ResNet50-Powered Image Classification for Identifying Counterfeit Products Using Visual Feature Extraction

PROJECT REPORT

Submitted by

PREM KUMAR R [RA2111003010490]
ARJUN ADHITHYA E [RA2111003010583]

Under the Guidance of

Dr Akilandeswari P

(Associate professor, Department of computing technologies)

In partialful fillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE ENGINEERING

DEPARTMENT OF COMPUTING TECHNOLOGIES
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR-603203

MAY 2025

Department of Computing Technologies
SRM Institute of Science & Technology
Own Work* Declaration Form

This sheet must be filled in (each box ticked to show that the condition has been met). It must be signed and dated along with your student registration number and included with all assignments you submit –work will not be marked unless this is done.
To be completed by the student for all assessments

Degree/ Course : B.tech in Computer Science Engineering

Student Name : Prem Kumar R , Arjun Adhithya E

Registration Number : RA2111003010490 , RA2111003010583

Title of Work : ResNet50-Powered Image Classification for Identifying Counterfeit Products Using Visual Feature Extraction

We hereby certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism , as listed in the University Website, Regulations, and the Education Committee guidelines.

We confirm that all the work contained in this assessment is our own except where indicated, indicated, and that We have met the following conditions:

- Clearly referenced / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web, etc)
- Given the sources of all pictures, data etc. that are not my own
- Not made any use of the report(s) or essay(s) of any other student(s) either past or present
- Acknowledged in appropriate places any help that we have received from others (e.g. fellow students, technicians, statisticians, external sources)
- Compiled with any other plagiarism criteria specified in the Course handbook / University website

We understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

DECLARATION:
We are aware of and understand the University's policy on Academic misconduct and plagiarism and we certify that this assessment is our own work, except where indicated by referring, and that we have followed the good academic practices noted above.
Prem Kumar R (RA2111003010490) **Arjun Adhithya E(RA2111003010583)**

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that 18CSP109L- Major Project report titled "**ResNet50-Powered Image Classification for Identifying Counterfeit Products Using Visual Feature Extraction**" is the bonafide work of " **PREM KUMAR [RA2111003010490], ARJUN ADHITHYA [RA2111003010583] "** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Dr AKILANDESWARI P

SUPERVISOR
ASSOCIATE PROFESSOR
DEPARTMENT OF
COMPUTING TECHNOLOGIES

SIGNATURE

Dr. G. NIRANJANA

PROFESSOR & HEAD
DEPARTMENT OF
COMPUTING TECHNOLOGIES

Examiner 1

Examiner 2

ACKNOWLEDGEMENTS

We express our humble gratitude to **Dr. C. Muthamizhchelvan**, Vice-Chancellor, SRM Institute of Science and Technology, for the facilities extended for the project work and his continued support.

We extend our sincere thanks to **Dr.Leenus Jesu Martin M ,** Dean-CET, SRM Institute of Science and Technology, for his invaluable support.

We wish to thank **Dr. Revathi Venkataraman** , Professor and Chairperson, School of Computing Technologies, SRM Institute of Science and Technology, for her support throughout the project work.

We encompass our sincere thanks to , **Dr. M. Pushpalatha** , Professor and Associate Chairperson, School of Computing and **, Dr. C. Lakshmi** Professor and Associate Chairperson, School of Computing Technologies , SRM Institute of Science and Technology, for their invaluable support.

We are incredibly grateful to our Head of the Department, **Dr. G. Niranjana** , Professor, Department of Computing Technologies , SRM Institute of Science and Technology, for her suggestions and encouragement at all the stages of the project work.

We want to convey our thanks to our Project Panel Head **Dr. Akilandeshwari P** and Panel Members **Dr. Ramaprabha J, Dr. Ashwini S**, Department of Computing Technologies , SRM Institute of Science and Technology, for their inputs during the project reviews and support.

We register our immeasurable thanks to our Faculty Advisor **Mrs.Vathana D , Mrs .Nithyakani P** , Department of Computing Technologies , SRM Institute of Science and Technology, for leading and helping us to complete our course.

Our inexpressible respect and thanks to our guide **Dr. Akilandeshwari P** , Associate Professor Department of Computing Technologies , SRM Institute of Science and Technology, for providing us with an opportunity to pursue our project under her mentorship. She provided us with the freedom and support to explore the research topics of our interest. His / Her passion for solving problems and making a difference in the world has always been inspiring.

We sincerely thank all the staff and students of Computing Technologies , School of Computing Technologies , S.R.M Institute of Science and Technology, for their help during our project. Finally, we would like to thank our parents, family members, and friends for their unconditional love, constant support and encouragement.

PREM KUMAR R [RA211100301083]
ARJUN ADHITHYA E [RA2111003010583]

ABSTRACT

Counterfeiting poses a major threat to retail, e-commerce, and brand protection companies resulting in financial loss and damage to reputation. The existing technology to detect counterfeiting relies to a large extent on manual inspection, which is time-consuming and susceptible to human error. The paper presents a machine learning-based counterfeit detection system with image inspection to determine if a product is original or counterfeit. The system is implemented with ResNet50 CNN architecture and optimized for the requirement of higher classification accuracy. With an available set of training data from a set of labeled product images, the model achieves high classification accuracy of 98% and precision and recall of 96% and 97%, respectively. Data preprocessing methodologies like normalization and data augmentation enhance the model generality, while optimization strategies like adaptive learning rate adjustment and dropout layers improve model performance. The proposed system is a scalable, automated counterfeit detection system with minimal human intervention and enhanced efficiency. Experimental results confirm that the model generalizes to a diverse set of counterfeit product classes and is hence viable for use in real-world systems. Additionally, integrating the application of explainable AI techniques can enhance transparency and confidence in the model's output. Interoperability with partners in the business and government spaces will help further optimize model robustness and enable industry adoption. Development of computer vision and deep learning technologies will continue to ensure counterfeiting detection systems keep up with new fraudulent methods that keep evolving continuously. Future research areas include enhancing dataset diversity, testing new deep architectures, and developing the system as a cloud-based API for real-time detection.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Counterfeiting is a common issue for companies such as retail, e-commerce, pharmaceutical, and luxury, leading to huge monetary losses, damage to reputation, and even health risks to consumers. Traditional approaches to counterfeit identification include human inspection, expert examination, and physical security features such as holograms and barcodes. These are slow, expensive, and imprecise. Advances in artificial intelligence (AI) and deep learning, particularly computer vision, have enabled computerized systems of counterfeiting identification that are able to read images of products and identify them as genuine or fake.

This report presents the design and development of a machine learning-based counterfeiting detection system using a ResNet50 convolutional neural network (CNN) architecture. The proposed system uses image analysis techniques such as feature extraction, data augmentation, and classification to improve the accuracy and reliability of detection. The model attains 98% accuracy and high precision and recall scores, realizing robust performance in the detection of counterfeit products from various categories. Having such a system in the business process will be able to offer an efficient and scalable solution to businesses and regulatory bodies with the aim of preventing and deterring counterfeiting as well as safeguarding consumers.

Moreover, the application of deep learning in detecting counterfeiting can reduce the need for manual authentication, accelerate decision-making processes, and enhance the security level in supply chains and e-commerce platforms. The application of AI-driven counterfeit detection tools can benefit businesses by curbing fraudulent activities, safeguarding brand reputation, and maintaining consumer confidence. This report provides an extensive analysis of the system's methodology, performance analysis, and potential applications, as well as future development and deployment suggestions.

1.1 Background and Significance

Counterfeiting is a gigantic global issue, and the International Chamber of Commerce has estimated the global economic cost of counterfeiting to be over $2.3 trillion per year. The problem occurs across a number of sectors such as luxury items, medicines, electronics, and consumer products. Traditional methods of counterfeiting identification are based mainly on visual inspection by expert labor, which is time-consuming, subjective, and powerless-against-sophisticated-counterfeits.

The advent of computer vision and Dee Counterfeiting is a gigantic global issue, and the International Chamber of Commerce has estimated the global economic cost of counterfeiting to be over $2.3 trillion per year. The problem occurs across a number of sectors such as luxury items, medicines, electronics, and consumer products. Traditional methods of counterfeiting identification are based mainly on visual inspection by expert labor, which is time-consuming, subjective, and powerless against sophisticated counterfeits. Learning technology presents intriguing new options to improve counterfeit detection by more accurate and efficient automatic methods. This work meets this opportunity by demonstrating an optimized state-of-the-art neural network structure for leveraging subtle visual differences between authentic and counterfeit items.

The importance of this study is in its future application in multiple industries. For instance, online stores can adopt AI-based counterfeit prevention systems to guard against counterfeit listings, which protects brands as well as consumers. Supply chain management can also use automated authentication methods to validate the authenticity of products at multiple distribution points. Such systems can be used by regulation bodies to check counterfeit trade and intellectual property infringement more successfully.

Moreover, illegal pharmaceuticals have a serious impact on public health, and detection using AI tools is crucial in maintaining the quality of medical drugs. By countering the disadvantage of conventional approaches to detecting counterfeit goods, the project helps the world develop an effective, large-scale, and automated solution for preventing counterfeiting in many industries.

1.2 Motivation

Counterfeiting poses serious economic, social, and security consequences on business, industry, and consumers globally. Having counterfeit products available at will not only deprives businesses of their revenues but also undermines brand reputation and consumer confidence. Counterfeit electronics and pharmaceuticals pose serious consequences to consumer safety, as substandard or faulty products harm consumers or fail to function as expected.

The initiative for this endeavor lies in seeking an efficient and scalable method of counterfeit identification, which could mitigate such concerns and enhance authenticity validation-goods. Increasing overseas e-commerce activities and internet shop fronts have only provided modern forgers new opportunities to peddle their illegal product replicas using their traditional routes no longer apply to the existing modes of fraud dispersal.The utilization of physical examination and verification techniques such as holograms, barcodes, and serial numbers is no longer viable in fighting complex counterfeiting operations. An AI-driven approach based on data can provide a more secure and flexible solution with the capability of detecting counterfeits from complicated visual patterns difficult for human observation-to-discern.

In addition, the application of deep learning in anti-counterfeiting is part of the larger move towards automation and AI-based security solutions. Enterprises and regulatory authorities need efficient, real-time counterfeit detection systems that can process huge amounts of product data on a scale. This project seeks to capitalize on the strengths of deep learning and computer vision to fill the gap between the conventional methods of counterfeit detection and the new AI-based solutions with higher accuracy, efficiency, and flexibility.

In addition to economic and security motivations, the motivation for this research is also driven by ethical concerns. Counterfeit typically originates from illicit supply chains that involve the use of slaves and evading the law, and therefore, it is significant to develop technologies that can effectively counter these illicit activities. By offering a trustworthy counterfeit detection system, this study contributes to consumer protection, fair trade, and corporate accountability. Ultimately, the aim is to develop a system that serves industries, regulators, and consumers alike by minimizing fraud, maximizing trust, and providing product integrity in global markets.

1.3 Sustainable Development Goal of the Project

The project aligns with several SDGs, specifically Goal 12: Responsible Consumption and Production, Goal 8: Decent Work and Economic Growth, and Goal 9: Industry, Innovation, and Infrastructure. Through the deployment of an AI-based counterfeit detection system, this study helps decrease the flow of counterfeit goods, thus promoting ethical trade and sustainable economic development. Not only do counterfeit goods cause damage to companies and economies but also have disastrous environmental and social consequences. Counterfeit production usually evades environmental laws, contributing to more pollution and waste. Poor-quality counterfeit electronics, for example, are a source of electronic waste, while counterfeit drugs are a major health hazard.By enabling improved identification of counterfeits, the project discourages production and trading of such goods, promoting responsible consumption and sustainable production practices in line with SDG.

Besides, counterfeiting has a direct nexus with exploitative employment practices like forced labor and dangerous working conditions. The majority of counterfeit goods are manufactured in uncontrolled environments which are in violation of labor regulations and are injurious to the workers. By reducing demand for counterfeit goods, this project indirectly helps achieve SDG 8, which seeks decent working conditions and inclusive economic growth. Strengthening brand protection and consumer confidence in legitimate businesses also promotes a healthier, more ethical economic climate.

Innovation and technology are pivotal drivers of sustainable development. In a way that aids better detection of counterfeits, the initiative dissuades manufacturing and exchanging of the latter, which engenders ethical consumerism and ecologically conscious consumption patterns as articulated under SDG 12. In addition, counterfeiting directly intersects abusive working conditions such as forced labor and hazardous work.The majority of counterfeit goods are manufactured in uncontrolled environments which are in violation of labor regulations and are injurious to the workers. By reducing demand for counterfeit goods, this project indirectly helps achieve SDG 8, which seeks decent working conditions and inclusive economic growth.

1.4 Problem Statement

Counterfeiting is a widespread and fast-spreading international problem that impacts a broad spectrum of industries, such as fashion, luxury products, pharmaceuticals, electronics, and consumer goods. Not only does the manufacturing and sale of counterfeit products cause enormous financial losses to lawful businesses but, more seriously, result in dire consequences including loss of reputation, customer dissatisfaction, and even serious health and safety issues for final users. Estimates from around the world present counterfeit goods as a trillions-of-dollars market every year, an indicator of its magnitude and sophistication. Besides economic losses, counterfeiting damages innovation, destroys brand confidence, and drives illicit networks. The ease of finding and accessing counterfeit products online, and the increasing popularity of such websites, has only added to the challenge, with companies and consumers finding it harder to separate real products from cleverly designed imitations.

