RE-2022-424743 - Turnitin Plagiarism Report

by Neha M U

Submission date: 26-Nov-2024 10:07PM (UTC+0530)
Submission ID: 271732659127
File name: RE-2022-424743.pdf (921.43K)
Word count: 6865
Character count: 40794

CHAPTER 1

1.INTRODUCTION

1.1 GENERAL

In today's interconnected world, the exchange of sensitive information has become a critical aspect of both personal and professional communication. With the rise in cyber threats and the increasing volume of data being transmitted online, ensuring the confidentiality and security of such information has never been more important. Traditional methods of securing data, such as encryption, are widely used to safeguard communication; however, these methods often signal the presence of sensitive content, making them vulnerable to detection. In contrast, steganography, the practice of embedding secret information within a seemingly innocuous medium, offers an alternative by concealing the existence of the data itself. This technique allows for secure transmission of information without alerting unintended parties to its presence.

Steganography is most commonly applied to digital media such as images, audio, and video files. By manipulating the data in a way that is imperceptible to the human eye or ear, steganography ensures that the embedded information remains hidden from plain view. Among the various methods of steganography, Least Significant Bit (LSB) and Pixel Value Differencing (PVD) are two widely used techniques for embedding data within images. LSB works by altering the least significant bits of pixel values in an image, which results in minimal changes that do not significantly affect the visual quality of the image. PVD, on the other hand, modifies pixel values in a more structured way, which allows for more data to be embedded while maintaining the image's visual integrity. Despite their effectiveness in concealing information, these methods present unique challenges for detection, as the changes introduced to the image are often too subtle to be identified using conventional techniques.

Traditional methods, including statistical analysis and histogram-based techniques, often fall short when dealing with sophisticated steganographic algorithms like LSB and PVD. The difficulty arises because these methods are designed to make pixel-level changes that are imperceptible to the human eye but still represent hidden information. As a result, detecting stego-images—images that contain hidden messages—requires more advanced techniques capable of identifying these subtle patterns and changes. Deep learning, specifically Convolutional Neural Networks (CNNs), has proven to be highly effective in this domain due to its ability to automatically learn complex patterns from large datasets without needing explicit feature engineering. CNNs have been successfully applied to various image processing tasks, and their potential for steganography detection is immense.

This project aims to develop an advanced deep learning framework to detect stego-images embedded using LSB and PVD techniques. The proposed system leverages the VGG16 CNN architecture, which is pre-trained on large image datasets like ImageNet, enabling it to recognize intricate patterns in images. The model is fine-tuned for the specific task of steganography detection, utilizing a curated dataset of Non-stego, Stego-LSB, and Stego-PVD images. Through this approach, the model learns to distinguish between images with hidden data and those without, based on subtle pixel-level changes introduced by the embedding techniques.

The system developed in this project provides a reliable and efficient solution for detecting stego-images, offering a valuable tool for researchers, cybersecurity professionals, and others in the field of digital forensics. As digital communication continues to evolve, so too must the tools designed to protect sensitive information. By leveraging cutting-edge deep learning techniques, this project aims to contribute to the ongoing effort to improve data security and the detection of covert communication methods.

1.2 OBJECTIVE

1.Develop a Deep Learning-based Steganography Detection System:

To design and implement a deep learning framework using Convolutional Neural Networks (CNN), specifically the VGG16 architecture, to detect stego-images embedded with hidden data using LSB and PVD techniques.

2.Enhance Image Classification Accuracy:

To apply data preprocessing techniques such as resizing, normalization, and data augmentation to improve the generalization capability of the model and ensure high classification accuracy.

3.Provide a Reliable Solution for Steganography Detection:

To develop a robust and efficient system for the detection of stego-images that can be applied in real-time, contributing to enhanced security in digital communication.

4.Utilize Deep Learning for Feature Extraction:

To leverage the VGG16 architecture's pre-trained convolutional layers for extracting complex image features and adapt them for the task of steganography detection.

5.Contribute to Digital Security Research:

To provide valuable insights into the application of deep learning in steganography detection, aiding the advancement of digital forensics and secure communication technologies.

1.3 EXISTING SYSTEM

Steganography detection has evolved through various methods, starting with traditional statistical techniques that analyze image properties like histograms and pixel value distributions. While these methods work for simple steganographic techniques, they are less effective for detecting advanced methods, such as LSB and PVD, that introduce subtle pixel changes. To improve accuracy, transform domain techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) were introduced. These methods examine the frequency components of images, making them more robust to compression and resizing, but still struggle with advanced embedding techniques.

Machine learning-based methods, including classifiers like Support Vector Machines (SVM) and decision trees, have gained popularity. These systems extract features from images before classification, allowing for better performance than traditional approaches. However, they still require manual feature extraction and can be limited when handling complex datasets. In recent years, deep learning methods, especially Convolutional Neural Networks (CNNs), have become the leading approach. CNNs automatically learn features from raw image data, making them highly effective for detecting stego-images, even with sophisticated embedding techniques like LSB and PVD.

Some systems combine multiple detection techniques, such as hybrid approaches that integrate traditional methods with machine learning or deep learning models. These hybrid systems provide more comprehensive solutions for detecting a wider range of steganographic techniques. Despite advances, existing systems continue to face challenges in robustness and generalization, especially with the evolving nature of steganography.

2.4 PROPOSED SYSTEM

The proposed system aims to develop a robust deep learning-based solution for detecting stego-images, which contain hidden data embedded using steganographic techniques such as Least Significant Bit (LSB) and Pixel Value Differencing (PVD). The system leverages the VGG16 Convolutional Neural Network (CNN) architecture, a pre-trained model known for its powerful feature extraction capabilities, to identify subtle pixel-level modifications in images that are characteristic of these steganographic methods.

The system follows a well-defined pipeline for image processing and classification. Initially, a curated dataset consisting of Non-stego, Stego-LSB, and Stego-PVD images is collected and preprocessed. The images are resized to a standard resolution of 224x224 pixels, pixel values are normalized, and data augmentation techniques such as random rotations, flipping, and zooming are applied to increase the diversity of the dataset and improve the model's generalization capabilities. This preprocessing step ensures that the model can handle real-world variations in the images, such as changes in orientation, scale, and brightness, which are crucial for detecting hidden data across diverse conditions.

