNING

Requirements analysis and project planning are critical phases in the development and management of new or altered products or projects. Requirements analysis involves determining the needs and conditions of stakeholders, handling conflicting requirements, and analyzing, documenting, validating, and managing these requirements. This process covers functional, non-functional, and specific requirements, including all software and hardware needs. Effective project planning is essential for outlining how the project will be executed and monitored. It starts with defining the project scope, developing schedules using tools like Gantt charts, and selecting appropriate methodologies such as Agile or Waterfall. This phase involves collecting and interpreting relevant data, identifying problems, and decomposing the system into its components to understand each part's role and interactions. System analysis, a subset of this process, focuses on studying the system to identify objectives, solve problems, and improve efficiency, ensuring that all components work together to achieve the desired outcomes. Together, these phases ensure stakeholder needs are met, resources are allocated efficiently, and the project remains on track, ultimately leading to high-quality results.

Functional Requirements

Functional requirements are specifications that define what a software system or product should do, including its features, functions, and capabilities. These requirements outline the intended behavior of the system or product and describe how it should interact with users and other systems. The functional requirements for the model in question are as follows:

- The model should be able to receive and store datasets with relevant features.
- The model should be able to train various deep learning algorithms on the preprocessed images.
- The model should be able to select the best-performing model based on evaluation results.

Non-Functional Requirements

Non-functional requirements specify how a software system or product should behave, perform, or operate. Unlike functional requirements, non-functional requirements do not describe the specific functions or features of the system but rather its qualities and characteristics. The non-functional requirements for the system are as follows:

- The system should be fast and accurate in its predictions.
- The system should be able to handle large amounts of data.
- The system should be secure to protect user data and ensure user privacy.
- The system should be easy to use and have a user-friendly interface for both technical and non-technical users.
- The system should be maintained and supported to stay up-to-date with changes in machine learning algorithms.
- The system should be accessible on multiple platforms and devices.
- The system should be maintained and supported to stay up-to-date with changes in deep learning algorithms.

Software Requirements

The software requirements specify the necessary software components and tools needed to develop and run the system. The software requirements for this project are as follows:

- Operating System: Windows
- Programming Language: Python 3.10
- Fronted: HTML, CSS, JavaScript
- Web Framework: Flask