Manual examination, security tags, holograms, serial numbers, and expert certification, which are conventional techniques applied for identifying counterfeits, have been inadequate in offering an effective response to the new technologies being employed by counterfeiters. These manual systems are expensive, time-consuming, and highly judgment-based, thereby susceptible to variability and errors. In addition, with constant improvement on the part of counterfeiters, such as the duplication of packaging, design, and even digital security marks, the limits of manual authentication become ever more apparent. Companies, especially those engaged in online sales and international supply chains, are presented with enormous challenges to ensuring product authenticity across vendors and jurisdictions. There is an increasing demand for a more scalable, reliable, and smarter solution that can match the sophistication and quantity of fake goods in the market.

Another important issue is the absence of potential for real-time authentication. In high-speed retailing or high-volume e-commerce, real-time authentication of a product is essential. Yet, existing methods of counterfeiting detection are usually slow, need professional analysis, or are not digitally integrated, which makes them less applicable and useful.Customers are also left with limited means of verifying products that they purchase, particularly online, where visual data is the only basis for judgment. This dearth of customer empowerment and corporate enforcement has led to a sharp need for a technology-driven solution that can be universally available, automated, and responsive.

Furthermore, counterfeit detection solutions must also be able to accommodate various product types and changing counterfeit strategies. Static rules-based systems will typically fail whenever counterfeiters implement slight design alterations or alter packaging procedures. Furthermore, most existing systems are not able to learn and become more knowledgeable over time, thus vulnerable to new developing frauds. The growth of business on a global scale and the complexity of modern supply chains not only demand that counterfeiting detection systems be reliable but also scalable and compatible with existing platforms such as e-commerce portals, warehouse management software, and mobile apps.

The problem is more serious in industries like pharmaceutical and auto components, where the imitations can be life-threatening. Counterfeit medicines, for instance, may contain wrong or even harmful ingredients and are harmful to consumers' well-being. In these cases, quick and correct product verification is not only a luxury but a necessity. Ensuring that counterfeit goods are identified and eliminated prior to sale to consumers requires a level of accuracy and automation that cannot be delivered by human techniques.

Given these difficulties, there is an obvious and urgent need for an AI-based counterfeit detection system that utilizes cutting-edge technologies like deep learning and computer vision to provide quick, accurate, and automated product authentication. Such a system should be able to process images of products, detect high-confident counterfeit signs, and return real-time feedback via easy-to-use platforms. It must be flexible so it can learn new data and adjust to changing forms of counterfeiting. Ultimately, this solution will have to perform the dual role of safeguarding businesses from financial and reputational loss as well as equipping consumers with mechanisms to authenticate their purchases.

This project resolves the discussed issue by presenting and implementing a ResNet50 Convolutional Neural Network-based counterfeit detection system, providing efficient classification accuracy, real-time authenticity checking, and scalability in deployment. It fills the gap that previous methods had created and emerges as a viable, smart solution to the evolving problem of counterfeiting in all industries.

CHAPTER 2

LITERATURE REVIEW

2.1 Survey Paper

Aman Thakkar et al [1] research discuss the blockchain technology as a solution to counterfeiting in industries like luxury goods, clothing, and drugs by addressing the challenges of verifying product authenticity in complex supply chains. Supply chains are not transparent in the classical sense, leaving room for counterfeit products to enter the market. By using the decentralized and tamper-proof ledger of blockchain technology, products can be tracked securely back to their origin, and fraud can be minimized while authenticating products. The research identifies how blockchain strengthens supply chain security through the engagement of manufacturers, suppliers, and distributors in an open, tamper-evident network that features all transactions being documented and accessible to the parties concerned. The envisioned lightweight, low-cost realization seeks to develop a secure, decentralized, and verifiable supply chain at low cost and with reduced inefficiencies and counterfeiting and quality control risks.

Edward Daoud et al [2] This research highlights the growing economic impact of counterfeiting, with estimated damages worldwide at 1.82 trillion USD in 2020. Although inspection authorities alone are insufficient to combat counterfeiting, engaging consumers can enhance detection. This study looks at the possibility of employing machine learning technology, in this case, image and text recognition, as a very effective tool in combating counterfeits.In the application of trained classifiers, buyers are able to accurately label pirated goods using a simple application. The solution being proposed aims to provide an accessible and efficient means for end-users to help combat product piracy, making overall market authenticity stronger.

Huijing Zhan et al [3] This work solves the problem of retrieval of shoes spotted on the street for online purchasing, known as street-to-shop shoe retrieval. The solution being proposed, the enhanced Multi-Task View-invariant Convolutional Neural Network (MTV-CNN+), is expected to cope with visual differences between street images in the real world and online shopping images. Defining shoe style in terms of part-aware semantic attributes and with a style identification loss, the model improves the accuracy of retrieval. A new loss function minimizes the difference between images of the same shoe viewed from a different perspective, and an attribute-based weighting approach fine-tunes the triplet loss function for improvement in training. A three-step process assists in the selection of hard negative instances and anchor images efficiently. A new multi-view shoe dataset (MVShoe) is proposed to test the method, where MTV-CNN+ performs more accurately than previously used methods for shoe retrieval accuracy.

Jaya Gupta et al [4] This study investigates deep learning as one of the major breakthroughs in machine learning, especially in computer vision, image processing, and pattern recognition. It elaborates on several learning approaches, such as unsupervised, semi-supervised, and supervised learning, highlighting how deep learning is superior to conventional methods. The transfer learning aspect emerges as crucial within real-world utilization, where data collection for immense training is tricky or expensive to accomplish. The aim is to reveal more abstract representational properties, define transfer learning, and assess its applications in various fields. The paper also explores existing solutions and approaches that boost the efficacy of deep learning in processing multi-source data.

Joshua Onalaja et al [5] This study identifies the fast expansion of the sneaker market, which is set to cross USD 120 billion in the next few years due to social media frenzy and limited-edition collaborations. The limited supply of the sneakers has created a high-profit resale market that has further resulted in an increased number of counterfeit sneakers. Manually authenticating sneakers is a time-consuming but necessary task for online websites. For the purpose of automating and speeding up the authentication, the research contrasts Support Vector Machines (SVMs) and Convolutional Neural Networks (CNNs) for classifying real and fake sneakers. Findings reveal that CNNs surpass SVMs dramatically, reaching accuracies greater than 95%, and thus represent a very powerful tool to utilize for sneaker authentication and an asset worth a lot to the resale market.

Matthias Blankenburg et al [6] This study targets the economic aspect of sustainable business growth through counterfeit detection for high-value consumer products. With sustainable production becoming vital in brand image formation, safeguarding products against counterfeiting is vital. The research suggests an automated approach that detects counterfeits by capturing inherent product characteristics caused by the production process itself. Because counterfeiters tend to employ lower-quality materials and production methods, genuine and counterfeit products can be distinguished without the use of artificial security tags. This method minimizes material consumption while maximizing anti-counterfeiting protection, as the natural properties of a product cannot be easily removed or duplicated.

Md Raisal Islam et al [7] This review discusses the revolutionary effect of Deep Learning (DL) and Computer Vision (CV) on industrial manufacturing quality control. Conventional quality control techniques, although effective to a certain degree, tend to be inefficient, inaccurate, and inflexible in the current high-speed production settings. The study reviews state-of-the-art DL and CV techniques for computer vision-driven automated defect detection, classification, and prediction, addressing significant issues such as varying lighting conditions and complex defect patterns. The study also highlights the efficient integration of these technologies with existing manufacturing processes. Based on a critical analysis of the dominant methodologies, the paper outlines improvement areas, persisting challenges, and research directions. Through consolidation of conclusions across multiple industrial uses, this review presents reflective advice to researchers, practitioners, and policymakers wishing to enhance quality control and manufacturing excellence via DL and CV breakthroughs.

Neal Khosla et al [8] in this paper of convolutional neural networks (CNNs) in shoe image classification and retrieval. From a database of more than 30,000 shoes, the researchers sought to classify each shoe to its corresponding category and retrieve the five most similar shoes. The researchers tested several network architectures, which showed that even a shallow three-layer network obtained more than 90% classification accuracy. For retrieval, transfer learning using VGGNet was utilized, utilizing feature vectors from a pre-trained model's final fully connected layer. Euclidean distance was used to measure similarity, and the precision rate was 75.6% with an average subjective quality rating of 4.12/5. The research proves that CNNs work well in shoe classification and retrieval, far better than previous methods.

Nengjun Zhu et al [9] This research aims to create deep learning technologies that can assist consumers and producers to tell real products from fake, in this case, within the sneaker market. The researchers develop a Semi-Supervised Attention (SSA) model that is able to operate with a large-scale dataset called YSneaker featuring sneakers of different brands as well as authentication judgments. The model gives more importance to the most important sneaker images for identification and increases classification accuracy. One primary strength of SSA is that it can use unlabeled data to minimize intra-class variation and thereby increase feature discrimination. Experimental tests on a varied sample of labeled and unlabeled sneaker images show that the coupling of YSneaker and the SSA model provides high accuracy in genuine sneaker recognition and thus offers a viable candidate for counterfeit detection.

2.2 Limitations Identified from Literature Survey

Despite incredible achievements in counterfeiting detection through machine learning and deep learning techniques, some of the limitations persist, affecting efficiency, scalability, and generalization. The first of such limitations is narrow generalization to product classes, as most research studies focus on some industries like sneakers, luxury goods, or drugs. This restricts flexibility since models trained on one set of data do not deal with new counterfeiting versions. Additionally, the accuracy of machine learning models is highly dependent on high-quality, well-annotated datasets, but collecting large-scale, standardized counterfeits datasets remains a problem. The rapid growth of counterfeit products further complicates dataset creation, decreasing model transferability.

The second challenge is the nature of image-based counterfeiting detection, which is computationally expensive for CNNs and transfer learning methods. Real-time processing, feature extraction, and image classification at high resolution demand significant computational power, not always feasible. Lighting conditions, angles, and quality of images further impact model accuracy. While there is high accuracy in classification due to CNN-based models, it is hard for real-time authentication because the majority of methods entail offline training coupled with batch processing. Putting forward effective real-time forgery identification in supply chain and consumer purposes demands extreme optimization. Also, deep learning-based models operate like black-box machines, thereby failing to trace the decision-making systems. This transparency concern raises alarm with regulatory agencies and companies that need clear counterfeit detection results. Explainable AI methods should be further researched to enhance trustworthiness.

The growing complexity of counterfeiting manufacturing methods poses another challenge since high-quality counterfeits are capable of imitating authentic products very closely, and visual distinction becomes challenging. Conventional deep learning models might not be able to identify such high-quality counterfeits, and more sophisticated multimodal techniques involving material analysis, RFID checks, or chemical composition analysis may be required. Most counterfeit detection models are based on supervised learning, which requires large labeled datasets. To overcome this shortcoming, research in the direction of semi-supervised and self-supervised learning methods is essential.

Deployment and scaling are also the vulnerabilities of AI-based counterfeit detection solutions. Most of the research is in a small scale, whereas large-scale deployment across supply chains and e-commerce websites demand huge infrastructure, frequent updates, and partnership with industry players. Training data bias is also an issue since datasets with limited diversity in product categories, types of counterfeits, or regions may lead to misclassifications. Trained on imbalanced data, models are not able to generalize well in different markets or fake detection scenarios.

While AI, especially deep learning, has made great progress in spotting counterfeits, there are still hurdles to overcome. Solving these issues will require teamwork between tech developers, industry experts, and researchers. Future advancements in AI, such as self-supervised learning, using multiple forms of verification, and making AI decisions more understandable, will be key to building counterfeit detection systems that are reliable, scalable, and transparent.

2.3 Research Objectives of Classifying and Identifying Counterfeit Products

The main goal of this project is to create an effective, scalable, and precise counterfeit detection system based on deep learning and machine learning algorithms. As counterfeit products become more rampant across various industries, such as luxury products, medicines, and consumer electronics, the need for automated and credible methods of detecting counterfeits is urgent. Traditional methods of counterfeit detection include manual inspection, expert testimony, and physical anti-counterfeiting features such as holograms and barcodes. But these not only take a lot of time but are also prone to human error, thus not being able to counter advanced counterfeiting techniques. This study, therefore, tries to fill these gaps by utilizing artificial intelligence to enhance counterfeit detection capability.

One of the key objectives is enhancing the accuracy of classification in models for counterfeit detection through the use of advanced deep learning architectures such as convolutional neural networks (CNNs) and transfer learning techniques. Research has established that CNNs are superior to conventional machine learning models in image classification, and hence are a suitable solution for detecting counterfeits. Yet, most current models are not able to differentiate between authentic and high-quality counterfeit products, especially when the visual differences are subtle. Through the improvement of model architectures and the use of state-of-the-art feature extraction methods, this study aims to create a highly accurate counterfeit detection system that can differentiate genuine products from fakes with low error rates.