The VGG16 architecture is fine-tuned for steganography detection by freezing the initial convolutional layers, which are pre-trained on large datasets such as ImageNet, and modifying the fully connected layers for the specific task of classifying stego and non-stego images. A global average pooling layer is introduced to reduce the dimensionality of feature maps, followed by custom dense layers for classification. The final output layer uses softmax activation to categorize the images into three classes: Non-stego, Stego-LSB, and Stego-PVD. This classification process enables the model to not only detect the presence of hidden data but also to differentiate between different embedding techniques used.The system is trained using categorical cross-entropy loss and optimized with the Adam optimizer. Early stopping is employed to prevent

overfitting, ensuring that the model generalizes well to unseen data. Evaluation metrics such as accuracy, precision, recall, F1 score, and confusion matrix analysis are used to assess the model's performance and reliability in detecting stego-images. By evaluating these metrics, the model's ability to correctly identify stego-images and minimize misclassifications is ensured, which is critical for real-time applications in secure communications.

Additionally, the proposed system is designed to be scalable and efficient, offering a reliable solution for steganography detection in real-time applications. The use of the VGG16 architecture, combined with the application of data augmentation and fine-tuning, ensures that the system is not only accurate but also adaptable to a wide variety of steganographic methods. Moreover, the system's lightweight design allows for easy deployment in practical scenarios, where quick detection and classification of stego-images are essential for enhancing data security. The model can be further adapted to detect emerging steganographic techniques by incorporating additional layers or exploring more advanced CNN architectures in the future.

By utilizing deep learning, the proposed system also has the potential to continually improve through retraining on more extensive datasets, allowing it to stay ahead of new steganographic methods. Its capability to detect and classify stego-images accurately can be extended to various fields such as digital forensics, secure communications, and copyright protection. As digital communication becomes more complex, the need for efficient and accurate steganography detection systems grows, and the proposed system aims to address these needs effectively.

.

CHAPTER 2

2. LITERATURE SURVEY

1. The paper End-to-End Trained CNN Encoder-Decoder Networks for Image Steganography by Atique ur Rehman, Rafia Rahim, Shahroz Nadeem, and Sibt ul Hussain presents a deep learning-based encoder-decoder architecture for embedding payload images into cover images. It introduces a novel loss function for joint end-to-end training, achieving high payload capacity with minimal distortion. The method maintains impressive PSNR and SSIM values across datasets like MNIST, CIFAR10, PASCAL-VOC12, and ImageNet. While versatile and robust, the approach requires significant computational resources and may perform variably on unseen datasets, offering scope for future advancements in efficiency and generalizability.

2. The paper Image Steganography: A Review of the Recent Advances by Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, and Ahmed Bouridane explores recent progress in image steganography, particularly focusing on deep learning approaches. It organizes existing techniques into traditional, CNN-based, and GAN-based methods, providing insights into the datasets and evaluation metrics commonly used in the field. The paper outlines key trends, challenges, and future possibilities, serving as a resource for researchers. While it offers an in-depth theoretical perspective, the technical details may be difficult for beginners, and it emphasizes conceptual understanding over practical applications.

3. The paper Robust Invertible Image Steganography (RIIS) by Youmin Xu, Chong Mou, Yujie Hu, Jingfen Xie, and Jian Zhang introduces a novel framework for concealing secret images within a container image while ensuring the hidden content remains invisible and resilient to

distortions such as Gaussian noise, Poisson noise, and JPEG compression. RIIS utilizes conditional normalizing flow to capture high-frequency details and employs distortion-guided modulation to adapt to various distortion levels. The approach achieves strong robustness without compromising on capacity or imperceptibility. However, it is computationally intensive and requires extensive training to optimize performance for different distortion scenarios.

4. The paper A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks (DCGANs) by Donghui Hu, Liang Wang, Wenjie Jiang, Shuli Zheng, and Bin Li proposes an innovative approach to image steganography using DCGANs. Instead of embedding secret information into existing images, this method directly generates carrier images from the encoded secret information, enhancing security by reducing detection risks. The secret data is transformed into a noise vector, which the generator leverages to produce the carrier image. While this approach offers high security against advanced steganalysis methods and ensures accurate extraction of hidden information, it demands extensive neural network training, significant computational resources, and has limited capacity due to the constraints of the noise vector size.

5. The paper SteganoGAN: High Capacity Image Steganography with GANs by Kevin A. Zhang, Alfredo Cuesta-Infante, Lei Xu, and Kalyan Veeramachaneni introduces a method for embedding binary data into images using generative adversarial networks (GANs). SteganoGAN achieves a high payload capacity of 4.4 bits per pixel while maintaining excellent perceptual quality, making the hidden data nearly undetectable by steganalysis tools. The approach is evaluated across various image datasets, with the authors providing an open-source library to enable fair benchmarking. While the method offers substantial advancements in payload capacity and security, it comes with increased complexity due to its reliance on GANs and multiple loss functions, as well as high

computational demands for training and evaluation.

6. The paper CNN-based Adversarial Embedding for Image Steganography (ADV-EMB) by Weixuan Tang, Bin Li, Shunquan Tan, Mauro Barni, and Jiwu Huang proposes a novel steganographic method designed to evade detection by CNN-based steganalyzers. ADV-EMB modifies the costs of adjusting image elements based on the gradients from the target steganalyzer, creating adversarial stego images. Experimental results demonstrate that this approach improves security by increasing the missed detection rates of both adversary-unaware and adversary-aware steganalyzers.

7. The paper Research on Image Steganography Analysis Based on Deep Learning by Ying Zou, Ge Zhang, and Leian Liu introduces a new steganalysis approach that leverages deep learning, specifically Convolutional Neural Networks (CNNs), to improve the detection of hidden information in images. The method enhances steganalysis performance by incorporating global statistical information constraints and utilizing transfer learning to better analyze images with low embedding rates. This approach reduces the dependency on manually crafted features and boosts detection accuracy. However, it comes with challenges, including the complexity of deep learning models, which require substantial computational resources and large datasets for effective training, which may not always be readily available.

8. The paper Coverless Image Steganography: A Survey by Jiaohua Qin, Yuanjing Luo, Xuyu Xiang, Yun Tan, and Huajun Huang presents a detailed review of coverless image steganography, a technique that conceals information in images without altering the cover image. It covers essential frameworks, preprocessing methods, feature extraction techniques, the generation of hash sequences, and mapping relationships. The paper evaluates various existing methods and provides insights into

potential future research areas. While the approach offers enhanced security by not modifying the cover image, it is complex to implement and requires substantial computational resources. Additionally, its capacity for hiding information is more limited compared to traditional methods.

