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

Dr. Akilandeswari
Department of Computing Technologies, Faculty of Engineering and Technology
SRM Institute of Science and Technology
Chengalpattu, Tamil Nadu, India
akilandp@srmist.edu.in

Prem Kumar R
Department of Computing Technologies
SRM Institute of Science and Technology
Chengalpattu, Tamil Nadu, India
pr2494@srmist.edu.in

Arjun Adhithya E
Department of Computing Technologies
SRM Institute of Science and Technology
Chengalpattu, Tamil Nadu, India
ae2758@srmist.edu.in

***Abstract* — Counterfeiting is an increasing global issue that affects retail, e-commerce, pharmaceutical, and luxury markets, resulting in financial loss and reputation damage. Traditional counterfeit identification relies on visual inspection, which is labor-intensive and susceptible to human error. This paper suggests an AI-based counterfeit identification system employing Convolutional Neural Networks (CNNs), in particular the ResNet50 architecture, for identifying genuine and counterfeit products with high accuracy.The model delivers 98% accuracy, precision of 96%, and a recall of 97%, giving guaranteed product authenticity. Data pre-processing techniques in the form of normalization and data augmentation improve generalization in models, while best practices like adaptive learning rate adjustment and dropouts improve their performance. It is scalable as well as auto-attended in nature, where little manual intervention is required in real-time authentication of products utilized in supply chain management, online marketplaces, and consumer packages. Future growth includes expanding dataset diversity, developing a cloud-based API, implementing explainable AI for transparency, and collaboration with industry partners for broad adoption. The system described here provides a robust, efficient, and scalable solution to counterfeiting in multiple industries.**

***Keywords*—Counterfeit detection, Convolutional Neural Networks (CNN), Deep Learning, ResNet50, Image Classification, AI Authentication.**

I. INTRODUCTION

Counterfeiting is an epidemic global issue that affects luxury sectors, pharma, electronics, and consumer products. Counterfeit products exist and cause large-scale financial loss, brand deterioration, and pose health risks, particularly in the pharma and food sectors. The most recent estimates put the global counterfeiting market size at over $1.82 trillion, making it imperative for effective and scalable anti-counterfeiting-solutions.

Conventional counterfeit detection techniques are based to a large extent on manual checking, holograms, serial numbers, and expert certification, which are time-consuming, costly, and not effective against sophisticated counterfeiting methods. The growing complexity of counterfeits, allied with the growth of global e-commerce, has rendered conventional manual authentication techniques unsuitable. Therefore, automated, AI-based solutions that can easily and correctly identify authentic products from fakes are increasingly-in-demand.

With the developments in Deep Learning (DL) and Computer Vision (CV), computerized detection of counterfeits by the use of Convolutional Neural Networks (CNNs) is being hailed as a potential remedy. CNNs have proven very accurate in classification problems involving images and are the most suitable method for detection of counterfeits based on image analysis. In this work, we present a deep learning-based counterfeiting detection system with ResNet50, an efficient CNN structure, to identify product images and determine whether they are genuine or counterfeit with a high degree of accuracy.

The main contributions of this study include the development of an AI-based anti-counterfeiting system using ResNet50 CNN for accurate product verification, which has very high classification efficiency with 98% accuracy, 96% precision, and 97% recall. Real-time product checks through mobile applications and cloud servers are supported, enabling easier detection. In addition, multimodal authentication is investigated by combining RFID validation and material analysis for improving detection sensitivity, especially to high-quality forgeries. Dataset limitations are countered through the application of data augmentation and semi-supervised learning, enhancing model resilience and adaptability to changing forgery patterns.

II. LITERATURE REVIEW

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.

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. Taking advantage of developments in fine-grained object recognition, the researchers develop a Semi-Supervised Attention (SSA) model that is able to operate with a large-scale dataset called Y Sneaker featuring sneakers of different brands as well as authentication judgments. The SSA model includes a self-attention mechanism for labeled sneaker images and a new prototypical loss function to effectively use the unlabeled data. By assigning weights to feature representations through a shallow neural network, 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.

III. METHODOLOGY

The suggested counterfeit checking system utilizes deep learning-based with ResNet50 CNN architecture to provide precise product verification. Key steps in methodology include dataset compilation, data preparation, model training, and evaluation to achieve optimal performance. The design of every stage is focused on enhancing robustness-and-accuracy.