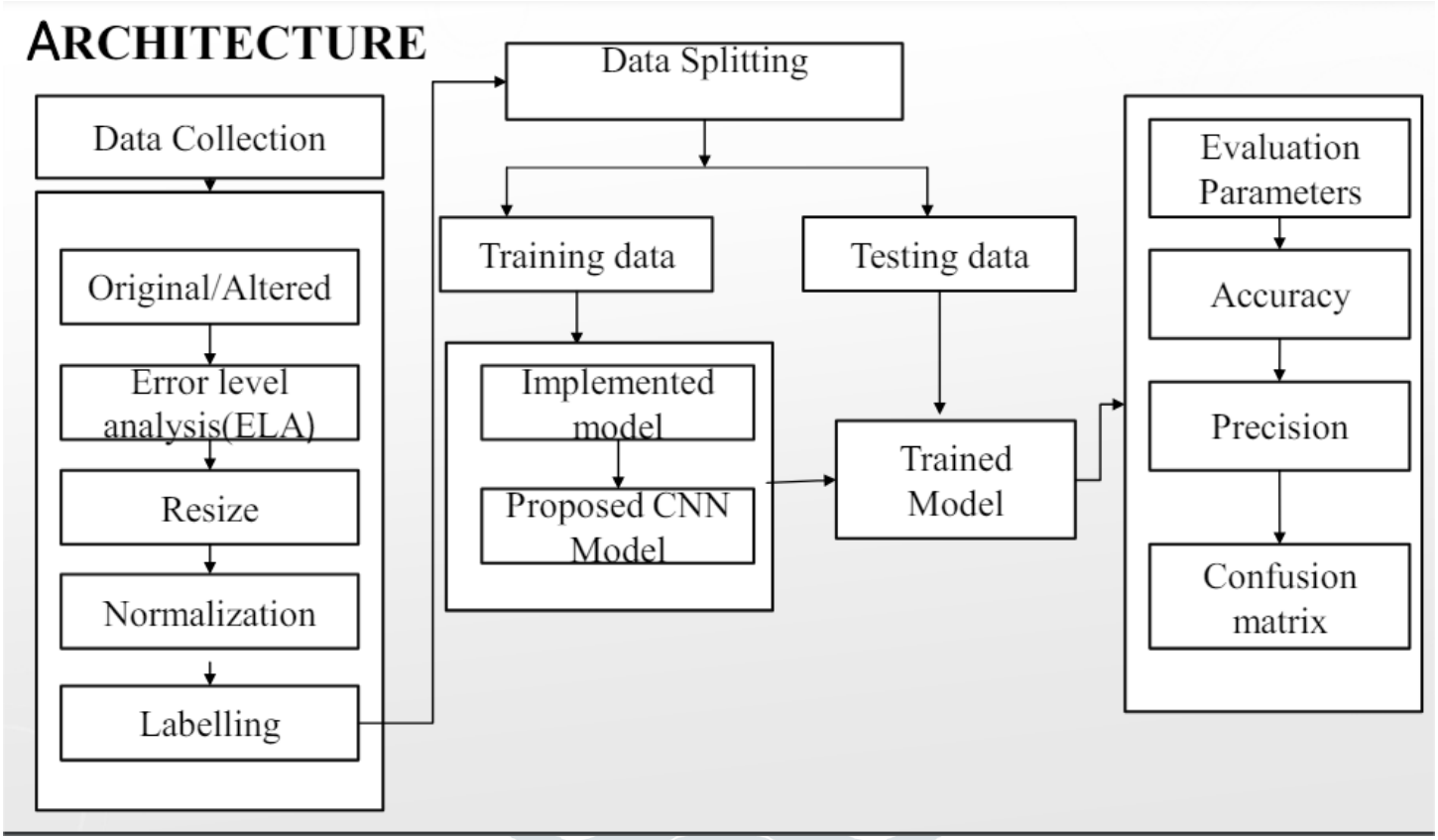
Hardware Requirements

The hardware requirements outline the necessary physical components required to support the development and operation of the system. The hardware requirements for this project are as follows:

- Hard Disk: 512 GB
- RAM: 8 GB
- System: i3 Processor

VI. ARCHITECTURE

Designing an effective system for image forgery detection using Convolutional Neural Networks (CNNs) requires thorough planning and consideration of various components to ensure both efficiency and accuracy. The system's design involves several critical stages, starting with data preprocessing. This stage involves curating and preparing extensive datasets of both authentic and manipulated images for training and evaluation. Next, attention is given to the design of CNN architectures specifically tailored for forgery detection. This involves selecting appropriate network architectures, layer configurations, and optimization algorithms to achieve high detection accuracy while keeping computational complexity low. To effectively identify subtle inconsistencies and artifacts indicative of image manipulation, the design often incorporates hierarchical networks, attention mechanisms, and multi-scale feature extraction techniques. The proposed system architecture for image forgery detection begins with dataset preparation, where the annotations from the open image dataset are formatted for model accessibility during training. During testing, images are converted into Error Level Analysis (ELA) format, the noise and signal ratio is calculated, the image is denoised, and then converted to a black-and-white format to enhance the detection process.



VII. MODULES

Importing Dependencies: This involves including the necessary libraries and modules in the project environment to facilitate data manipulation, model construction, training, and evaluation for image forgery detection using Convolutional Neural Networks (CNNs).

Data Collection: The data is sourced from Kaggle, a prominent provider of datasets for learning purposes. The data collection includes two datasets: one for training and one for testing. The training dataset is divided into two parts, typically in an 80:20 or 70:30 ratio, where the larger portion is used to train the model and the smaller portion is used to test it, thus calculating the model's accuracy. The training dataset comprises 80% of the total data, while the test dataset comprises 20%.