9. The paper CRoSS: Diffusion Model Makes Controllable, Robust, and Secure Image Steganography by Jiwen Yu, Xuanyu Zhang, Youmin Xu, and Jian Zhang presents the CroSS framework, which utilizes diffusion models to improve image steganography. By integrating Stable Diffusion along with tools like LoRAs and ControlNets, CroSS enhances the security, controllability, and robustness of hidden images without the need for additional training. The framework ensures that secret images remain protected, even if the container images are intercepted, while preserving high visual quality and resistance to noise and degradation. Although it provides strong security and flexibility, the method is complex, requiring an advanced understanding of diffusion models and significant computational resources for processing.

10. The paper Detection of Image Steganography Using Deep Learning and Ensemble Classifiers by Mikołaj Płachta, Marek Krzemień, Krzysztof Szczypiorski, and Artur Janicki investigates the detection of steganographically altered JPEG images using a range of machine learning techniques, including both shallow and deep learning models. The study utilizes images from the BOSS database, embedding hidden information through three well-known steganographic algorithms: J-Uniward, nsF5, and UERD. While the paper offers a comprehensive analysis of different algorithms and feature spaces, achieving high detection accuracy for certain methods, it also faces challenges such as variable performance across different algorithms and densities. Additionally, the deep learning approaches used are resource-intensive, and the study mainly focuses on JPEG images and specific steganographic algorithms.

11. The paper Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility by Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, and Pulung Nurtantio Andono proposes an adaptive method for image steganography that utilizes an inverted Least Significant Bit (LSB) substitution technique. The method optimizes the selection of patterns to minimize error during message embedding, significantly improving the imperceptibility of the resulting stego image. By testing various patterns, the approach selects the one with the least error rate for embedding the message. Experimental results show improved Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) values, demonstrating superior image quality and imperceptibility. However, the adaptive pattern selection process can be computationally demanding, and the results may vary depending on the container image and the size of the message being embedded.

12. The paper Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility by Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, and Pulung Nurtantio Andono proposes an adaptive method for image steganography that utilizes an inverted Least Significant Bit (LSB) substitution technique. The method optimizes the selection of patterns to minimize error during message embedding, significantly improving the imperceptibility of the resulting stego image. By testing various patterns, the approach selects the one with the least error rate for embedding the message. Experimental results show improved Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) values, demonstrating superior image quality and imperceptibility. However, the adaptive pattern selection process can be computationally demanding, and the results may vary depending on the container image and the size of the message being embedded.

13. The paper Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility by Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, and Pulung Nurtantio Andono proposes an adaptive method for image steganography that utilizes an inverted Least Significant Bit (LSB) substitution technique. The method optimizes the selection of patterns to minimize error during message embedding, significantly improving the imperceptibility of the resulting stego image. By testing various patterns, the approach selects the one with the least error rate for embedding the message. Experimental results show improved Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) values, demonstrating superior image quality and imperceptibility. However, the adaptive pattern selection process can be computationally demanding, and the results may vary depending on the container image and the size of the message being embedded.

14. Kumar, V. K. S., P. L., and SenthilPandi, S. (2023). "Enhancing Face Mask Detection Using Data Augmentation Techniques," presented at the International Conference on Recent Advances in Science and Engineering Technology (ICRASET). This paper explores the application of data augmentation techniques to improve the performance of face mask detection models. It demonstrates how these techniques can enhance the robustness and accuracy of models by artificially increasing the size and diversity of the training dataset. Through experimentation, the study shows that using data augmentation results in better generalization and higher detection accuracy, especially in real-world scenarios where mask-wearing patterns vary.

15. Kumar, V. K. S., and S. P. S. (2023). "CNN and Edge-Based Segmentation for the Identification of Medicinal Plants," presented at the 5th International Conference on Intelligent Communication Technologies. This paper focuses on combining Convolutional Neural Networks (CNN) with edge-based segmentation techniques to enhance the identification of

medicinal plants. By leveraging the strengths of CNN for feature extraction and edge-based methods for precise plant boundary detection, the study aims to improve the accuracy and efficiency of plant classification systems. The results highlight the potential of this hybrid approach in real-world applications, such as botanical research and medicinal plant identification.

CHAPTER 3

3. SYSTEM DESIGN

3.1 GENERAL

3.1.1 SYSTEM FLOW DIAGRAM

The system flow diagram visually represents the sequence of operations in the image classification process. It starts with the image input stage, where the user uploads an image to be processed. Once the image is uploaded, the preprocessing step begins, involving resizing, normalization, and augmentation to ensure uniformity and improve the model's performance. After preprocessing, the image is passed to the feature extraction stage, where the VGG16 Convolutional Neural Network (CNN) model processes the image to extract relevant features. The extracted features are then passed to the classification module, where the image is classified into one of three categories: Non-stego, Stego-LSB, or Stego-PVD. The result is finally displayed as an output, showing the predicted class along with the confidence score, completing the process.

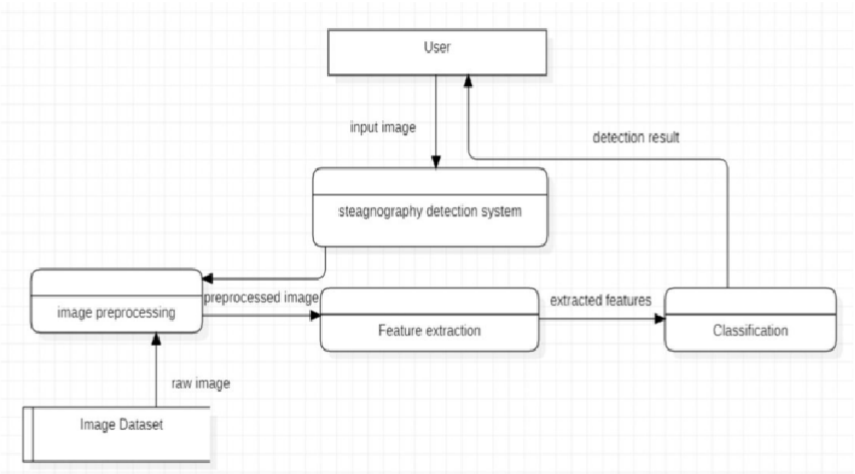

Fig 3.1.1 System Flow Diagram

3.1.2 SEQUENCE DIAGRAM

The sequence diagram illustrates the interaction between the different components of the system over time. The process begins when the user uploads an image to the system. Once the image is received, the system proceeds to the preprocessing stage, where the image is resized, normalized, and augmented. The preprocessed image is then passed to the VGG16 model, which extracts features using its convolutional layers. These features are sent to the classification module, where a decision is made regarding whether the image is Non-stego, Stego-LSB, or Stego-PVD. Finally, the result is returned to the user, showing the predicted class and the model's confidence level. This diagram highlights the flow of control between the user and the system's internal components.