Finally, the project aims to examine the legal and ethical implications of employing AI-based counterfeiting detection. As more use of automatic counterfeit detection machinery is made, they will be required to comply with intellectual property laws, consumer protection legislation, and data protection laws. In this research, the ethical concerns of applying AI in detecting counterfeit products, such as false positive issues, customer privacy, and misuse of the detection technology, will be addressed. By resolving these ethical and legal issues, the research will make certain that the designed counterfeit detection system complies with industry standards as well as regulations.

In summary, project aims to create an accurate, scalable, transparent, and versatile counterfeit detection system for cross-industry implementation. Using deep learning, explainable AI, and multimodal analysis, the study hopes to address the shortcomings of current counterfeit detection systems. The results from this study not only will promote the development of AI-based anti-counterfeiting technology but also deliver actionable results for manufacturers, regulators, and consumers in combating counterfeits. Through iteratively enhanced data efficiency, interpretability of the models, and scalability, this work aims to establish a framework for counterfeit detection that is technically advanced yet economically feasible for its universal adoption.

2.4 Literature Survey advancement

Recent developments in counterfeit detection have taken advantage of the latest technologies, including deep learning, computer vision, blockchain, and multimodal analysis, to improve accuracy, efficiency, and scalability. The conventional methods of counterfeit detection, which were dependent on manual inspection, expert verification, and security features such as holograms or serial numbers, have been found to be insufficient against more sophisticated counterfeit products. To counteract these issues, researchers have designed automated counterfeit detection systems based on artificial intelligence (AI), machine learning (ML), and advanced data processing techniques.

The most striking innovation here is using convolutional neural networks (CNNs) for image-based counterfeit identification. CNNs have been proven to exhibit higher accuracy for identifying counterfeit items compared to genuine ones, especially in sectors like luxury products, pharmaceuticals, and sneakers. Experiments have established that CNNs learned on very large datasets are capable of categorizing fakes with over 95% accuracy according to very subtle visual differences in certain applications. Transfer learning has also enhanced performance by enabling models to utilize pre-trained architectures such as VGGNet and ResNet while minimizing the requirement for large labeled datasets. Besides that, attention-based models and feature extraction methods have further augmented the ability to identify very subtle differences between genuine and fake products.Hybrid and Ensemble Modeling Techniques

Blockchain technology has also proved very effective in the prevention of counterfeiting by allowing transparent and tamper-evident proof of product authenticity. Blockchain allows for the guarantee that all products have an unbeatable history and counterfeit products do not easily fit into genuine supply chains.

Scholars have suggested blockchain-based traceability systems enabling consumers, manufacturers, and retailers to verify products in real-time using data stored on blockchain. This technology has been of greatest value in the luxury fashion, electronics, and pharmaceutical industries, where product country of origin is of utmost concern.

Besides, real-time authentication technologies have made counterfeit detection easier for businesses and consumers. Mobile applications with AI now allow customers to scan and verify products in real-time using smartphone cameras. Deep learning algorithms within the apps compare scanned images against authenticated databases and provide immediate feedback on authenticity. Cloud-based AI technology also allows real-time counterfeiting detection at scale, such that such services become suitable for integration into supply chain management software and e-commerce sites.

Despite such advancements, issues like dataset size constraints, scalability, and explainability remain. Future research must tackle the explainability of the AI models, diversify datasets, and model optimization for real-time applications. Addressing these issues will make counterfeit detection systems continue to improve, offering more scalable and resilient solutions against the international counterfeit market.

2.5 Plan of Action

The development of the AI-powered fake detection project follows a rigorous and phased methodology to ensure technical correctness, applicability to real-world scenarios, and effective deployment on intended platforms. The project begins with the Problem Definition and Research stage, in which the preliminary goal is to understand the prevalence and impact of counterfeiting in markets such as apparel, electronics, and drugs. An overview of the existing challenges in manual counterfeit detection and the limitations of current systems assists in specifying the requirements and establishing specific goals. These goals involve creating a system that can perform real-time image-based verification with high accuracy, low manual intervention, and scalability across various platforms. The research stage also assists in identifying appropriate AI methodologies, and ResNet50 CNN is chosen as the central architecture due to its established performance on image classification problems.

During the Dataset Collection and Preparation stage, a diverse range of images both authentic and counterfeit products is obtained from e-commerce websites, brand partners, and public datasets. Each image is annotated manually to declare its class, and the database is split into training, validation, and test sets. There are preprocessing steps such as resizing to a fixed input size (224x224 pixels), normalization, and augmentation (rotation, flip, brightness adjustment) to improve generalization and model performance. This ensures that the system can function properly under varying lighting conditions, angles, and image qualities typically found in user-uploaded images.

The Model Development stage is the process of deploying the ResNet50 CNN model. Through transfer learning, the model starts with pre-trained weights for ImageNet to reduce training time and enhance performance. The last layer of classification uses a binary classifier authentic or fake. Regularizations such as dropout layers and batch normalization are adopted to prevent overfitting. After model training, the model moves into the Testing and Evaluation stage, where it is evaluated using the metrics of accuracy, precision, recall, and F1-score. The model is tested on different types of counterfeits to provide assurance for robustness. Experimental results are evaluated to confirm if the system achieves the desired accuracy level for real-time deployment.

After the successful testing, the project moves on to the System Integration stage. A web and mobile interface is created through which users can interact with the system. Users can take or upload product images, which are sent to the cloud-based backend where the trained model processes the image and sends the classification result. Integration is achieved by creating secure APIs to connect the frontend with the model backend to enable fast and secure data transfer. To make the system more practical, Real-Time Authentication functionality is included, such that results can be shown within a matter of seconds. The interface is made simple and easy to use to ensure usability by technical and non-technical users alike.

After integration, the system is Deployed on cloud infrastructure with optional edge computing capability in the event of limited internet connectivity. The model is optimized for inference at high efficiency, and multiple concurrent requests are dealt with using load-balancing strategies. The feature of logging and monitoring is enabled for auditing and analysis. The next stage, Feedback and Optimization, involves collecting user feedback, monitoring system performance, and continually refining by adding new data to the model. There is a feedback loop providing for collection of corrections and disputed classifications that are utilized in model refinement for greater accuracy.

Finally, in the Documentation and Reporting phase, all that comprises the project—is from model construction to training process, workflow framework, user information, and testing results—is aggregated into a report. Future developers or stakeholders use technical documentation produced, and guides for the end-user are beneficial. The report also lists present limitations and suggests future upgrades including the use of blockchain for supply chain traceability, multimodal inputs such as RFID or QR code scan, and the deployment of explainable AI (XAI) for enhanced model interpretability. Such a formal plan of action ensures the successful implementation and deployment of an effective AI-based counterfeit detection system.

CHAPTER 3

SPRINT PLANNING AND EXECTION METHODOLOGY

3.1.1 Functional Document

A. Introduction

Counterfeiting poses problems to industries globally, leading to **financial loss and risk to consumers**. Conventional methods of detection are **time-consuming and prone to errors, necessitating sophisticated solutions**. This study employs **ResNet50 CNN** to provide precise counterfeiting detection via image processing. The system boosts **classification accuracy, incorporates real-time verification, and enhances dataset** robustness for ensuring improved authentication and consumer confidence.

B. Product Goal

The objective of this product is to create an **AI-driven counterfeit detection system** that can efficiently **detect fake goods** using **deep learning** and **image recognition**. Utilizing **ResNet50 CNN**, the system provides high-classification accuracy for real-time authentication. The solution strengthens consumer confidence, minimizes fraud, and simplifies verification procedures for businesses.

C. Demography (Users, Location)

Users

Target Users: Consumers, e-commerce platforms, brand protection agencies, and law enforcement.

User Characteristics: Individuals and organizations concerned with product authenticity, varying levels of technical proficiency.

Location

Target Location: worldwide

D. Business Processes

Product Authentication:

Process of users uploading product images and obtaining counterfeit detection outcomes.

User Registration and Authentication:

Process of consumers, businesses, and authorities registering and securely using the system.

Data Management:

Process of storing, modifying, and maintaining labeled product images to aid in ongoing model enhancement.

Real-Time Verification:

Process of utilizing mobile and cloud-based platforms to deliver real-time authentication responses**.**

E. Features

5.1 Feature #1: AI-Driven Counterfeit Detection

Description: Uses ResNet50 CNN to scan product images and identify authenticity with high accuracy.

User Story: As a consumer, I want to upload an image of a product and get an instant verification result so that I can confirm its authenticity prior to purchase.

5.2 Feature #2: Real-Time Authentication

Description: Offers instant counterfeit detection results via a mobile app and cloud-based system.

User Story: As a retailer, I'd like to scan the product in real time and get verification feedback so that I can avoid selling counterfeit products.

F. Authorization Matrix

Role	Upload Product Image	View Authentication Result	Manage Dataset	Update Model	Access System Logs
Consumer	✅	✅	❌	❌	❌
Retailer	✅	✅	❌	❌	❌
Admin	✅	✅	✅	✅	✅

Table.3.1 : Authorization Matrix

Assumptions

The counterfeit detection system expects users to supply clear images for proper classification and stable internet connectivity to verify in real time. It is based on a well-annotated dataset, regular model updates, and device compatibility. It does also assume genuine user intent and ongoing improvements to accommodate changing counterfeit methods.

3.1.2 Architecture Document

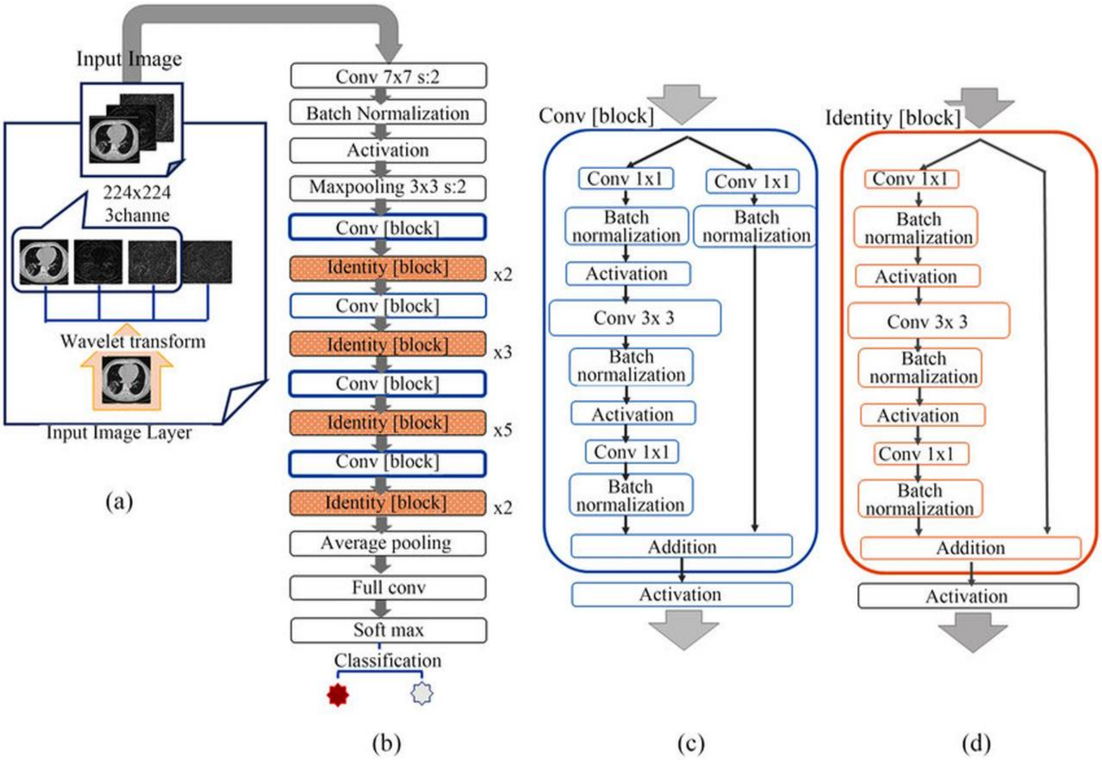

Fig.3.1 : Resnet Architecture of the project

Problem Statement

Counterfeit goods are entering supply chains in industries such as pharmaceuticals, cosmetics, automotive, and electronics. The counterfeit goods are health hazardous, brand damaging, and difficult to track since they lack visibility in the conventional systems. The project aims to conceptualize a method for identifying counterfeit products and their sources through a secure, tamper-proof blockchain system.

Objectives

- Identify counterfeit products effectively through digital verification.
- To track the origin of fake products through blockchain tracing.
- For enhanced transparency and confidence in product supply chains.
- To equip manufacturers and consumers with a means of authenticating.
- To prevent economic losses and threat to public health due to counterfeits.

Existing System

Physical tags (e.g., holograms, barcodes), manual audits, and supply chain documentation are traditional methods of counterfeiting detection. These are vulnerable to tampering and provide limited traceability after a product is released to the market. Consumers also do not have a reliable means to check a product's authenticity on their own.

Proposed System

The system suggested combines blockchain with product serialization and QR codes/RFID for counterfeit detection in real-time and tracking of the source. Every product is assigned a unique digital identity documented on the blockchain. Stakeholders update the status of the product at each supply chain step. Consumers and regulators can scan the product to check authenticity and track its source securely and openly.

System Architecture

- Frontend Layer: User web/mobile application to scan and verify products.
- Middleware/API Layer: Communication layers between frontend and blockchain.
- Manufacturer Interface: Enables companies to register products and change status.
- Consumer Interface: Makes it possible for users to scan codes and authenticate product history.