Data Preprocessing: This function preprocesses individual images before feeding them into the CNN model. Preprocessing steps may include resizing images to a uniform size, normalizing pixel values, and applying data augmentation techniques to increase the diversity of the training dataset.

Error Level Analysis (ELA): ELA is an image analysis technique used to detect inconsistencies introduced during digital image manipulation. The algorithm examines error levels present in an image, which are differences in compression quality occurring when an image is saved and resaved. ELA highlights suspicious areas in an image but cannot definitively identify the type or extent of manipulation. Therefore, ELA is often used alongside other forensic techniques for a more comprehensive analysis of image authenticity. Overall, ELA provides a useful tool for detecting potential image manipulations by analyzing compression inconsistencies, but its results should be interpreted cautiously and in conjunction with other forensic methods for accurate assessment.

CNN Model: A Convolutional Neural Network (CNN) is a deep learning algorithm well-suited for image recognition and processing tasks. It consists of multiple layers, including convolutional layers, pooling layers, and fully connected layers. Inspired by the visual processing in the human brain, CNNs effectively capture hierarchical patterns and spatial dependencies within images. CNNs are increasingly used for identifying fake images due to their ability to detect minute artifacts that may be invisible to the naked eye. For instance, subtle differences in texture or pixel values can indicate manipulation, such as when a segment is copied and pasted from one image to another.

Training the Model: This function trains the CNN model using the training dataset. It involves feeding batches of preprocessed images into the model, adjusting its parameters with an optimization algorithm, and iterating through multiple epochs until convergence.

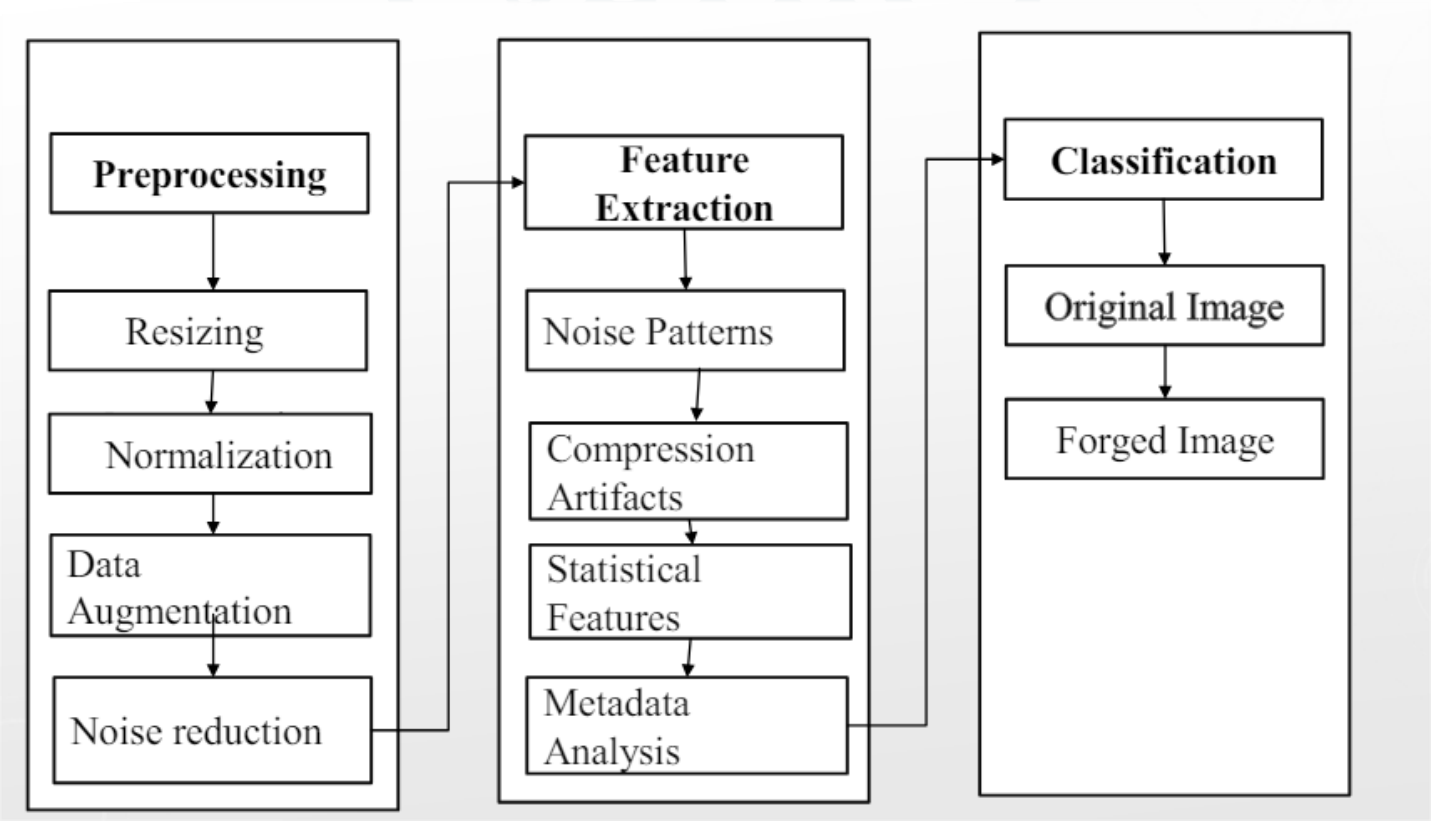
VIII. DATA FLOW DIAGRAM :