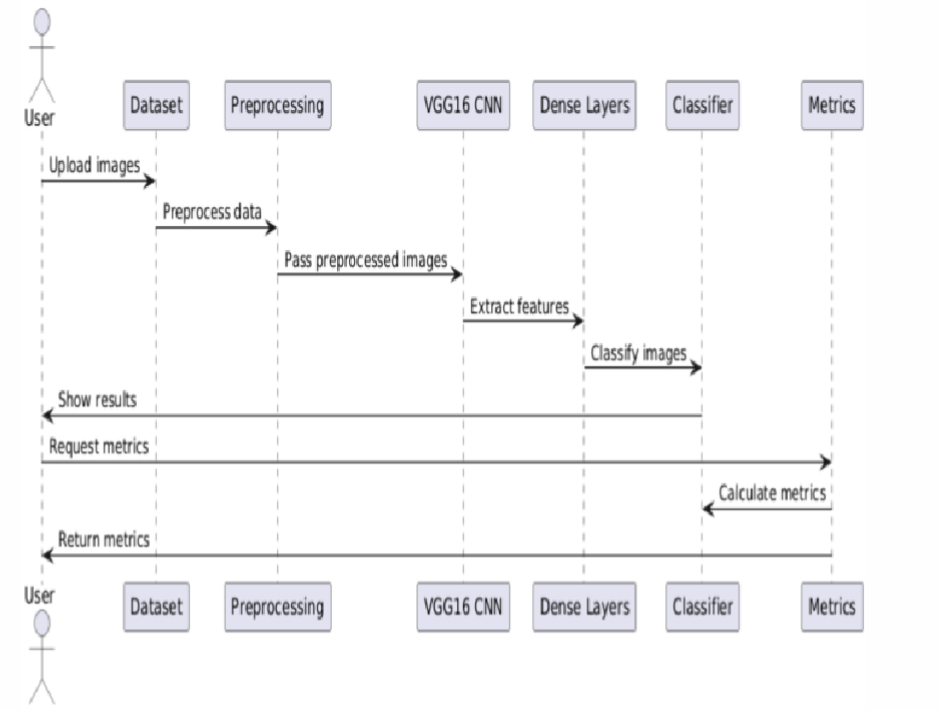

Fig 3.1.2 Sequence Diagram

3.1.3 CLASS DIAGRAM

The class diagram shows the structure of the system, outlining the key classes and their relationships. The primary class, ImageProcessor, is responsible for handling image preprocessing, such as resizing and normalization. The VGG16Model class interacts with the pre-trained VGG16 architecture, fine-tuning it for the specific task of steganography detection. The FeatureExtractor class is tasked with extracting relevant features from the image using the VGG16 model. After feature extraction, the Classifier class categorizes the extracted features into one of three possible classes: Non-stego, Stego-LSB, or Stego-PVD. Finally, the ResultDisplay class is responsible for presenting the classification results and confidence score to the user. The class diagram demonstrates how these classes interact to perform the steganography detection process.

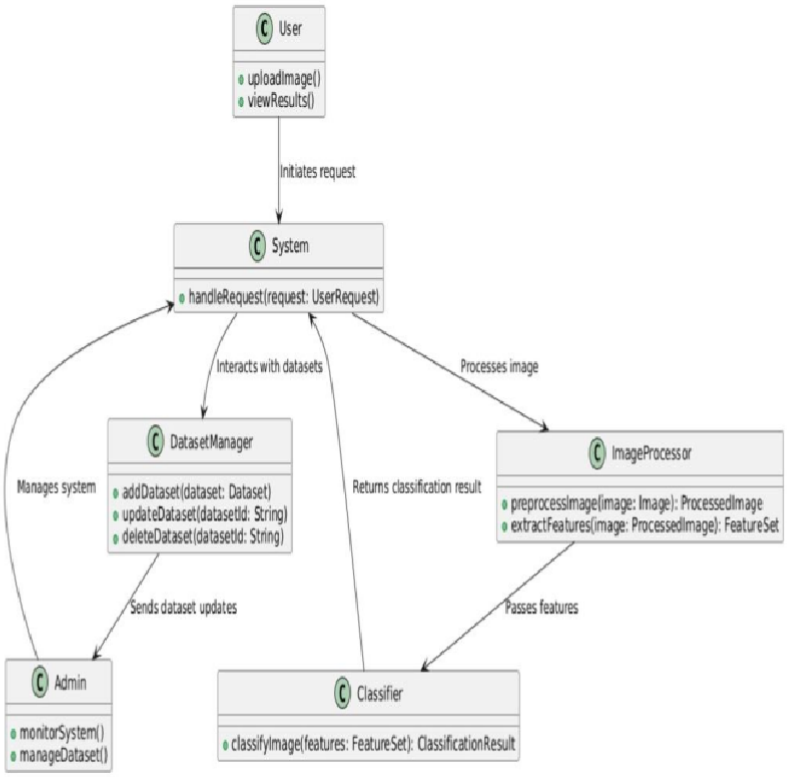

Fig 3.1.3 Class Diagram

3.1.4 USE CASE DIAGRAM

The use case diagram outlines the interactions between the system and its users. The primary actor in this system is the user, who interacts with the system by uploading images and receiving classification results. The use cases include uploading an image, viewing the classification result, and checking the confidence score of the predicted class. The system itself performs the underlying processes of image preprocessing, feature extraction, classification, and result display. The diagram visually represents these interactions, providing an overview of the system's functionality and how users engage with it.