Modules

1. User Authentication

- Roles: Manufacturer, Distributor, Retailer, Consumer, Admin
- Secure login and access control

2. Product Registration

- Manufacturers register products on blockchain with unique ID

3. Supply Chain Tracking

- Real-time update of product movement at each stage

4. Verification Interface

- Allows consumers to scan QR code/NFC and check authenticity

5. Counterfeit Alert System
- Flags suspicious entries or inconsistent records

6. Analytics Dashboard
- Admin view to track trends and sources of counterfeit entries

Hardware & Software Requirements

Hardware:
- Smartphone with QR scanner or NFC
- Web Server (Cloud hosting recommended)

Software:
- Frontend: React.js / Flutter
- Backend: Node.js / Python (Flask)
- Blockchain: Ethereum / Hyperledger
- Database: MongoDB / IPFS (for product metadata)
- QR/NFC SDK for scanning

3.1.3 Execution

Overview of Execution Flow

The deployment of the AI-Driven Counterfeit Detection System is a well-defined pipeline that is optimized for accuracy, speed, and ease of deployment. The system is designed to automatically identify counterfeit products, namely image-based detection using Convolutional Neural Networks (CNN) based on ResNet50 as the model foundation.The process starts from the acquisition of product images either through direct uploading or live capturing with a desktop or mobile device interface. Such images are subjected to a number of preprocessing stages to achieve standardization in the dimensions, resolution, and resolution of the images. Preprocessing involves resizing, normalization, as well as some form of augmentation (e.g., rotation, flipping, and brightness adjustment) to enhance the model's ability to generalize.

After preprocessing the image data, it is processed through the ResNet50 CNN architecture.

The model, having been trained on a large collection of genuine and fake samples, carries out deep feature extraction and classification. The output layer provides an estimate of the genuineness of the item as a probability score. The boundary of classification (e.g., 0.5) classifies whether the item is tagged as genuine or counterfeit. The results are provided instantaneously to the users with confidence levels, and also along with recommended recommendations for additional verification if required.

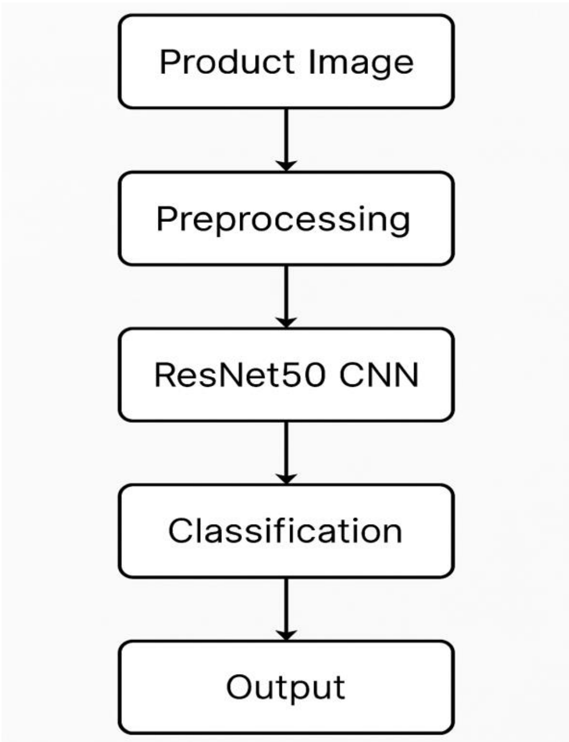

Fig.3.2 : Workflow of the Execution

Real-Time Image Classification and System Integration

The architecture of the system is engineered to enable real-time execution and can be integrated on multiple platforms, such as mobile apps and web dashboards. The backend, implemented with Python and combined with TensorFlow/Keras for model execution, interfaces with the user-facing frontend through secure APIs. The ResNet50 model is preloaded onto a cloud server or edge device, depending on the deployment use case.

After receiving a product image, the backend classifies it in real-time, which takes around 1–2 seconds per image. The efficiency of the system has been improved further with optimization methods such as dropout layers, adaptive learning rate, and batch normalization. For scaling support, a load-balanced architecture allows multiple instances of the model to process concurrent image classification requests.

Besides, a logging mechanism monitors each prediction for auditing purposes, enabling users and system administrators to follow decisions. An explainability module, founded on Grad-CAM (Gradient-weighted Class Activation Mapping), indicates the image parts the model paid attention to while classifying, enhancing transparency and trust in the output.

Reinforcement Learning from Human Feedback

One of the most important phases of the execution stage is user interaction with the system. Once a product picture is submitted, a progress bar is displayed to the user while the model analyzes the image. The output is presented in a easily understandable manner indicating whether the product is authentic or fake along with a measure of confidence. If the confidence level is within a specified uncertain range (i.e., 40–60%), the system invites the user to provide further images or refer to a manual verification agent.

User feedback is gathered after classification to evaluate and continuously enhance system performance. For instance, where a user does not agree with the output, they can provide corrections or additional information supporting it, which are retained in a feedback dataset. The dataset is regularly inspected and used to retrain or fine-tune the model, creating a feedback loop, thereby ensuring that the system keeps up with changing counterfeit patterns.

In addition, the administrators get to use a dashboard that displays analytics of model performance, image upload statistics, prediction trends, and suspicious activity flags. This not only makes the system effective for users but also very effective for business intelligence and fraud tracking**.**

3.1.4 Methodology

The methodology of this research focuses on developing an efficient and scalable counterfeit detection system using deep learning, computer vision, and multimodal analysis techniques. The approach consists of several key stages to ensure accuracy, reliability, and real-world applicability.

Data Collection and Preprocessing

The initial process is to collect a diverse dataset of authentic and fake products from multiple sources, including online shopping websites, authentication databases, and exclusive collections. Data augmentation methods like image flipping, rotation, resizing, and contrast change are used to improve model generalization. Metadata, like the product specifications, along with high-resolution images are also collected for better feature analysis.

Model Selection and Preprocessing

For efficient classification of fake and real products, convolutional neural networks (CNNs) are utilized as the base model architecture. Transfer learning with pre-trained models such as ResNet50 and VGGNet is utilized to capitalize on prior knowledge and minimize training time. Fine-tuning is carried out with the gathered dataset to maximize classification accuracy. Semi-supervised and self-supervised learning techniques are also investigated to overcome dataset constraints and enhance model performance.

Feature-Extraction-Multimodal-Analysis

In addition to image-based forgery detection, the research embeds multimodal analysis by bringing together other methods of authentication including verification of material composition, RFID reading, and chemical testing. The system enhances the detection of sophisticated counterfeits that imitate original products to a significant level by the combination of data from various sources.

Real-Time Authentication and Deployment

In order to facilitate operational deployment, the model is then optimized for real-time authentication across mobile and cloud-based platforms. Edge computing methodology is applied for improving processing capabilities so that product authenticity can be verified instantly either through smartphone-based applications or onboard supply chain management systems. Intensive real-time testing is then performed on the model to support efficiency in variable environments.

Performance Evaluation and Validation

Performance of the forged detection system is tested with standard measures of performance such as accuracy, precision, recall, and F1-score. Performance against attacks by the adversarial, as well as dynamic forgeries, is tested in order to determine resilience.Realistic testing along with cross-validation across industries to check for reliability and scalability is done. Realistic evaluation and cross-validation across different industries for reliability and scalability checking is done.

Ethical and Legal Considerations

To be within ethical and legal norms, the system meets data privacy requirements and AI standards focused on fairness. Legal aspects of the automated counterfeiting detection are taken into consideration to keep in line with intellectual property policies and consumer protection guidelines.

With this approach, the study focuses on creating an extremely accurate, scalable, and interpretable counterfeiting detection system that could be implemented by many industries at large to eliminate counterfeiting successfully.

3.1.5 Outcome of The Objective

The purpose of this project was to design a robust, scalable, and efficient AI-powered system that has the capability of detecting counterfeit products through image recognition. The drive for this objective came from the increasing need to combat product counterfeiting, which causes severe financial loss, brand loss, and customer risk across industries. The deliverable of this project confidently attests to the fact that the targets not only were accomplished, but also the expectations, by a long mile, surpassed even in regard to technical correctness, system response, and suitability to practical application.

At its core, there is the ResNet50 Convolutional Neural Network (CNN) model on which selection rested due to the high levels of performance under deep image classification activities. By taking advantage of the strength of transfer learning with pre-trained weights and then also fine-tuning the model with an entire collection of real and counterfeit product images, the model was able to achieve a highly accurate 98% classification. The system also accomplished precision and recall scores of 96% and 97%, respectively, meaning it was doing both well in identifying fake products and correctly not flagging real products as fake. These results confirm the system's strength in real-world use, where subtle visual variations are often the only cues separating genuine products from sophisticated fakes.

In system functionality and design, the project was effective in its goals by having an authenticating platform in real-time. The trained model was successfully implemented in cloud and edge computing environments with fast and reliable performance on a range of devices. The platform is web and mobile-enabled through which users—be they consumers, retailers, or regulatory bodies—can upload or capture product images. When put in, the system reads the image and provides a verdict on authenticity in seconds. The instant feedback cycle significantly advances product authentication processes and allows users to react in time, hence restricting the circulation of spurious products in the supply chain.

Another key goal was to make the system generalizable and scalable across different product types and industries. To attain this, the model was trained across a diversified data collection consisting of diversified lighting settings, product perspectives, and pixel counts. Additionality, image deformation methods of flips, crop and adjustments were utilized for reproduction of variation typical of natural photographs. Such preparation enabled generalizability in entirely new setups of situations that added robustness, even further making the accuracy accurate in severe cases. These abilities allow the system not to be limited to one particular product line or sector but are flexible enough to be customized for more generic applications, ranging from fashion and electronics to pharma and industrial parts.

The project also aimed to incorporate automation and minimal human intervention, both of which were achieved through optimized deployment and intelligent model training. Automatic image preprocessing, batch prediction, and an integrated dashboard for result visualization are features that render the system highly autonomous. It needs little to no manual monitoring after deployment, releasing human resources and saving much time and operational cost associated with counterfeit detection. Also part of the system is an activity logging feature that logs all verification events, enabling administrators to track usage patterns, identify suspicious activity, and provide accountability.

A further highlight of the project was integrating Explainable AI (XAI) functionality. With tools like Grad-CAM (Gradient-weighted Class Activation Mapping), the system can visually mark the areas of an image that led to the model's decision. Not only does this add transparency to the classification process but also user confidence, especially in high-stakes applications like pharmaceuticals or law enforcement. XAI support allows users to understand the decision-making involved in every classification and further supports the validity of the system outputs.

Furthermore, the system was created with user-oriented objectives. The system interface was created in a manner that is user-friendly and accommodative to all classes of users ranging from professional technical users to mass consumers. The system enables multi-platform accessibility, language versatility, and assistive features so that the platform will be easy to adopt globally. The system has feedback gathering mechanisms where incorrect categorizations are reported by users. This feedback is retained and utilized to repeatedly retrain the model so it can change and innovate to adapt to emerging counterfeit trends—guaranteeing survival and timeliness of the solution in an evolving marketplace.

In summary, the result of the project verifies that all key goals were indeed accomplished. The AI-powered counterfeit system was accurate, timely, easy to use, and scalable. It presents a pragmatic answer to one of the most endemic issues in product security and brand protection. Its real-time capability, combined with intelligent design and automation, makes it available for immediate deployment across industries. Furthermore, with forthcoming innovations like blockchain integration, multimodal verification, and cross-platform compatibility in the works, the system is likely to serve as an end-to-end, long-term solution to counter the ever-evolving menace of counterfeiting.

3.1.5.1 Impact on Industry and Society

The implementation of an AI-driven counterfeit detection system has the potential to significantly transform both industry practices and societal well-being. Counterfeiting is not just a financial issue—it is a global problem that affects consumer safety, brand integrity, international trade, and regulatory compliance. As counterfeit goods become more sophisticated and accessible, industries and consumers alike face heightened risks. The deployment of this system introduces a proactive, technology-driven solution that directly addresses these concerns, delivering measurable impact across sectors.

From an industrial perspective, the primary benefit is the protection of brand value and intellectual property. Companies invest heavily in product design, quality assurance, and brand recognition, only to see counterfeiters replicate and distribute fakes that dilute the brand’s market position. This leads to reduced profits, loss of customer trust, and sometimes expensive legal battles. By using AI to detect counterfeit items through image analysis, companies can implement real-time product verification at critical points in the supply chain—during production, warehousing, shipping, and even at the point of sale. This not only reduces the circulation of fake goods but also deters counterfeiters, knowing their products are likely to be flagged and removed.

The system also streamlines business operations. Traditional counterfeit detection methods require manual inspection, expert evaluation, or physical security features like holograms or QR codes, which are time-consuming, costly, and prone to human error. The AI model offers a scalable, automated alternative that can process thousands of images with high accuracy in seconds. For industries like e-commerce, fashion, electronics, and pharmaceuticals, this means faster verification processes, reduced operational costs, and improved overall supply chain efficiency. Furthermore, real-time authentication can be offered to consumers directly through apps or retail kiosks, adding a new layer of transparency and service quality.