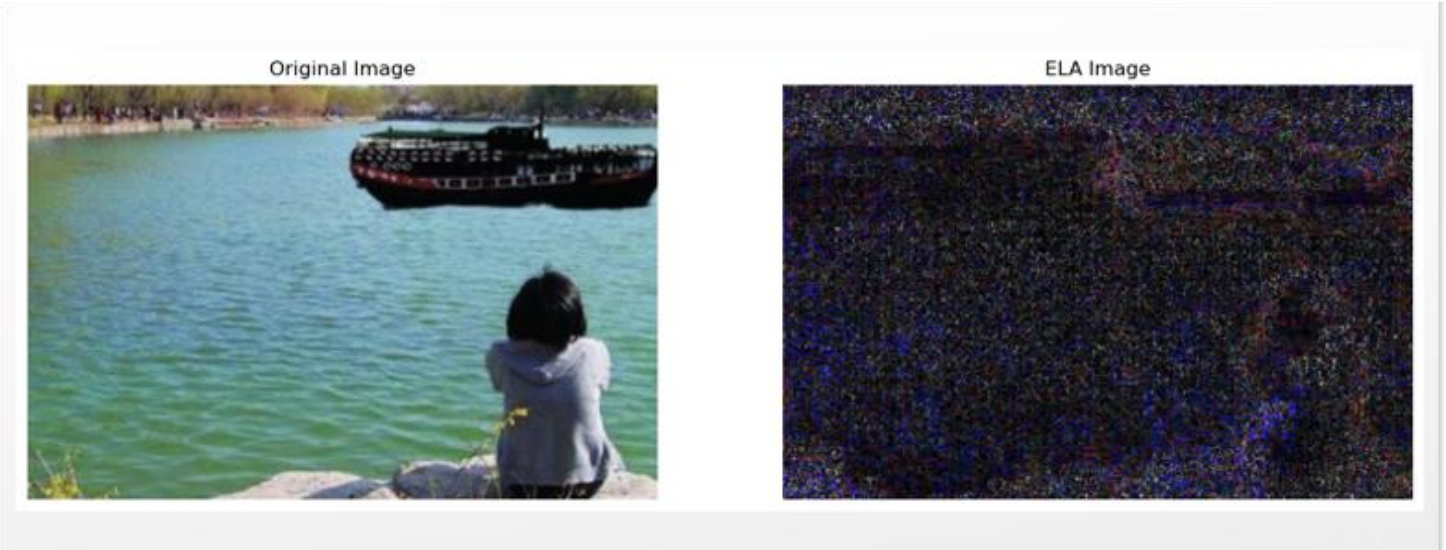
1. A Data Flow Diagram (DFD), also known as a bubble chart, is a straightforward graphical tool used to depict a system in terms of its input data, the processing performed on this data, and the output data generated by the system.