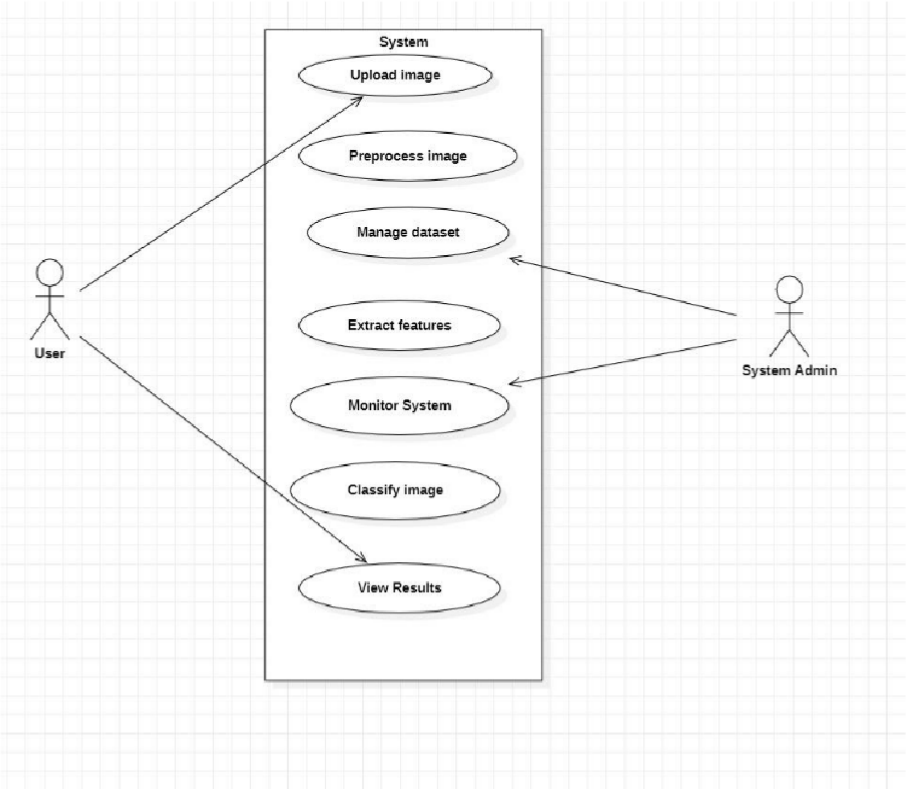

Fig 3.1.4 Use Case Diagram

3.1.5 ARCHIETECTURE DIAGRAM

The architecture diagram provides a high-level view of the system's components and their interactions. At the core of the system is the User Interface (UI), which handles user interactions such as image uploads and displaying results. The Preprocessing Module is responsible for resizing and normalizing the input images to ensure they are in a suitable format for the model. The Feature Extraction Module uses the pre-trained VGG16 CNN to process the image and extract features. These features are then passed to the Classification Module, which classifies the image into one of the three categories. Finally, the Database stores image data or results, if required for future reference. The diagram shows how data flows between these components and how they work together to achieve the system's objectives.

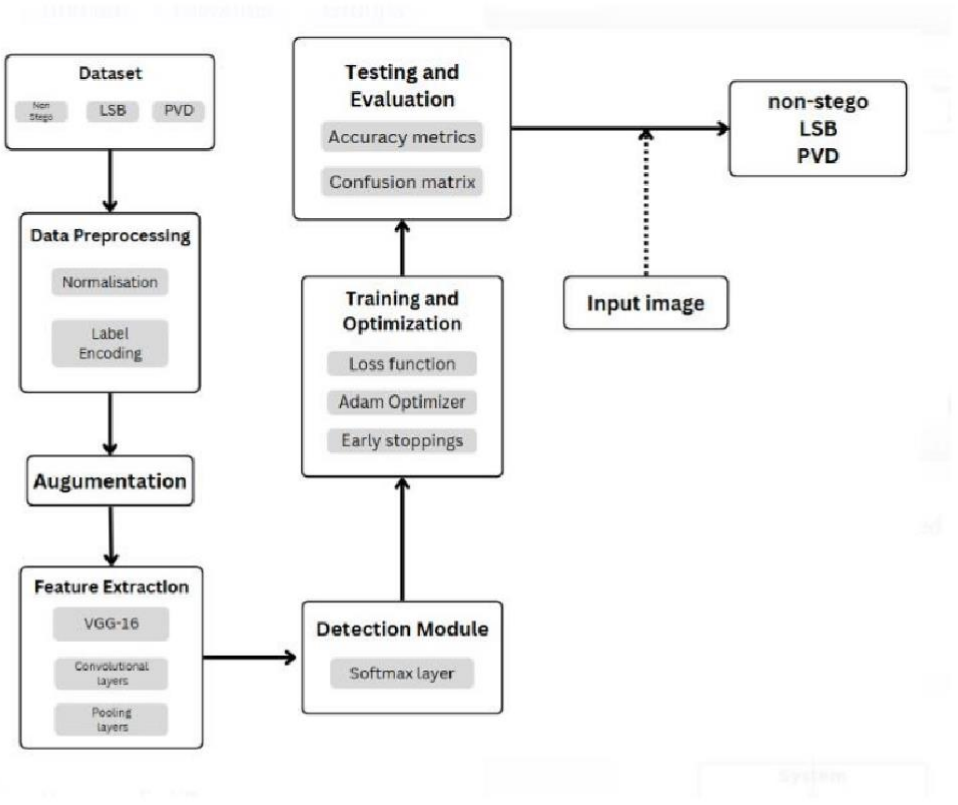

Fig 3.1.5 Architecture Diagram

3.1.6 ACTIVITY DIAGRAM

The activity diagram illustrates the sequence of activities that the system performs, from the beginning to the end of the process. The diagram starts with the image upload, followed by the preprocessing step, where the image is resized, normalized, and augmented. Next, the system performs feature extraction using the VGG16 model. After extracting features, the system proceeds to the classification stage, where the image is categorized as Non-stego, Stego-LSB, or Stego-PVD. The final step involves outputting the classification result along with the confidence score, which is displayed to the user. The activity diagram emphasizes the flow of operations and provides a clear overview of the steps involved in classifying an image.