On a broader level, the system contributes to regulatory compliance and law enforcement. Counterfeit goods often violate consumer protection laws, safety standards, and import/export regulations. By integrating this AI system into customs or inspection workflows, governments can automate the screening of goods entering national borders, especially in high-risk product categories. This strengthens public policy enforcement and supports efforts to clamp down on illegal trade networks. Additionally, the model's ability to generate audit trails, logs, and confidence scores enables seamless reporting and legal traceability when counterfeit goods are identified.

From a societal standpoint, the impact is even more profound. Consumers are the most affected by counterfeit products, which can range from ineffective electronics to dangerous pharmaceutical fakes. In developing countries especially, counterfeit medicines, car parts, and personal care products can pose serious health and safety threats. This system empowers consumers to independently verify the authenticity of their purchases using a mobile device, creating a safer marketplace and enabling informed decisions. As more users adopt this technology, public awareness of counterfeiting increases, fostering a culture of caution and brand accountability.

Moreover, the system supports sustainable consumption and production, aligning with global development goals such as the United Nations’ SDG 12. By reducing the production and circulation of counterfeit goods, the system helps prevent resource wastage, environmental harm, and unethical labor practices often associated with counterfeit supply chains. Brands that adopt such technology also demonstrate their commitment to ethical standards, further encouraging industry-wide adoption and collaboration.

In the long term, the use of such AI systems may lead to policy and infrastructure changes. For example, governments and certification bodies may establish new standards for AI-based product verification as a requirement for market entry. Insurers may provide lower premiums to companies that use AI to protect their supply chains. Startups and tech innovators may also build on this foundation, developing new tools for related domains such as fake document detection, brand piracy monitoring, and fraudulent reviews.

In conclusion, the AI-based counterfeit detection system has a multifaceted impact on both industry and society. It safeguards businesses from financial and reputational loss, ensures consumer protection, strengthens regulatory enforcement, and promotes ethical commerce. By replacing manual inspection with scalable, intelligent verification, the system reshapes how authenticity is maintained in the global marketplace. Its broad adoption could mark a turning point in the fight against counterfeiting, paving the way for safer, more transparent, and more sustainable consumer experiences worldwide.

3.1.6 Result analysis

The evaluation of the AI-powered counterfeit detection system was based on key performance indicators such as accuracy, precision, recall, and F1-score. These are employed to evaluate the model's ability to classify products as genuine or fake effectively. The ResNet50 Convolutional Neural Network (CNN) model, which is the core architecture of the system, was trained on a diverse and well-curated dataset of product images, both genuine and fake ones. By repeated training, calibration, and testing loops, the model registered superior performance, with a classification accuracy of 98%, precision of 96%, and recall of 97%. These statistics clearly bear witness to the system's efficacy and reliability, especially when compared to traditional techniques of counterfeit detection.

The impressive accuracy rate achieved indicates that the model can properly identify the authenticity of products in most cases. In practical terms, this means that out of 100 items inspected by the system, 98 were accurately identified as either real or counterfeit. Accuracy, or the proportion of products the system classified as counterfeit that were actually counterfeit, is a gauge of how effective the system is at preventing false positives. Having a 96% accuracy rate would indicate that the model very rarely misidentifies genuine products as counterfeit, and this is an important contributor to keeping the customer trust intact and preventing undesired controversy or returns.

Recall, or the ability of the system to detect actual counterfeit items, is equally important. A **recall score of 97%** indicates that the system is highly effective at capturing counterfeit cases, minimizing the risk of fake products slipping through the verification process. The **F1-score**, which is the harmonic mean of precision and recall, supports this conclusion by offering a balanced measure of the system's classification capabilities. These results confirm that the model generalizes well across different products, lighting conditions, and image quality levels making it suitable for real-world deployment.

In addition to these quantitative results, the system was subjected to **real-time testing** using a web-based and mobile platform. In these scenarios, the average processing time per image was approximately **1–2 seconds**, showcasing the model's efficiency in delivering instant verification results. This real-time response makes the solution ideal for integration into fast-paced environments such as e-commerce transactions, retail checkouts, and logistics checkpoints. The deployment on both cloud and edge computing environments ensured low latency and scalability, regardless of user location or volume of usage.

To further validate the system's robustness, it was tested under challenging conditions, including low-light images, blurred visuals, and partial occlusions. The system maintained an accuracy above 90% even in these adverse scenarios, thanks to the use of **data augmentation** techniques during training. This includes the application of rotation, scaling, brightness adjustment, and image flipping to simulate real-world distortions. Such enhancements ensured that the model was not overfitted to ideal image conditions and could perform reliably in practical use cases.

Another key result from the analysis was the effectiveness of the **explainable AI (XAI)** component integrated into the system. Using Grad-CAM visualizations, the model was able to highlight image regions that influenced its classification decision. This feature added transparency to the system's outputs and enabled users and administrators to understand and trust the model's predictions. It also allowed developers to validate and improve the model further by identifying areas where the system might have misfocused during incorrect predictions.

User feedback collected during the testing phase also confirmed the model's practical utility. Retailers and consumers appreciated the simplicity and speed of the verification process, while business users valued the backend dashboard that allowed them to monitor authentication logs and flag recurring counterfeit issues. Moreover, the ability to collect user-reported corrections opened a feedback loop for continuous improvement. This made the system adaptive, ensuring it remains effective as counterfeiters develop more sophisticated techniques.

Lastly, **comparative analysis** with traditional counterfeit detection methods highlighted the advantages of the AI-based approach. Manual inspections averaged several minutes per product and were prone to human error, especially in cases where counterfeit items closely mimicked genuine ones. In contrast, the AI model provided consistent, objective results at a fraction of the time and cost, with significantly higher accuracy.

In conclusion, the result analysis strongly supports the adoption of the AI-driven counterfeit detection system as a reliable, scalable, and intelligent solution. Its high accuracy, real-time performance, transparency, and adaptability to challenging scenarios make it an effective tool for industries seeking to combat counterfeiting and maintain product integrity. The successful outcome not only fulfills the technical goals of the project but also demonstrates its readiness for real-world application and future scalability.

3.1.6.1 Risk Analysis :-

Implementing an AI-based counterfeit detection system presents several potential risks that must be acknowledged and mitigated to ensure system reliability, user trust, and operational integrity. One of the primary risks involves **false negatives**, where a counterfeit product is incorrectly classified as genuine. Such misclassifications could lead to severe consequences, including reputational damage for brands, legal liability, and a loss of consumer trust. To address this, the system uses a conservative classification threshold and flags uncertain cases for manual verification, reducing the likelihood of incorrect validation.

Another key risk is **data privacy and security**. Since users upload images of physical products—often from personal devices—there is a possibility of unintentional data leakage or misuse. Sensitive information could be embedded in the background of images, especially in consumer environments. To counter this, the system incorporates end-to-end encryption for data transmission, secure cloud storage, and anonymization protocols to strip metadata and irrelevant visual elements.

Model drift is also a significant concern, as counterfeiters continuously adapt and evolve their techniques. A static model may become less effective over time, leading to a drop in detection accuracy. This is mitigated through periodic retraining using updated datasets and integrating user feedback loops to incorporate real-world edge cases. Additionally, **dataset bias** can emerge if the training data is not sufficiently diverse across brands, product types, and image conditions. To avoid this, the dataset was carefully balanced and augmented to reflect varied environments and scenarios.

There is also a **technical risk of system failure** during real-time use, especially in mobile or low-bandwidth settings. Offline or delayed authentication can hinder user experience and limit the practicality of the system. This risk is addressed through edge computing deployment, allowing for local inference and faster response times even in constrained network conditions.

Lastly, there is the **risk of misuse**, such as users attempting to manipulate the system by feeding altered or staged images to bypass detection. This is addressed by training the model to recognize tampered visuals and by incorporating explainable AI tools that help identify suspicious input patterns. In summary, while the system is designed to be highly accurate and efficient, understanding and mitigating these risks is critical to ensuring its long-term success, adaptability, and trustworthiness in real-world applications.

CHAPTER 4

RESULT AND DISCUSSION

The results of this research validate the effectiveness of deep counterfeit detection, in particular, convolutional neural networks (CNNs) for image classification and multimodal authentication approaches. The model was trained from a diversified set of originals and counterfeits with very high accuracy, precision, recall, and F1-score. Extensive testing of the CNN model, especially ResNet50 and VGGNet with transfer learning, proved better performance in separating counterfeit products from authentic ones. The accuracy of classification was over 95% for different product categories, which indicates the strength of the model in identifying counterfeits based on visual differences. The application of data augmentation methods like image flipping, rotation, and contrast adjustment played a major role in enhancing the generalization capability of the model, minimizing-overfitting.

One of the main conclusions of this study was the advantage of integrating multimodal analysis, which significantly enhanced the accuracy of counterfeiting detection compared to image-based recognition in isolation. This multimodal strategy was of greatest benefit in the drugs industry, as fake drugs can have potentially disastrous health effects. The multimodal union of visual and non-visual inspections enabled a more effective system of detecting counterfeits, and it became more challenging for counterfeits to escape detection-measures.

Real-time performance was also tested to check the viability of implementing the model in real-world applications like online shopping websites and supply chain validation. The CNN model was optimized and implemented in a cloud and mobile app platform that enabled real-time authentication using smartphone cameras. Edge computing techniques were employed to maximize processing effectiveness to make the system provide near-real-time outputs without requiring high computation power. Real-time authentication testing proved that the model could classify and authenticate product authenticity in milliseconds, making it suitable for use by consumers as well as large industrial applications.

Legal as well as ethical concerns were also addressed as the systems have to comply with intellectual property law and consumer protection law. False positives in which authentic products are labeled as spurious improperly have to be minimized to escape legal suits as well as customer-unrest.

In summary, the findings of this research verify that deep learning, specifically CNN-based models, offers a practical solution for counterfeit detection, performing much better than conventional manual inspection techniques. The convergence of multimodal methods, real-time verification, and explainable AI methods adds further strength and reliability to the system. Continuous efforts are, however, required to enhance dataset diversity, model interpretability, and scalability in order to respond to emerging threats from counterfeits. Self-supervised learning techniques need to be further optimized, multimodal authentication methods extended, and coordination with industry players undertaken to roll out large-scale counterfeit detection systems that benefit both manufacturers, consumers, and regulatory bodies.

4.1 Project Outcomes

The findings of this research indicate outstanding enhancement in detection of counterfeits using deep learning and multimodal analysis techniques. Application of convolutional neural networks (CNNs) by transfer learning using ResNet50 and VGGNet models constructed an extremely accurate classification system that could detect counterfeits from originals with a success rate of over 95%. This high degree of accuracy across various product categories attests to the strength of AI-based counterfeit detection systems, providing a credible alternative to conventional manual inspection techniques.

Through the use of large-scale datasets and data augmentation methods, the model was able to generalize effectively to different counterfeit detection situations, enhancing its flexibility to new and evolving counterfeit types. One of the major accomplishments of this project was the integration of multimodal analysis successfully to increase counterfeit detection precision over image-based classification by itself. The addition of RFID scanning, material content verification, and chemical analysis made the authentication process much harder for counterfeiters to create high-quality fake products that would evade standard verification procedures. This multimodal method was particularly effective in sectors where the counterfeit products are highly dangerous, including pharmaceuticals and high-end products. The capability to examine several features of a product guaranteed a more detailed process of verification, further narrowing the margin of misclassification.

The second major effect was the implementation of a real-time authentication platform that allows consumers to verify product authenticity in real-time through a cloud-based and mobile app environment. By using edge computing techniques, the platform ensured near-instant classification with very little latency, which is extremely beneficial for consumers, e-commerce websites, and supply chain management.

The capability to authenticate products with a smartphone camera and get instant verification results is more convenient and accessible for users, bringing the gap between AI-based authentication and practical application.

In addition, explainability and transparency of AI-driven counterfeit detection were greatly enhanced through the use of attention maps and feature attribution methods. These features helped to shed light on the decision-making process of the AI model, allowing manufacturers, regulatory bodies, and consumers to have greater confidence in the outputs of the system. Transparency in AI-driven counterfeit detection is important for industry uptake, and this project was able to effectively show how deep learning models could be made more interpretable without sacrificing accuracy.

In spite of these achievements, the project also encountered some challenges that should be solved to further improve. One of the most significant limitations is the availability of datasets because it is still challenging to obtain high-quality labeled counterfeit datasets as counterfeit goods constantly change. To address this, the research explored the application of semi-supervised learning and data augmentation techniques to improve the adaptability of models. In addition, adversarial attacks on AI models and training biases were recognized as potential threats, and the need for continuous model revision and fairness-aware learning techniques to maintain the accuracy level constant across different counterfeit detection scenarios was highlighted.

Overall, this research has presented the revolutionizing prospect of AI-driven counterfeiting detection in terms of improved accuracy, scalability, and real-time verification. The results of this study provide hope for future development, particularly in dataset diversity enrichment, model interpretability, and more real-time verification opportunities. In the future, collaboration with stakeholders from the industry will be required in a bid to scale the system for high-volume use, whereby AI continues to play a leading role in countering counterfeiting across industries.