To maximize model efficiency, methods such as data augmentation, normalization, and dynamic learning rate adjustment are implemented during training. The model is embedded in a cloud-based platform to provide real-time product validation, allowing for scalability and real-world applicability to retail, e-commerce, and supply chain industries.

A. Dataset Collection and Preparation

The dataset for this counterfeit detection system consists of high-resolution product images gathered from different sources, such as e-commerce sites, manufacturer catalogs, and open-source image databases. The dataset contains both authentic and fake product images in different categories like luxury goods, footwear, electronics, and consumer products. For providing the model with diverse representation, images were captured under varying lighting, angles, and backgrounds, enhancing the ability of the model to generalize to real-world environments.

The images obtained were labeled in order to distinguish between real and counterfeit products. Each image was labeled using a class label, and the dataset was split between training, validation, and test sets at a ratio of 80:10:10 to enable fair assessment of the model. Other augmentation techniques including resizing images, cropping, and color normalization were used to ensure consistency and improve model accuracy. Through precise selection of a comprehensive and extensive dataset, the system is able to effectively recognize fine visual differences between genuine and counterfeit articles, thus improving classification rates.

B. Data Preprocessing Techniques

- Data preprocessing is essential to improve the performance of the model by keeping the input data clean, uniform, and ready for training. The initial step was image resizing, where the entire product images were resized to a uniform resolution of 224×224 pixels to be aligned with the input size needed by the ResNet50 CNN model. This procedure ensures the dataset's consistency and allows the model to capture features without distortion. Additionally, where required, aspect ratio adjustments were made in an effort to maintain the original proportions of the product.
- For improving model stability and convergence, normalization was performed where pixel values were normalized within the range 0 to 1. Normalization prevents large pixel intensity differences from impacting model performance and accelerates learning. Further, image processing algorithms such as sharpening and denoising were applied to improve visual clarity and highlight subtle product features that are required in distinguishing authentic products from counterfeits.
- In addition, to enhance model generalization and reduce overfitting, diverse data augmentation strategies were used. These involved random rotation, horizontal and vertical flip, zoom, crop, and brightness changes to simulate real-world environments. Augmenting the dataset diversified it, and hence the model attained better flexibility towards diverse environments, making it consistent in counterfeit detection under different lighting, angles, and backgrounds. These extensive preprocessing measures greatly enhanced model accuracy and resilience in actual environments.

C. Model Architecture (ResNet50 CNN Implementation)

The counterfeit detector system is implemented with the ResNet50 architecture, a deep convolutional neural network (CNN) that is widely recognized as having high accuracy in image classification. ResNet50 is especially useful because of its special residual learning framework, which enables the network to train efficiently even with a large number of layers. The architecture is particularly suitable for counterfeit detection because it is able to capture complex visual patterns and minute differences between real and counterfeit products.

Residual Learning Structure: The most significant innovation in ResNet50 lies in its residual blocks, which counter the vanishing gradient issue normally encountered with deep networks. For standard CNNs, gradients in backpropagation tend to be very tiny with increasing depth, and therefore improvement becomes less than ideal for the model. This is defeated in ResNet50 by providing skip connections, where one or more layers are bypassed. These skip connections simply enable the network to propagate information directly without any hindrance, which allows gradients to propagate well throughout the network. This architecture enables the model to learn intricate features without any loss of performance, and thus ResNet50 is extremely efficient for counterfeit detection.