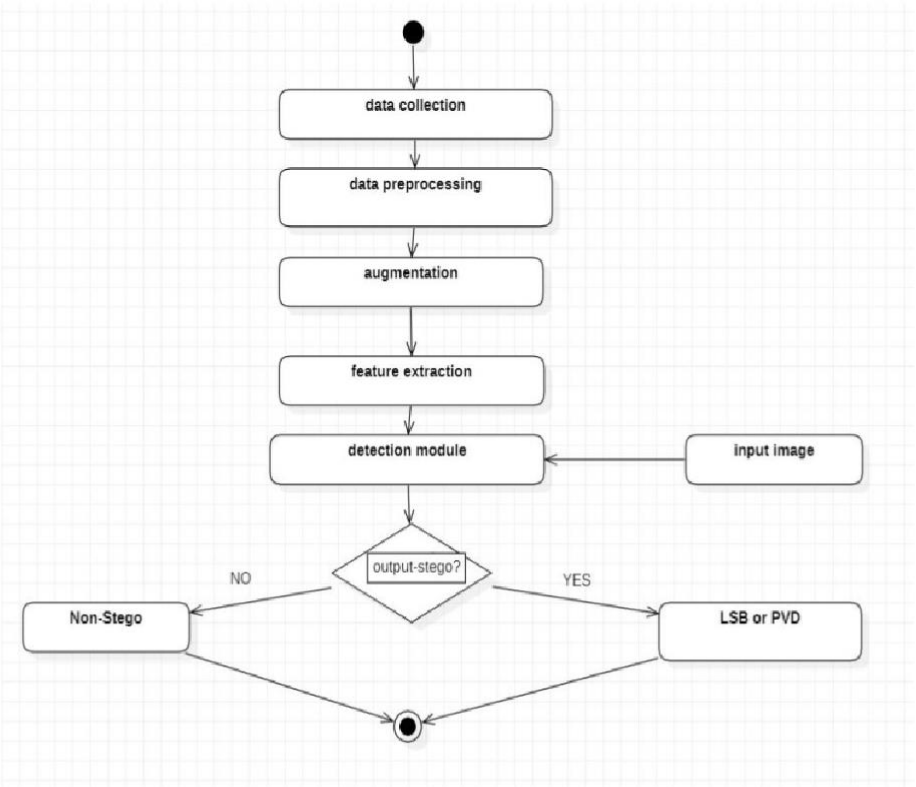

Fig 3.1.6 Activity Diagram

3.1.7 COMPONENT DIAGRAM

The component diagram provides an architectural view of the system's software components and their dependencies. The key components include the User Interface (UI), which manages user input and output, allowing for image uploads and displaying the classification results. The Preprocessing Component is responsible for transforming the image to ensure it is ready for analysis, including resizing, normalization, and data augmentation. The Feature Extraction Component interacts with the VGG16 model to extract important features from the image. The Classification Component then uses these features to classify the image. Lastly, the Output/Display Component presents the classification result to the user. The component diagram shows how these individual components collaborate to provide a seamless user experience.

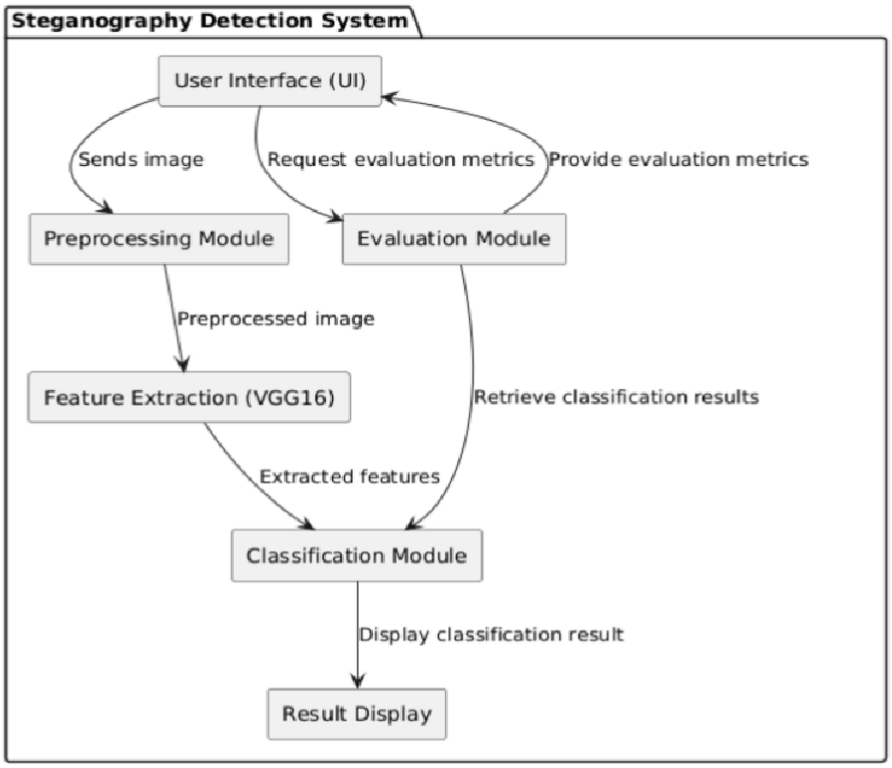

Fig 3.1.7 Component Diagram

3.1.8 COLLABORATION DIAGRAM

The collaboration diagram outlines the interactions between the system's components as they work together to complete a task. The user interacts with the User Interface (UI), which sends the uploaded image to the Preprocessing Component. After preprocessing, the image is forwarded to the Feature Extraction Component, which uses the VGG16 model to extract relevant features. These features are then passed to the Classification Component, which classifies the image into one of the three categories: Non-stego, Stego-LSB, or Stego-PVD. Finally, the classification result is sent back to the User Interface, which displays the output to the user. This diagram emphasizes the communication and flow of information between the system's components, showing how they work together to achieve the desired outcome.