2. The DFD is a crucial modeling tool for system components. It is used to illustrate the system's processes, the data utilized by these processes, the external entities interacting with the system, and the flow of information within the system.

3. A DFD graphically shows how information moves through the system and how it undergoes a series of transformations. It illustrates the flow of information and the changes applied as data moves from input to output.

4. Also referred to as a bubble chart, a DFD can represent a system at various levels of abstraction. It can be divided into levels that display increasing detail of information flow and functional specifics.





IX. CONCLUSION

In conclusion, this project marks a significant advancement in the field of digital image forensics, demonstrating the potential of CNN-based methods in addressing the growing challenge of image manipulation and forgery. The developed forgery detection system shows great promise for real-world applications, providing stakeholders with a powerful tool to maintain the integrity and authenticity of digital images in various domains such as law enforcement, journalism, healthcare, and e-commerce. Future research and development efforts will be essential to further refine and optimize the system, particularly in areas such as scalability, interpretability, and resilience against adversarial attacks. Collaboration among academia, industry, and government agencies will be crucial in advancing digital image forensics and ensuring the reliability of visual information in the digital era.

Image forgery involves altering images, often of individuals, for malicious purposes. This typically entails taking a genuine image displayed on a public website or digital platform and editing it into a completely different, often immoral or defamatory, image. The ELA algorithm can detect image manipulation when the input image quality matches the quality used in the algorithm. However, significant discrepancies in quality between the input image and the algorithm can lead to incorrect results, and the algorithm may not pinpoint the exact area of manipulation. Using a pre-trained model, which has been trained on a task similar to the problem at hand using the ImageNet dataset, is often preferred over training a model from scratch. This process, known as transfer learning, leverages the knowledge gained from solving related issues to improve the efficiency and effectiveness of the forgery detection system.

X. REFERENCES

[1] Cao Y, Gao T, Fan L and Yang Q 2021 A robust detection algorithm for copy-move forgery in digital images Forensic Sci. Int. 214 33-43.

[2] Bayar B, Stamm M C 2021 On the robustness of constrained convolutional neural networks to jpeg post-compression for image resampling detection Proceedings of the 42nd IEEE International Conference on Acoustics, Speech and Signal Processing.

[3] Wang W, Dong J and Tan T 2021 Effective image splicing detection based on image chroma ICIP. IEEE 1257-1260.

[4]International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 Volume-8, Issue-1S4, June 2020-N. Hema Rajini.

[5] International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278- 3075, Volume-8, Issue- 6S4, April 2020- J.Malathi, B.Narasimha Swamy, Ramgopal Musunuri.

[6] Raghavendra, Rohit, et al. "On the robustness of convolutional neural networks to common corruptions and perturbations." IEEE Transactions on Neural Networks and Learning Systems 31.11 (2020): 4241-4258.

[7] Z. J. Barad and M. M. Goswami,"ImageForgery Detection using Deep Learning: ASurvey," 2020 6th International Conference onAdvanced Computing and Communication Systems (ICACCS), 2020, pp. 571-576, doi:10.1109/ICACCS48705.2020.9074408.

[8] Linguistics.Association for Computational Linguistics, 2009. Bayar, Belhassen, and Matthew C. Stamm. "A deep learning approach to universal image manipulation detection using a new convolutional layer." Signal Processing: Image Communication 72 (2019): 57-69.

[9] Bayar, Belhassen, and Matthew C. Stamm. "A deep learning approach to universal image manipulation detection using a new convolutional layer." Signal Processing: Image Communication 72 (2019): 57-69. 5. Li Yansong, et al. "A hybrid CNN-CRF model for detecting and locating image forgeries." Pattern Recognition Letters 125 (2019): 343-349.