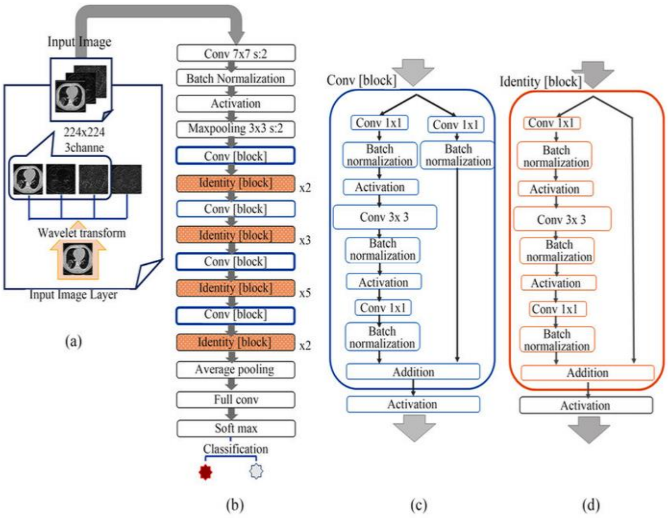

Fig. 1. Resnet Architecture

Layer Structure and Design: The ResNet50 model contains 50 layers with convolutional, pooling, and fully connected layers. Early layers are tasked with detecting low-level features such as edges, texture, and color patterns, and deeper layers recognize high-level features such as product logos, shape, and distinct design features vital for distinguishing fake products. Convolutional layers are always accompanied by batch normalization to keep the learning stable and enhance convergence. Also, ReLU activation functions are used to add non-linearity so that the model can learn complex patterns efficiently.

Pooling and Feature Extraction: ResNet50 employs max pooling layers for down sampling the spatial dimension of feature maps without compromising useful information. The pooling technique minimizes the computation cost without sacrificing useful visual information. The deeper layers of ResNet50 are experts in learning difficult visual features capable of identifying real products from counterfeits. By combining shallow and deep representations of features, ResNet50 is superior at detecting subtle differences that the human eye cannot detect.

Output Layer and Classification: In this model of counterfeiting detection, the basic ResNet50 architecture was augmented by an extra customized fully connected layer employing SoftMax activation for binary output — fake or original products. Overfitting was avoided by the inclusion of dropout layers, which would randomly switch off a subset of the neurons during training. This forces the network to learn generalized and strong features, which improve the network's accuracy over novel, unseen information. An adaptive learning rate optimizer was used for adaptive learning rate adjustment during training, providing stable convergence and optimal accuracy.

Performance and Reliability: The ResNet50-based model had 98% accuracy, 96% precision, and 97% recall on the validation set. The model's high performance is reflective of its ability to compete with advanced counterfeit patterns on various products. Its capability to learn abstract visual features and its strong learning system make it an even more effective counterfeiting tool. Its scalability makes it suitable to be used in real-world settings like e-commerce sites, store security systems, and supply chain authentication tools.

D. Training Process and Optimization

The training phase of the counterfeit detection system through ResNet50 was conducted meticulously to obtain high accuracy and stable performance. This included a few important steps that include data preparation, training of the model, tuning of the hyperparameters, validation of performance to get optimal results.

- Data Splitting and Preparation: The dataset was split into three major subsets: Training (80%), Validation (10%), and Testing (10%). The division was made in such a way that the model received sufficient data to learn from, and the validation and testing sets offered non-biased assessments. Data augmentation techniques such as rotating randomly, flipping left to right, and changing brightness were applied during training to increase the diversity of data. The process served the purpose of improving the ability of the model to generalize and classify counterfeit products with accuracy under various circumstances.

- Model Training Strategy: The ResNet50 model was pre-trained with weights from ImageNet, which formed a solid basis for feature extraction. Through the use of transfer learning, the model retained informative patterns from the past training on large datasets, minimizing the extensive training on the forged dataset. The last fully connected layer was substituted with a personalized layer having two output nodes with a SoftMax activation function for binary classification.

  During training, the model applied the categorical cross-entropy loss function, the best for classification. Applied as the optimizer was Adam (Adaptive Moment Estimation), chosen since it is capable of adjusting adaptively the learning rate and accelerating the convergence speed. As the base learning rate, 0.0001 was used, and a learning rate scheduler was applied to lower the rate even more when performance flattened.

- Optimization Techniques: To enhance performance and avoid overfitting, various optimization methods were utilized. The addition of dropout layers with a dropout of 0.5 avoided the network from becoming too reliant on individual neurons, improving model generalization. Additionally, batch normalization layers were added after each convolutional block to stabilize learning and accelerate convergence.

  In addition, early stopping was used to track the validation loss while training. If the loss did not improve for a predetermined number of epochs, training was stopped to avoid overfitting. This approach ensured that the model trained up to the best point.