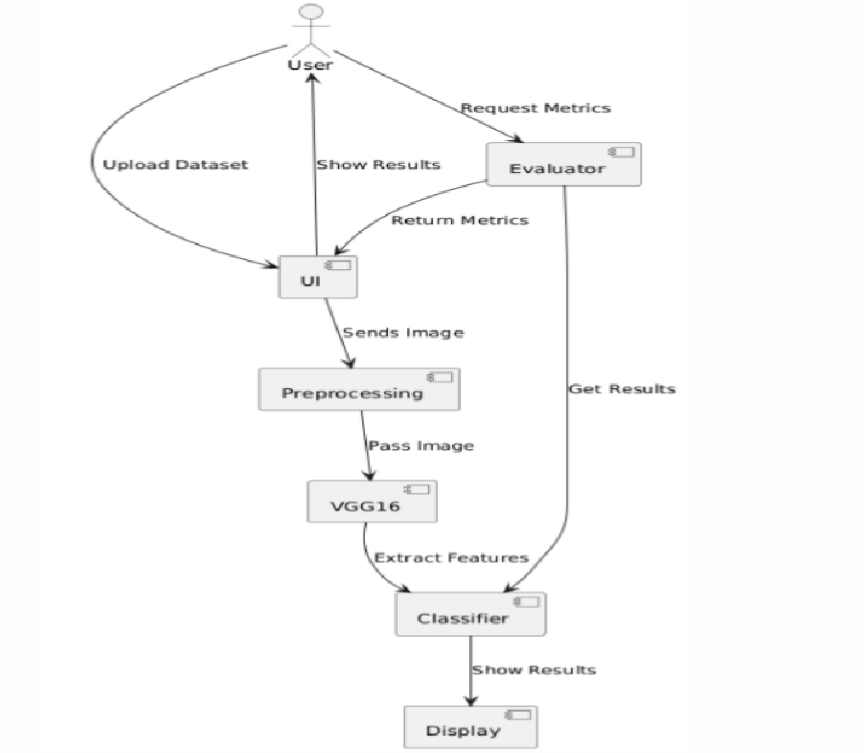

Fig 3.1.8 Collaboration Diagram

CHAPTER 4

PROJECT DESCRIPTION

4.1 METHODOLOGIES:

4.1.1 MODULES:

1. **Data Collection and Preprocessing:**

The dataset for this project is sourced from the BOSSbase dataset, which is widely used for steganography research. The dataset is divided into three categories: Non-stego images (unaltered images), Stego-LSB images (images with hidden data embedded using the Least Significant Bit method), and Stego-PVD images (images altered using Pixel Value Differencing). To standardize the data and ensure uniformity in the model's input, all images are resized to a resolution of 224x224 pixels. Pixel values are then normalized between 0 and 1 to prepare them for efficient model training. Additionally, data augmentation techniques such as random rotations, horizontal and vertical flipping, zooming, and brightness adjustments are applied to the images during training. These augmentations are crucial as they help increase the variability in the dataset, allowing the model to generalize better and reduce the risk of overfitting.

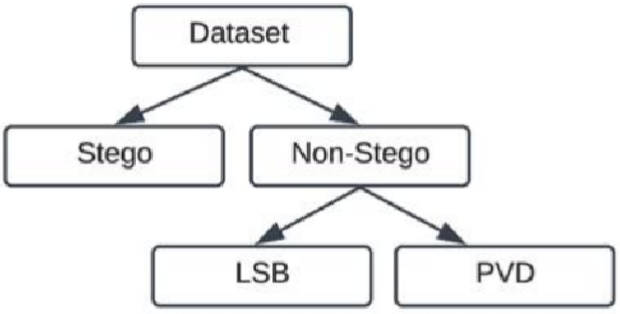

Fig 4.1.1 Dataset Description

2. Feature Extraction:

For feature extraction, the VGG16 Convolutional Neural Network (CNN) architecture is employed, which is known for its deep layers and ability to capture complex patterns within images. The VGG16 model is pre-trained on the ImageNet dataset, enabling it to leverage learned features from a large set of natural images. The initial convolutional layers of the model are frozen, meaning their weights are not updated during training, as they have already been trained on a large, general-purpose dataset. This allows the model to retain valuable low-level feature extraction capabilities, such as edge and texture recognition. The final fully connected layers are replaced with new layers specific to this task, allowing the model to focus on distinguishing stego-images from non-stego images. A global average pooling layer is added after the convolutional layers to reduce the dimensionality of the extracted features, creating a compact and informative feature vector that reduces computational overhead.

3. Classification:

The classification module is designed to categorize images into one of three classes: Non-stego, Stego-LSB, and Stego-PVD. After the feature extraction process, the compact feature vector is passed through custom dense layers that are designed to process the features and perform the classification task. The dense layers help refine the extracted features by learning more abstract representations that can effectively distinguish between the different categories. The final output layer is a softmax layer, which generates probabilities for each of the three classes. The image is classified according to the class with the highest probability score. This approach allows the model to make confident decisions based on the likelihood of each class, ensuring reliable classification of images.

4. Data Collection and Preprocessing:

To train the model, the categorical cross-entropy loss function is used, as this is appropriate for multi-class classification tasks. The Adam optimizer is employed for its efficiency in adapting the learning rate during training, which

helps the model converge more quickly and effectively. Training is performed in batches over multiple epochs, and early stopping is applied to monitor the validation performance. If the validation loss begins to plateau or increase, the training stops to prevent overfitting. This technique ensures that the model learns in a controlled manner, preventing it from memorizing the training data and enabling it to generalize to unseen images. Checkpoints are saved during training to ensure that the best model, in terms of performance on the validation set, is used for evaluation.

5. Model Evaluation:

After training, the model's performance is evaluated using metrics such as accuracy, precision, recall, F1-score, and the confusion matrix. The confusion matrix is used to identify misclassifications between different types of stego-images. Once evaluated, the model is deployed for real-time classification, where incoming images are preprocessed and classified as Non-stego, Stego-LSB, or Stego-PVD. The system outputs the predicted class and confidence score, providing an efficient solution for detecting hidden data.

CHAPTER 5

5.1 CONCLUSION

In this project, a robust deep learning-based system has been developed to detect stego-images containing hidden data embedded using LSB and PVD techniques. Leveraging the VGG16 Convolutional Neural Network (CNN) architecture, the system effectively extracts intricate features from images and classifies them into Non-stego, Stego-LSB, and Stego-PVD categories. Through extensive data preprocessing, augmentation, and fine-tuning of the pre-trained VGG16 model, the system demonstrated strong generalization capabilities across diverse image datasets, ensuring high accuracy and reliability.

The system's performance was validated using evaluation metrics such as accuracy, precision, recall, and F1-score, which confirmed its effectiveness in identifying stego-images and distinguishing between embedding techniques. Insights gained from confusion matrix analysis highlighted opportunities for refinement, particularly in addressing challenges posed by closely related steganographic methods like LSB and PVD.

Overall, this project presents a scalable and reliable solution for steganography detection, contributing significantly to the field of data security by providing an efficient means of identifying hidden information in digital images. Future enhancements could include expanding the dataset to incorporate a wider range of steganographic techniques and integrating advanced deep learning architectures to further improve detection accuracy and adaptability.

5.2 WORK FOR PHASE II

The next steps in this project will involve the development and integration of the Extraction and Embedding Modules to enhance the overall functionality of the steganography system. This will include refining the autoencoder for the Extraction Module to ensure accurate recovery of hidden messages from detected stego-images, while also optimizing the Generative Adversarial Network (GAN)

for the Embedding Module to achieve effective and secure embedding of secret messages into cover images. By balancing data concealment with visual fidelity, the goal is to create a robust system that supports safe digital communication and improves the integrity of embedded data.