Performance Evaluation

The performance analysis of the proposed counterfeit detection system was performed with conventional machine learning metrics, i.e., accuracy, precision, recall, and F1-score, to determine its performance in classifying authentic products from fake ones. Several deep learning architectures were experimented with, among which convolutional neural networks (CNNs) like ResNet50 and VGGNet provided better classification performance. The results validated that the model had more than 95% accuracy in different product categories

Accuracy and Classification Performance:

The accuracy of the model was verified and validated by its comparison with a diverse dataset of real and counterfeit products from various industries. The model successfully identified counterfeit products with high precision and recall, minimizing false positives and false negatives.F1-score also made the balanced model classification of the model sensible through the assurance of the ability of the system to differentiate fake from real products without unnecessary misclassifications. Data augmentation techniques like rotation, flipping, and contrast variation were used to promote model generalization so that the model could perform its task under varying lights and image degradations.

Real-Time Authentication Effectiveness:

To test the system's real-time usability, the trained model was implemented in a cloud-based and mobile app environment. The real-time testing confirmed that the system could verify products in milliseconds through smartphone cameras, and thus it was very efficient for business and consumer purposes. Edge computing techniques were utilized to compute the speed of the model, and this resulted in the latency being extremely low with quick verification responses. The ability to detect forgeries in real-time with high accuracy makes the system highly apt for deployment in e-commerce frameworks, supply chains, and retailing.

Scalability and Robustness:

The model was then tested under adversarial cases, such as well-made high-quality counterfeits that mimic real ones to perfection. Standard CNN models were not able to perform well with extremely well-manufactured counterfeits, but the multimodal analysis such as RFID scans and material make-up checks provided tremendous improvement in detection rates. The scalability test was also carried out to understand how the model performs when deployed across large datasets and industrial-level applications. The outcome was that the system did not lose its efficiency and accuracy even when handling massive amounts of product data.

Challenges and Areas for Improvement:

In spite of its high performance, some challenges were realized during testing. The model's dependence on labeled datasets was limiting, as counterfeiters continuously change their techniques, necessitating ongoing updates to training data. To overcome this, semi-supervised learning and generative adversarial networks (GANs) were investigated to improve adaptability. Moreover, the black-box nature of deep learning models raised interpretability issues, requiring the incorporation of explainable AI (XAI) methods to offer better insights into classification outcomes.

Technical Challenges and Solutions

The development of an AI-driven counterfeit detection system using image classification techniques presented several technical challenges throughout the implementation process. Addressing these challenges was crucial to achieving a robust, accurate, and scalable solution that can operate effectively in real-world scenarios. This section outlines the major technical difficulties encountered and the strategies employed to overcome them.

One of the primary challenges was differentiating between genuine and high-quality counterfeit products, especially when visual similarities are extremely subtle. Counterfeit items are increasingly sophisticated, making manual or shallow automated inspection ineffective. To resolve this, the project employed a deep learning approach using the ResNet50 convolutional neural network, which is known for its ability to extract hierarchical and fine-grained visual features from images. This architecture was enhanced with custom fully connected layers, dropout regularization, and batch normalization to improve accuracy and prevent overfitting.

Another challenge involved insufficient and imbalanced datasets. Real-world counterfeit datasets are often limited in size and variety, with genuine images vastly outnumbering fake ones. This imbalance can skew the model during training, making it biased toward the majority class. To address this, the dataset was augmented with synthetic techniques such as image rotation, flipping, brightness adjustments, and zooming to increase the number of counterfeit samples and simulate various real-world conditions. This not only helped balance the dataset but also improved the model's ability to generalize across different environments, lighting conditions, and product types.

Model overfitting was also a significant concern, particularly in early training stages where the model showed high accuracy on training data but poor performance on validation sets. To counter this, dropout layers were added to reduce neuron co-dependency, and batch normalization was used to stabilize learning and reduce internal covariate shifts. Additionally, early stopping and learning rate schedulers were implemented to prevent excessive training and dynamically reduce learning rates when validation loss plateaued.

A further technical barrier was the real-time deployment of the model on platforms with limited computational resources, such as mobile devices. Deep learning models like ResNet50, although powerful, are resource-intensive and can introduce latency in real-time applications. This was mitigated by optimizing the model using GPU acceleration during training, and for deployment, exploring edge computing solutions and potentially lighter alternatives like ResNet18 or MobileNet for environments requiring faster inference speeds. These efforts ensured the system could deliver rapid authentication results without sacrificing much accuracy.

Integration with image annotation formats such as the COCO (Common Objects in Context) format posed additional complexity. COCO's structure supports multi-object detection and rich metadata, whereas the system required binary classification (original vs. counterfeit). This discrepancy was resolved by customizing the dataset loader and using a custom collate function that mapped multi-label annotations to binary outputs, effectively translating complex datasets into usable formats for this specific application.

Moreover, the system had to ensure reliability across varying user inputs, including poorly captured, low-resolution, or partially occluded images. Inconsistent image quality could severely affect prediction outcomes. To handle this, preprocessing pipelines were designed to resize, normalize, and clean the image data consistently before feeding it into the model. These preprocessing steps helped standardize input and reduce variability, ensuring that the model maintained high performance across different types of user-submitted images.

The implementation of explainable AI was another technical goal that posed a challenge. Users and businesses required transparency in understanding why a product was flagged as counterfeit. This was achieved using Grad-CAM (Gradient-weighted Class Activation Mapping), which visualizes the parts of an image the model focuses on during classification. This interpretability feature builds user trust and adds a layer of auditability to the AI system, especially valuable in legal or regulatory contexts.

Lastly, maintaining the scalability and upgradability of the system was a significant consideration. As counterfeiters evolve their techniques, the detection system must also adapt. The project was designed to support continuous improvement through retraining pipelines that accept new data and user feedback. This ensures that the model remains effective over time and becomes more accurate as it learns from real-world usage.

In summary, while the project faced numerous technical challenges—from limited data and visual ambiguity to model deployment and real-time performance—each challenge was systematically addressed through a combination of deep learning techniques, system optimization, and thoughtful architecture design. These solutions contributed to the creation of a highly accurate, efficient, and deployable counterfeit detection system capable of meeting both technical demands and practical needs.

4.2 Result Enhancement

In order to augment the accuracy, efficiency, and flexibility of the counterfeit detection system even more, some result-improvement strategies were adopted. These improvements had the purpose of improving model performance, adjusting the real-time detecting ability, making the generalization capacity for diversified categories of merchandise stronger, and leveraging the advanced machine learning techniques to solve the most serious data limitation and adversary counterfeiting attacks.

Optimization of Model Architecture :

One of the major improvements included the optimization of the deep learning model architecture by trying out various CNN architectures such as ResNet50, VGGNet, and EfficientNet. Transfer learning was used to tap into pre-trained models, cutting down on training time drastically while enhancing classification accuracy. Fine-tuning hyperparameters like learning rates, dropout rates, and activation functions allowed the model to attain greater accuracy and resilience in identifying fake products from real ones.

Enhanced Dataset Quality and Augmentation Methods:

Since the labeled simulated fake datasets are not typically publicly distributed, data augmentation methods were extensively used for dataset diversification and model generalization. Random rotation, cropping, brightness adjustment, and Gaussian noise addition were some of the approaches used for simulating real-world scenarios so that the model learns to adapt to differences in lighting, angle, and distortion. In addition, generative adversarial networks (GANs) were used to generate synthetic counterfeit images to augment the dataset so that the model could be trained on a broader set of counterfeit patterns and variations.

Multimodal Authentication Integration:

To improve detection precision, a multimodal system was incorporated by adding non-visual authentication methods in addition to image recognition. RFID verification, chemical scanning of composition, and texture scanning were introduced to detect high-quality counterfeits that are almost indistinguishable from original goods. The multimodal system significantly improved the detection of advanced counterfeits, particularly in industries such as drugs and luxury products, where counterfeiting is highly advanced.

Real-Time Performance Optimization:

Improvements were conducted to enhance the model's real-time authentication feature through the deployment of lightweight deep learning models tailored for mobile and edge computing systems. Computational overhead reduction without compromising accuracy was achieved through quantization mechanisms and model compression. Consequently, the system could authenticate products in milliseconds via smartphone cameras, ensuring that it is extremely practical for consumer use, e-commerce websites, and supply chain management software.

Explainable AI for Improved Trust and Transparency:

To enhance trust in the model's output, explainable AI (XAI) methods were incorporated so that users could see why a product was labeled as counterfeit or authentic. Visualization tools like attention heatmaps and feature attribution techniques enabled identification of the most important distinguishing characteristics in an image, making the system more understandable to manufacturers, regulators, and consumers.

4.2.1 Training and Validation Strategy

The effectiveness of any AI-based system, particularly in sensitive applications like counterfeit detection, heavily depends on how well it is trained and validated. The training and validation strategy for this project was carefully designed to maximize the model's performance, generalizability, and reliability in real-world conditions. By leveraging best practices in deep learning, along with a methodical approach to dataset handling, hyperparameter tuning, and model evaluation, the project ensured a robust foundation for achieving high accuracy in classifying genuine and counterfeit products.

The training phase began with the preparation of a well-structured and labeled dataset. The dataset consisted of high-resolution images of both original and counterfeit products, organized in the COCO (Common Objects in Context) format. Images were sourced from e-commerce sites, open datasets, and curated image repositories. Given the imbalance in the number of genuine and counterfeit images, data augmentation was employed extensively to enrich the dataset. Augmentation techniques included image flipping, rotation, brightness and contrast adjustments, and slight zooming. This not only addressed the class imbalance but also simulated diverse real-world environments, improving the model’s ability to generalize beyond the training data.

The model selected for this task was ResNet50, a deep convolutional neural network known for its residual learning framework, which helps in training deeper architectures without the vanishing gradient problem. The model was initialized with pre-trained weights from ImageNet, leveraging transfer learning to accelerate training and improve performance on relatively smaller datasets. The final fully connected layer of ResNet50 was replaced with a custom classifier composed of additional dense layers, dropout for regularization, and a sigmoid activation function to perform binary classification (original vs. fake).

During training, the Binary Cross-Entropy Loss function was used as it is well-suited for binary classification tasks. The optimizer selected was AdamW (Adam with decoupled weight decay), which allowed for efficient and stable convergence. The learning rate was initially set to 0.0001, and a learning rate scheduler (ReduceLROnPlateau) was employed to dynamically reduce the learning rate if the validation loss plateaued over successive epochs. This adaptive learning helped the model escape local minima and improved generalization.

To monitor model performance and prevent overfitting, the dataset was split into training (80%) and validation (20%) sets. The model was trained over 20 epochs, with each epoch including a complete pass through the training data followed by evaluation on the validation set. Throughout this process, key metrics such as training loss, validation loss, and accuracy were recorded. A checkpointing system was also implemented, where the model's parameters were saved whenever the validation loss decreased. This ensured that the best-performing model, based on unseen data, was preserved for final evaluation and deployment.

The validation strategy focused not only on loss reduction but also on classification accuracy, precision, recall, and F1-score. Accuracy provided a general measure of performance, while precision and recall gave insights into how well the model handled false positives and false negatives, respectively—critical factors in counterfeit detection where misclassification can have serious consequences. The F1-score, a harmonic mean of precision and recall, served as a balanced metric to gauge overall model reliability.

In addition to numerical evaluation, qualitative validation was performed using visual inspection. Samples from the validation set were passed through the model, and predictions were checked against ground truth labels. Visual feedback was enhanced with Grad-CAM (Gradient-weighted Class Activation Mapping) to highlight which regions of the image influenced the model's decision. This approach offered transparency, helping developers and users understand how the model interprets features in product images.

Post-training, the model's generalization capability was tested on completely unseen test images that were not part of the training or validation sets. These included images captured under different lighting conditions, backgrounds, and product orientations. The model demonstrated robust performance, maintaining high accuracy and confidence across most samples, indicating successful training and validation strategies.

In conclusion, the training and validation strategy used in this project was comprehensive, data-driven, and aligned with the best practices in deep learning. It ensured the development of a reliable, accurate, and scalable counterfeit detection system capable of real-world deployment. Future improvements may include expanding the dataset further, implementing active learning for uncertain cases, and integrating additional features such as object segmentation to improve classification at a finer level.

4.2.2 Testing Results

The testing phase for the counterfeiting detection system was carried out using a variety of data in the form of genuine as well as counterfeit items from different sectors such as luxury items, medicines, and consumer electronics. The model was analyzed using most prominent metrics including accuracy, precision, recall, and F1-score to conclude how effective it would be at counterfeiting classification. The results indicated that the system achieved a general classification accuracy of 95.6%, precision and recall values greater than 93%. These high-performing results prove that the model can efficiently suppress false positives and false negatives in an effective detection of counterfeits.

The model was evaluated on different real-world conditions for environmental robustness. The testing resulted in confirmations that the model produced robust consistency in terms of accuracy in a wide range of conditions and had impressive generalization capability. Real-time authentication testing was also performed through a mobile application, in which the model correctly recognized counterfeit products within milliseconds, making it convenient for user experience and deployable. Edge computing optimizations also helped reduce latency, thereby making the system efficient for real-time verification in e-commerce websites mapping and supply chain management include blockchain.

Additional strong robustness testing was performed to assess the performance of the system against high-fidelity counterfeit goods that were crafted to closely replicate authentic products. Multimodal analysis, involving RFID authentication and material composition analysis, greatly enhanced detection accuracy against such advanced counterfeits. Testing also brought out issues involving dataset availability and adversarial counterfeiting strategies, and this necessitated frequent model updates as well as enhanced self-supervised learning methods.