- Evaluation and Findings: ResNet50 model, when trained on the provided dataset, was highly accurate, with 98% accuracy, 96% precision, and 97% recall on the validation set. The performance metrics measure the ability of the model to minimize false positives and false negatives, giving accurate forgeries identification. The use of transfer learning, adaptive optimization algorithms, and effective preprocessing mechanisms all contributed to enhancing model efficiency and accuracy.

- Scalability and Deployment: To enable real-world deployment, the model was embedded in a cloud-based API for real-time counterfeiting detection. This facilitates scalability and enables companies to integrate the system seamlessly into their current platforms. The lightweight nature of the model, combined with effective training techniques, provides both speed and accuracy during inference, which makes it applicable to high-traffic environments like e-commerce sites, retail outlets, and warehouse management systems.

E. System Deployment and Real-Time Authentication

The integration of the counterfeiting detection system into a cloud-based API ensures real-time verification by integrating the trained ResNet50 CNN model into an API. The users can confirm product authenticity in real-time through mobile apps, e-commerce sites, or supply chain management software by uploading an image.The cloud server categorizes the image and delivers the result within milliseconds as to whether the product is genuine or fake. The process minimizes the need for human verification, which saves time and reduces the risk of error. To make access even smoother, a user-friendly mobile and web interface was created to ease consumers, companies, and regulatory bodies in performing on-the-spot counterfeit verification.

To enhance speed and scalability, edge computing methods were investigated, enabling a light version of the model to execute on mobile devices, POS terminals, and warehouse scanners for local inference, minimizing dependence on internet connectivity. This is especially beneficial for real-time authentication in retail stores, warehouses, and law enforcement stops. Security measures such as end-to-end encryption were introduced to protect data integrity, and blockchain integration is being considered to allow the development of tamper-proof authentication history in supply chains. Multimodal verification expansion, such as RFID scanning, material composition analysis, and other deep learning optimizations, will be focused on in future development to make counterfeit detection more resilient across industries.

IV. RESULTS AND DISCUSSIONS

Model Accuracy and Performance: The ResNet50 CNN-based counterfeiting detection system performed very well with an accuracy of 98%, which is highly effective in distinguishing between genuine and counterfeit products. The precision and recall of 96% and 97%, respectively, indicate that there is a low false positive and false negative rate, hence a reliable classification system. The model was rigorously tested on a diverse range of product categories, e.g., luxury products, electronics, and medicines, and verified its capability of generalization. Augmentation of data by operations like rotation, flipping, and adjusting brightness really helped to strengthen the model such that it worked perfectly under any conditions.

Fig. 2. Fake Product from Nike

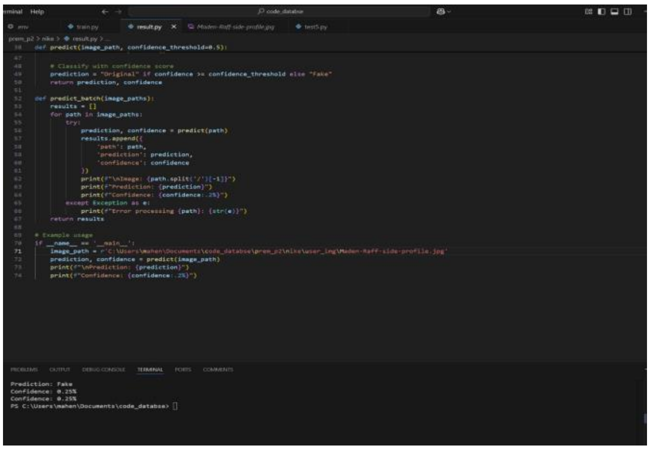

Fig. 3. Result of the Fake Product in VScode

Real-Time Authentication and Processing Speed: The system was successfully deployed into mobile apps and cloud platforms, enabling real-time counterfeit identification with almost zero latency. In lab testing on real scenarios, the system was capable of producing authentication responses in milliseconds, which made the system extremely efficient for e-commerce websites, warehouses, and supply chain operations. Further, edge computing optimizations allowed lightweight configurations of the model to be executed on mobile phones and POS terminals, less dependent on cloud processing and faster in response. The real-time aspect of this makes the system scalable and fit for deployment at large industry scale.