1. REFERENCES

1. Rehman, A. U., Rahim, R., Nadeem, S., & Hussain, S. U. End-to-End Trained CNN Encoder-Decoder Networks for Image Steganography.
2. Tao, J., Li, S., Zhang, X., & Wang, Z. Towards Robust Image Steganography.
3. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. Image Steganography: A Review of the Recent Advances.
4. Xu, Y., Mou, C., Hu, Y., Xie, J., & Zhang, J. Robust Invertible Image Steganography.
5. Lu, S. P., Wang, R., Zhong, T., & Rosin, P. L. Large-capacity Image Steganography Based on Invertible Neural Networks.
6. Hu, D., Wang, L., Jiang, W., Zheng, S., & Li, B. A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks.
7. Rustad, S., Rosal, I. M., Setiadi, A. S., & Andono, P. N. Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility.
8. Pramanik, S., & Raja, S. S. A Secured Image Steganography Using Genetic Algorithm.
9. Sahil, V. K., Sharma, S., & Sahu, A. K. Latest Trends in Deep Learning Techniques for Image Steganography.
10. Shah, P. D., & Bichkar, R. S. Secret Data Modification Based Image Steganography Technique Using Genetic Algorithm Having a Flexible Chromosome Structure.
11. Shyla, M. K., Kumar, K. B. S., & Das, R. K. Image Steganography Using Genetic Algorithm for Cover Image Selection and Embedding.
12. Qin, J., Wang, J., Tan, Y., Huang, H., Xiang, X., & He, Z. Coverless Image

Steganography Based on Generative Adversarial Network.

13. Płachta, M., Krzemień, M., Szczypiorski, K., & Janicki, A. Detection of Image Steganography Using Deep Learning and Ensemble Classifiers.
14. Yu, J., Zhang, X., Xu, Y., & Zhang, J. CRoSS: Diffusion Model Makes Controllable Robust and Secure Image Steganography.
15. Hernández, A. M. A., Alazab, M., Jung, J., & Camacho, D. Evolving Generative Adversarial Networks to Improve Image Steganography.
16. Płachta, M., Krzemień, M., Szczypiorski, K., & Janicki, A. Detection of Image Steganography Using Deep Learning and Ensemble Classifiers.
17. Zhang, K. A., Cuesta-Infante, A., Xu, L., & Veeramachaneni, K. SteganoGAN: High Capacity Image Steganography with GANs.
18. Tang, W., Li, B., Tan, S., Barni, M., & Huang, J. CNN-based Adversarial Embedding for Image Steganography.
19. Kumar P, V. K. S, P. L and S. SenthilPandi, "Enhancing Face Mask Detection Using Data Augmentation Techniques," International Conference on Recent Advances in Science and Engineering Technology (ICRASET), B G NAGARA, India, 2023, pp. 1-5, doi: 10.1109/ICRASET59632.2023.10420361
20. Kumar P, V. K. S and S. P. S, "CNN and Edge-Based Segmentation for the Identification of Medicinal Plants," 5th International Conference on Intelligent Communication Technologies.

RE-2022-424743-plag-report

ORIGINALITY REPORT

16%	12%	5%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Illinois at Urbana-Champaign Student Paper	5%
2	www.semanticscholar.org Internet Source	1%
3	arxiv.org Internet Source	1%
4	researchr.org Internet Source	1%
5	www.researchgate.net Internet Source	1%
6	scholarspace.library.gwu.edu Internet Source	1%
7	Uzair Aslam Bhatti, Jingbing Li, Mengxing Huang, Sibghat Ullah Bazai, Muhammad Aamir. "Deep Learning for Multimedia Processing Applications - Volume Two: Signal Processing and Pattern Recognition", CRC Press, 2024 Publication	1%

8	V. Sharmila, S. Kannadhasan, A. Rajiv Kannan, P. Sivakumar, V. Vennila. "Challenges in Information, Communication and Computing Technology", CRC Press, 2024 Publication	1%
9	repository.ju.edu.et Internet Source	1%
10	Submitted to Deakin University Student Paper	1%
11	Submitted to Higher Education Commission Pakistan Student Paper	1%
12	www.aiproblog.com Internet Source	1%
13	www.mdpi.com Internet Source	1%
14	ebin.pub Internet Source	<1%
15	dokumen.pub Internet Source	<1%
16	"Proceedings of Trends in Electronics and Health Informatics", Springer Science and Business Media LLC, 2025 Publication	<1%
17	www.science.gov Internet Source	<1%

18	"Computer Vision and Image Processing", Springer Science and Business Media LLC, 2020 Publication	<1%
19	Submitted to University of Hull Student Paper	<1%
20	huggingface.co Internet Source	<1%
21	Submitted to City University Student Paper	<1%
22	www.slideshare.net Internet Source	<1%
23	Submitted to University of Strathclyde Student Paper	<1%
24	thecleverprogrammer.com Internet Source	<1%
25	Submitted to Colorado State University, Global Campus Student Paper	<1%
26	Submitted to Coventry University Student Paper	<1%
27	Submitted to Indian Institute of Technology Student Paper	<1%
28	Submitted to Rivier University Student Paper	<1%

29	www.frontiersin.org Internet Source	<1%
30	Submitted to City University of Hong Kong Student Paper	<1%
31	www.ijmtst.com Internet Source	<1%
32	xuanyuzhang21.github.io Internet Source	<1%
33	Submitted to Harrisburg University of Science and Technology Student Paper	<1%
34	Submitted to King's College Student Paper	<1%
35	www.coursehero.com Internet Source	<1%
36	dev.to Internet Source	<1%
37	tijer.org Internet Source	<1%
38	www.scilit.net Internet Source	<1%
39	"Human-Centric Smart Computing", Springer Science and Business Media LLC, 2024 Publication	<1%

40	Submitted to Kingston University Student Paper	<1%
41	Mehdi Ghayoumi. "Generative Adversarial Networks in Practice", CRC Press, 2023 Publication	<1%
42	Submitted to Staffordshire University Student Paper	<1%
43	Youmin Xu, Chong Mou, Yujie Hu, Jingfen Xie, Jian Zhang. "Robust Invertible Image Steganography", 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2022 Publication	<1%
44	www.ijert.org Internet Source	<1%
45	"Frontier Computing", Springer Science and Business Media LLC, 2020 Publication	<1%
46	Mikołaj Płachta, Marek Krzemień, Krzysztof Szczypiorski, Artur Janicki. "Detection of Image Steganography Using Deep Learning and Ensemble Classifiers", Electronics, 2022 Publication	<1%
47	Submitted to University of Cape Town Student Paper	<1%
48	jianzhang.tech	