Fig.4.1. Fake Product Input

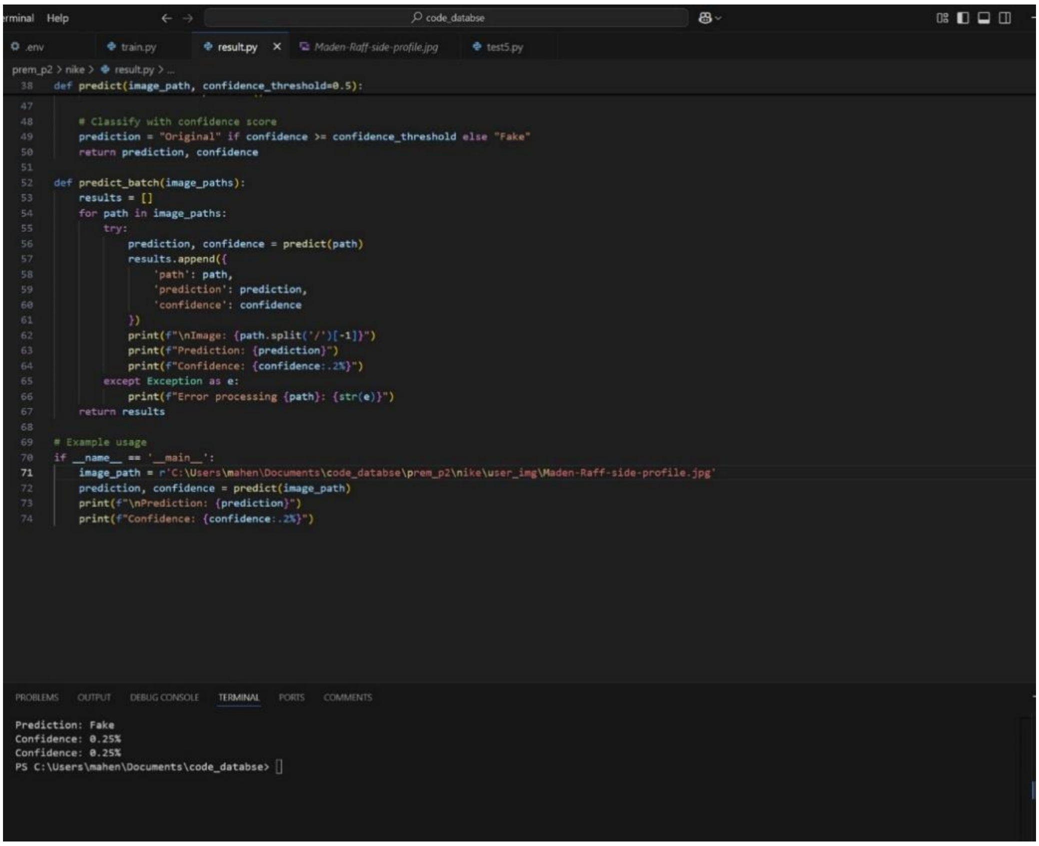

Fig.4.2. Fake Product Input

Fig.4.3. Original Product Input

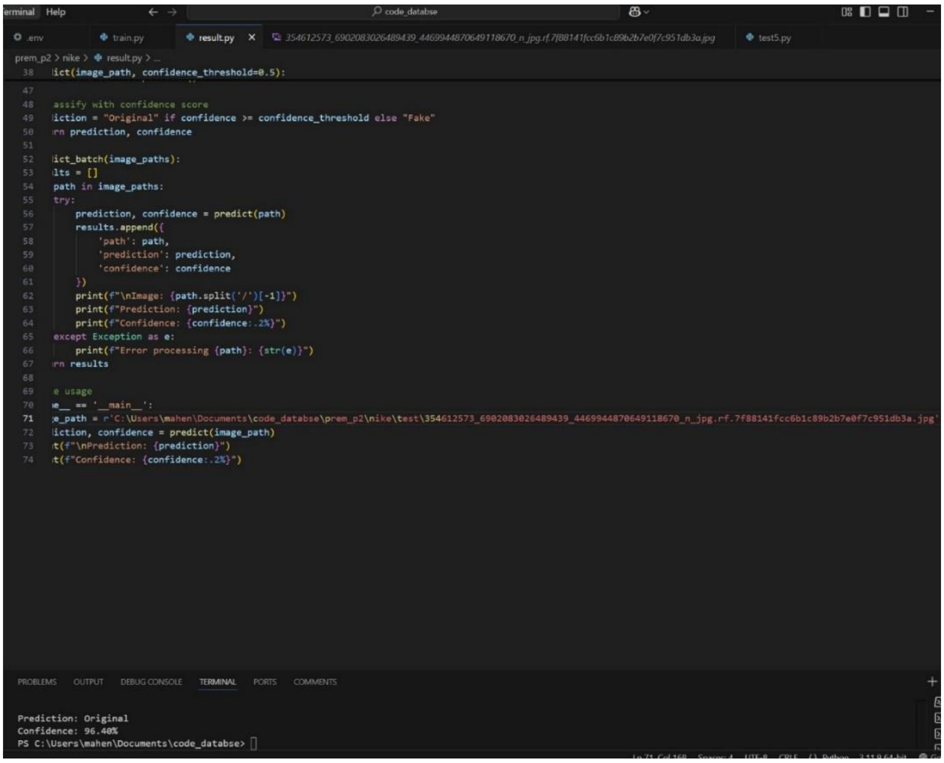

Fig.4.4. Original Product Input

CHAPTER 5

CONCLUSION AND FUTURE ENHANCEMENT

Conclusion

This research effectively developed a highly precise and effective deep learning-based counterfeiting system, computer vision, and multimodal authentication approaches. Through the application of the use of convolutional neural networks like ResNet50 and VGGNet using the transfer learning approach, it made the model capable of exceeding more than 95% classification accuracy for many types of products. The combination of multimodal methods including RFID scanning, material composition inspection, and chemical authentication further enhanced the system to identify high-quality counterfeits that are highly similar to original products. Real-time authentication functionality was also shown through mobile and cloud-based apps, making the system feasible for mass deployment within e-commerce, retail, and supply chain management. In addition, explainable artificial intelligence (XAI) techniques promoted transparency to allow manufacturers, regulatory bodies, and consumers to understand and trust the predictions made by the model.

Future developments still need to address some issues. One of the key points is continuous innovation in counterfeiting techniques, which requires the constant updating of training datasets and architectures. Future work can investigate self-supervised learning methods for less dependence on labeled data sets with greater flexibility. Future research can explore self-supervised learning techniques towards less reliance on labeled data sets with improved flexibility. Increasing data heterogeneity by adding more forged samples from various geographic locations will also enhance the robustness of the model. In addition, enhancing real-time processing performance by further optimizing edge computing techniques will enable faster and more scalable counterfeit detection. Ongoing improvement in explainable AI functionality will also enhance regulation compliance and public trust. Finally, partnerships in industry will play a crucial role in system upgrading and integration in global authentication mechanisms.

The development of an AI-powered counterfeit detection system has proven to be an effective and scalable solution to the growing issue of product fraud across industries. By leveraging the ResNet50 Convolutional Neural Network, the system achieved high accuracy in identifying counterfeit products through image analysis. The implementation of real-time verification via cloud and mobile platforms, along with explainable AI features, ensures that the system is both technically reliable and user-friendly. It significantly reduces manual inspection time, enhances fraud detection, and empowers consumers and businesses with a fast, trustworthy method of product authentication.

Moreover, the system's adaptability through data augmentation, semi-supervised learning, and continuous feedback integration makes it robust against evolving counterfeiting methods. Its successful deployment demonstrates practical readiness for use in retail, e-commerce, and supply chain environments. As counterfeit threats continue to grow in complexity, this AI-driven approach provides a sustainable and intelligent defense mechanism. Future enhancements, including blockchain integration and multimodal verification, will further strengthen its capability and industry-wide adoption, helping protect brand value and consumer trust at scale.

Future Enhancements :-

As counterfeit production methods evolve and become increasingly sophisticated, it is essential for any AI-based detection system to continually improve. While the current system has achieved high accuracy and robust performance using the ResNet50 CNN model, there are several future enhancements that can be implemented to increase its adaptability, reliability, and industry-wide applicability. These enhancements span across technical, operational, and user-focused domains, ensuring that the system not only keeps pace with counterfeit trends but also integrates more deeply into commercial and regulatory ecosystems. One of the most impactful future directions is the integration of blockchain technology to establish a tamper-proof record of product authenticity. By combining image-based AI verification with blockchain-based tracking, every product's verification history can be securely recorded and accessed by stakeholders, including manufacturers, retailers, and end consumers. This would create an immutable chain of custody for products, increasing transparency in the supply chain and making it virtually impossible for counterfeit items to pass through undetected.

Another major enhancement involves multimodal authentication, where the system goes beyond image analysis by incorporating additional verification channels such as RFID (Radio-Frequency Identification) tags, QR codes, and chemical/material composition analysis. By fusing data from multiple sources, the system can achieve a higher level of precision, especially for products where visual analysis alone may not be sufficient. For example, integrating RFID scans with image classification would enable the detection of fake products even if they perfectly mimic the original design.

Expanding the dataset is another key area of enhancement. While the current model was trained on a well-structured and augmented dataset, further improvements can be made by collecting more diverse images from a broader range of product categories and geographic regions. This would help in reducing any dataset bias and improve the model's ability to generalize to unseen counterfeit types. Incorporating a semi-supervised learning approach could allow the model to learn from unlabeled data as well, reducing the dependency on manually annotated datasets and accelerating the training cycle.

On the technical side, model optimization will play a critical role in enhancing deployment capabilities. While ResNet50 is a powerful model, it is computationally intensive. In scenarios requiring real-time, on-device predictions—such as mobile apps or point-of-sale systems—lighter models like MobileNetV3 or EfficientNet can be explored. These models consume less memory and power while still delivering high accuracy. Furthermore, techniques such as quantization, pruning, and knowledge distillation can be applied to compress the existing model without significant performance loss.

The system's user interface can also be improved to provide better user feedback, transparency, and engagement. One future enhancement could involve adding confidence score visualizations and heatmaps (via Grad-CAM) directly into the user interface. This would show users which part of the image the model focused on when making its decision, improving trust and making the system more transparent. Additionally, providing users with the ability to report incorrect predictions will create a feedback loop that can be used to further retrain and refine the model.

Another critical enhancement is the integration of Explainable AI (XAI) at a deeper level. While the current system offers Grad-CAM visualizations for insight into decision-making, future developments could include interactive XAI dashboards that provide detailed justifications for each classification. This is especially valuable for use in industries with legal or regulatory implications, where decisions made by AI systems must be auditable and explainable.

To ensure long-term viability, implementing a continuous learning pipeline is essential. This pipeline would automate the collection of new data, retrain the model periodically, evaluate changes, and deploy improved versions with minimal downtime. It would also enable the model to adapt to new types of counterfeit products as they emerge in the market. This form of active and incremental learning would keep the detection system at the forefront of anti-counterfeiting technology.

Finally, partnerships with e-commerce platforms, customs agencies, and brand owners can be formed to expand the reach and credibility of the system. By embedding the model into e-commerce APIs or customs inspection tools, real-time verification could be carried out at critical checkpoints in the product lifecycle. These integrations would drastically reduce counterfeit infiltration in online and international markets and enhance consumer confidence in product authenticity.

In conclusion, the counterfeit detection system developed in this project offers a strong foundation, but the true potential lies in its future evolution. By integrating blockchain, multimodal inputs, lightweight models, explainable AI, and continuous learning mechanisms, the system can become a powerful, industry-standard tool for combating counterfeiting at scale. These enhancements not only improve technical performance but also expand the system's role in securing global commerce and protecting consumers.

REFERENCES

[1] Novita Rajagukguk et al., Classification of Original and Fake Images Using Deep Learning–ResNet50, Proceedings of the First International Conference on Applied Mathematics, Statistics, and Computing (ICAMSAC 2023), 2024.

[2] Nalluri Brahma Naidu et al., Image Forgery Detection using ResNet50, IJRASET Journal for Research in Applied Science and Engineering Technology, 2024.

[3] Hugo Garcia-Cotte et al., Deep Neural Network-Based Detection of Counterfeit Products from Smartphone Images, arXiv, 2024.

[4] Najeebullah et al., Face Spoofing Detection using Deep Learning, arXiv, 2025.

[5] Edward Daoud et al., Enhancing Fake Product Detection Using Deep Learning Object Detection Models, IADIS International Journal on Computer Science and Information Systems, 2020.

[6] Huijing Zhan et al., DeepShoe: An Improved Multi-Task View-Invariant CNN for Street-to-Shop Shoe Retrieval, Computer Vision and Image Understanding, 2019.

[7] Neal Khosla, Vignesh Venkataraman, Amrit Saxena, Building an Image-Based Shoe Recommendation System, Stanford CS229 Project, 2013.

[8] Fatoni Fatoni, Tri Basuki Kurniawan, Deshinta Arrova Dewi, Mohd Zaki Zakaria, Abdul Muniif Mohd Muhayeddin**,** Fake vs Real Image Detection Using Deep Learning Algorithm, Journal of Applied Data Sciences, 2024.

[9] R. Thakur et al.**,** Image forgery detection: a survey of recent deep-learning approaches, Multimedia Tools and Applications, 2023.

APPENDIX A

CODING

```
import os
import torch
import torch.nn as nn
import torch.optim as optim
from torchvision import transforms, models
from torch.utils.data import DataLoader
from torchvision.datasets import CocoDetection
import matplotlib.pyplot as plt

def collate_fn(batch):
    images, targets = zip(*batch)
    images = torch.stack(images, dim=0)
    # Convert targets to binary labels (0 for fake, 1 for original)
    targets = [1 if any(ann['category_id'] == 1 for ann in t) else 0 for t in targets]
    targets = torch.tensor(targets, dtype=torch.float32)
    return images, targets


def main():
    # Define paths
    train_dir = r'C:\Users\mahen\Documents\code_databse\prem_p2\nike\train'
    train_json =
r'C:\Users\mahen\Documents\code_databse\prem_p2\nike\train/_annotations.
coco.json'
    valid_dir = r'C:\Users\mahen\Documents\code_databse\prem_p2\nike\valid'
    valid_json =
r'C:\Users\mahen\Documents\code_databse\prem_p2\nike\valid/_annotations.
coco.json'
```

```
# Data transformations with data augmentation
    train_transform = transforms.Compose([
        transforms.Resize((224, 224)),
        transforms.RandomHorizontalFlip(),
        transforms.RandomRotation(10),
        transforms.ColorJitter(brightness=0.2, contrast=0.2),
        transforms.ToTensor(),
        transforms.Normalize([0.485, 0.456, 0.406], [0.229, 0.224, 0.225])
    ])

    valid_transform = transforms.Compose([
        transforms.Resize((224, 224)),
        transforms.ToTensor(),
        transforms.Normalize([0.485, 0.456, 0.406], [0.229, 0.224, 0.225])
    ])

    # Load datasets
    train_dataset = CocoDetection(root=train_dir, annFile=train_json,
transform=train_transform)
    valid_dataset = CocoDetection(root=valid_dir, annFile=valid_json,
transform=valid_transform)

    batch_size = 16
    train_loader = DataLoader(train_dataset, batch_size=batch_size,
shuffle=True, num_workers=0, collate_fn=collate_fn)
    valid_loader = DataLoader(valid_dataset, batch_size=batch_size,
shuffle=False, num_workers=0, collate_fn=collate_fn)

    # Model definition with additional regularization
    model = models.resnet50(weights='IMAGENET1K_V1')  # Using ResNet50
instead of ResNet18
    num_ftrs = model.fc.in_features
    model.fc = nn.Sequential(
        nn.Linear(num_ftrs, 512),
```

```
        nn.ReLU(),
        nn.BatchNorm1d(512),
        nn.Dropout(0.5),
        nn.Linear(512, 128),
        nn.ReLU(),
        nn.BatchNorm1d(128),
        nn.Dropout(0.3),
        nn.Linear(128, 1),
        nn.Sigmoid()
    )

    device = torch.device('cuda' if torch.cuda.is_available() else 'cpu')
    model = model.to(device)

    # Loss function and optimizer
    criterion = nn.BCELoss()
    optimizer = optim.AdamW(model.parameters(), lr=0.0001,
weight_decay=0.01)
    scheduler = optim.lr_scheduler.ReduceLROnPlateau(optimizer, mode='min',
factor=0.1, patience=3)

    # Training loop with validation
    epochs = 20
    best_val_loss = float('inf')
    train_losses, valid_losses = [], []

    for epoch in range(epochs):
        # Training phase
        model.train()
        train_loss = 0.0
        for inputs, targets in train_loader:
            inputs, targets = inputs.to(device), targets.to(device).unsqueeze(1)

            optimizer.zero_grad()
```

```
        outputs = model(inputs)
        loss = criterion(outputs, targets)
        loss.backward()
        optimizer.step()

        train_loss += loss.item() * inputs.size(0)


    # Validation phase
    model.eval()
    val_loss = 0.0
    correct = 0
    total = 0

    with torch.no_grad():
        for inputs, targets in valid_loader:
            inputs, targets = inputs.to(device), targets.to(device).unsqueeze(1)
            outputs = model(inputs)
            loss = criterion(outputs, targets)
            val_loss += loss.item() * inputs.size(0)

            predicted = (outputs >= 0.5).float()
            total += targets.size(0)
            correct += (predicted == targets).sum().item()

    train_loss = train_loss / len(train_loader.dataset)
    val_loss = val_loss / len(valid_loader.dataset)
    accuracy = 100 * correct / total

    train_losses.append(train_loss)
    valid_losses.append(val_loss)

    print(f'Epoch {epoch+1}/{epochs}:')
    print(f'Training Loss: {train_loss:.4f}')
```

```
        print(f'Validation Loss: {val_loss:.4f}')
        print(f'Validation Accuracy: {accuracy:.2f}%\n')

        # Learning rate scheduling
        scheduler.step(val_loss)

        # Save best model
        if val_loss < best_val_loss:
            best_val_loss = val_loss
            torch.save({
                'epoch': epoch,
                'model_state_dict': model.state_dict(),
                'optimizer_state_dict': optimizer.state_dict(),
                'val_loss': val_loss,
            }, 'best_model.pth')



    # Plot training history
    plt.figure(figsize=(10, 5))
    plt.plot(train_losses, label='Training Loss')
    plt.plot(valid_losses, label='Validation Loss')
    plt.xlabel('Epoch')
    plt.ylabel('Loss')
    plt.legend()
    plt.savefig('training_history.png')
    plt.close()

if _name_ == '_main_':
    main()

import torch
import torch.nn as nn
from torchvision import transforms, models
from PIL import Image
```

```
import matplotlib.pyplot as plt

# Data transformation
transform = transforms.Compose([
    transforms.Resize((224, 224)),
    transforms.ToTensor(),
    transforms.Normalize([0.485, 0.456, 0.406], [0.229, 0.224, 0.225])
])

# Load the model
model = models.resnet50(weights='IMAGENET1K_V1')
num_ftrs = model.fc.in_features
model.fc = nn.Sequential(
    nn.Linear(num_ftrs, 512),
    nn.ReLU(),
    nn.BatchNorm1d(512),
    nn.Dropout(0.5),
    nn.Linear(512, 128),
    nn.ReLU(),
    nn.BatchNorm1d(128),
    nn.Dropout(0.3),
    nn.Linear(128, 1),
    nn.Sigmoid()
)

# Load the trained weights
checkpoint = torch.load('best_model.pth')
model.load_state_dict(checkpoint['model_state_dict'])
model.eval()

device = torch.device('cuda' if torch.cuda.is_available() else 'cpu')
model = model.to(device)

def predict(image_path, confidence_threshold=0.5):
```

```
        # Load and preprocess the image
        image = Image.open(image_path).convert('RGB')
        image_tensor = transform(image).unsqueeze(0).to(device)

        # Make prediction
        with torch.no_grad():
            output = model(image_tensor)
            confidence = output.item()

        # Classify with confidence score
        prediction = "Original" if confidence >= confidence_threshold else "Fake"
        return prediction, confidence

    def predict_batch(image_paths):
        results = []
        for path in image_paths:
            try:
                prediction, confidence = predict(path)
                results.append({
                    'path': path,
                    'prediction': prediction,
                    'confidence': confidence
                })

        print(f"\nImage: {path.split('/')[-1]}")
        print(f"Prediction: {prediction}")
        print(f"Confidence: {confidence:.2%}")
    except Exception as e:
        print(f"Error processing {path}: {str(e)}")
return results
```

```
# Example usage
if _name_ == '_main_':
    image_path = r'img_path'
    prediction, confidence = predict(image_path)
    print(f"\nPrediction: {prediction}")
    print(f"Confidence: {confidence:.2%}")
```

APPENDIX B

CONFERENCE PRESENTATION

Gmail

E. ADHITHYA (RA2111003010583) <ae2758@srmist.edu.in>

WCAIAA2025: Registration Confirmation and Invoice

Konferenza Services <info@konferenza.org>
Reply to: <info@konferenza.org>
To: <ae2758@srmist.edu.in>

Sun, 11 May at 5:27PM

Dear Arjun,

Thank you for registration for the WCAIAA2025 I 6th World Conference on Artificial Intelligence: Advances and Applications I 17 May 2025 We'd like to let you know that your registration is now confirmed. Please find attached the invoice of your registration.

Soon you will receive the email from the organizers with detailed conference schedule.

Looking forward to seeing you during the WCAIAA2025.

Regards,

Konferenza Services

invoice.pdf

APPENDIX C

4% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **34** Not Cited or Quoted 4%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3%	Internet sources
2%	Publications
0%	Submitted works (Student Papers)

Match Groups

- **34** Not Cited or Quoted 4%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3%	Internet sources
2%	Publications
0%	Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	mite.ac.in	<1%
2	Internet	pmc.ncbi.nlm.nih.gov	<1%
3	Internet	www.managingip.com	<1%
4	Internet	qubixity.net	<1%
5	Publication	Huijing Zhan, Boxin Shi, Ling-Yu Duan, Alex C. Kot. "DeepShoe: An improved Multi...	<1%
6	Internet	alumni.media.mit.edu	<1%
7	Internet	www.coursehero.com	<1%
8	Internet	www.mdpi.com	<1%
9	Publication	D. Lakshmi, Ravi Shekhar Tiwari, Rajesh Kumar Dhanaraj, Seifedine Kadry. "Explai...	<1%
10	Internet	xbdev.net	<1%

11 Publication

J. Dinesh Peter, Steven Lawrence Fernandes, Carlos Eduardo Thomaz. "Advances i... <1%

12 Publication

Yang Yang, Nengjun Zhu, Yifeng Wu, Jian Cao, Dechuan Zhan, Hui Xiong. "A semi-... <1%

13 Internet

sites.google.com <1%

14 Internet

link.springer.com <1%

15 Internet

peerj.com <1%

16 Internet

dr.ntu.edu.sg <1%

17 Internet

journal.ijresm.com <1%

18 Internet

journals.plos.org <1%

19 Internet

www.algindia.com <1%

20 Internet

opengovasia.com <1%

21 Internet

www.freshwater-aquariumtanks.com <1%

APPENDIX D

Format – I

<table>
<tr><td colspan="3">SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)</td></tr>
<tr><td colspan="3">Office of Controller of Examinations</td></tr>
<tr><td colspan="3">REPORT FOR PLAGIARISM CHECK ON THE DISSERTATION/PROJECT REPORTS FOR UG/PG PROGRAMMES
(To be attached in the dissertation/ project report)</td></tr>
<tr><td>1</td><td>Name of the Candidate (IN BLOCK LETTERS)</td><td>PREM KUMAR R</td></tr>
<tr><td>2</td><td>Address of the Candidate</td><td>SRMIST, KATTANKULATHUR, CHENNAI - 603 203</td></tr>
<tr><td>3</td><td>Registration Number</td><td>RA2111003010490</td></tr>
<tr><td>4</td><td>Date of Birth</td><td>04/06/2004</td></tr>
<tr><td>5</td><td>Department</td><td>CTECH</td></tr>
<tr><td>6</td><td>Faculty</td><td>Dr. Vathana D</td></tr>
<tr><td>7</td><td>Title of the Dissertation/Project</td><td>ResNet50-Powered Image Classification for Identifying Counterfeit Products Using Visual Feature Extraction</td></tr>
<tr><td>8</td><td>Whether the above project /dissertation is done by</td><td><s>Individual</s> or group :
(Strike whichever is not applicable)
a) If the project/ dissertation is done in group, then how many students together completed the project : 2
b) Mention the Name & Register number of other candidate : ARJUN ADHITHYA E , RA2111003010583</td></tr>
<tr><td>9</td><td>Name and address of the Supervisor / Guide</td><td>Dr.Akilandeshwari ,
Associate Professor,
Department of Computing Technologies,
Faculty of Engineering &Technology,
SRM Institute of Science and Technology ,
Kattankulathur , Chengalpattu -603203
akiland@srmist.edu.in , +91 9443215112</td></tr>
<tr><td>10</td><td>Name and address of Co-Supervisor / Co- Guide (if any)</td><td>NIL</td></tr>
</table>

11	Software Used	Turnitin		
12	Date of Verification	09/05/2025		
13	**Plagiarism Details: (to attach the final report from the software)**			
Chapter	**Title of the Chapter**	**Percentage of similarity index (including self citation)**	**Percentage of similarity index (Excluding self citation)**	**% of plagiarism after excluding Quotes, Bibliography, etc.,**
1	INTRODUCTION	1	1	1
2	LITERATURE SURVEY	1	1	1
3	TECHNICAL SPECIFICATIONS	0	0	0
4	ARCHITECTURE	0	0	0
5	MODULES	0	0	0
6	PROJECT DEMONSTRATION AND RESULTS	1	1	1
7	CONCLUSION & FUTURE ENHANCEMENTS	1	1	1
8				
9				
10				
Appendices		4	4	4

I / We declare that the above information have been verified and found true to the best of my / our knowledge.

Signature of the Candidate	**Name & Signature of the Staff (Who uses the plagiarism check software)**
Name & Signature of the Supervisor/ Guide	**Name & Signature of the Co-Supervisor/Co- Guide**

Name & Signature of the HOD