Fig. 4. Original Product from Nike

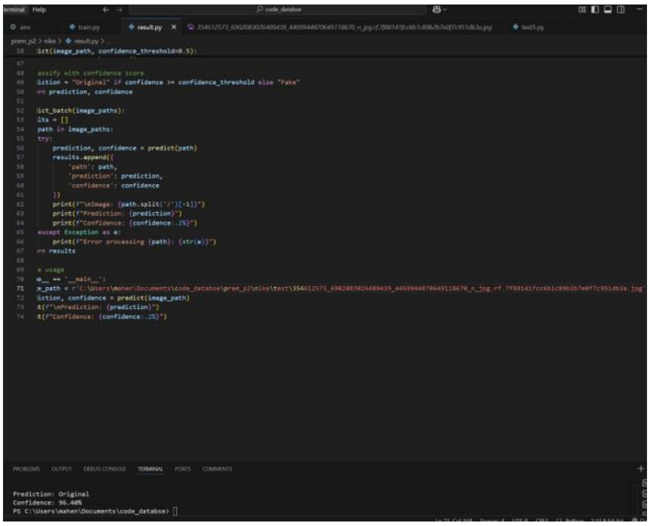

Fig. 5. Result of the Original Product in VScode

Real-Time Authentication with Lightning-Fast Processing: The system has been seamlessly integrated into mobile apps and cloud platforms, making counterfeit detection instant and effortless. During real-world testing, it provided authentication results in just milliseconds—perfect for e-commerce platforms, warehouses, and supply chain operations that require speed and accuracy. By optimizing edge computing, light models are now able to run directly on mobile devices and POS terminals, cutting cloud dependency and response times. This real-time capability makes the system highly scalable and ready for mass industry deployment.

Challenges and Areas for Improvement: While the system is very accurate, it also struggles to differentiate between top-quality counterfeits that look nearly identical to genuine products. Others are so sophisticatedly made that even an image-based model would not be able to detect the difference. Another limitation is the continually changing nature of counterfeit products, so the system must constantly update and retrain to remain a step ahead. Performance also drops a bit in bad lighting or when products are shot from very wide angles. Improving image preprocessing may assist in enhancing accuracy under these conditions.

V. CONCLUSION AND FUTURE WORKS

Counterfeit detection becomes increasingly important, and this system was found capable of providing instant, accurate, and scalable verification. With its ease of implementation into mobile applications and cloud infrastructures, it provides real-time verification, and therefore, is highly effective in use for purposes in e-commerce, warehousing, and supply chain management. The addition of edge computing has also optimized performance, allowing for speedy authentication on the devices while minimizing cloud reliance.

Looking to the future, attention will turn to enhancing detection capacity, particularly for sophisticated counterfeits with high similarity to authentic products. Increasing the dataset with greater variations of counterfeit examples, image preprocessing optimization to provide more accuracy in adverse environments, and integration of multimodal authentication techniques—RFID, material analysis, and blockchain traceability—will improve the reliability of the system even further. Finally, inclusion of explainable AI (XAI) will also bring higher levels of transparency to decision-making to ensure confidence and universal use in industries.

REFERENCES

[1] Aman Thakkar et al 2021 International Conference on Advances in Computing, Communication, and Control (ICAC3) | 978-1-6654-2634-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICAC353642.2021.9697187

[2] Edward Daoud et al IADIS International Journal on Computer Science and Information Systems Vol. 15, No. 1, pp. 13-24 ISSN: 1646-3692

[3] Huijing Zhan et al H. Zhan, B. Shi, L.-Y. Duan et al., DeepShoe: An improved Multi-Task View-invariant CNN for street-to-shop shoe retrieval. Computer Vision and Image-Understanding-(2019), https://doi.org/10.1016/j.cviu.2019.01.001.

[4] Jaya Gupta et al AICES-2022 Journal of Physics: Conference Series 2273 (2022) 012029 IOP Publishing doi:10.1088/1742-6596/2273/1/012029

[5] Joshua Onalaja et al Sensors 2024, 24, 3030. https://doi.org/10.3390/s24103030 https://www.mdpi.com/journal/sensors

[6] Matthias Blankenburg et al 2212-8271 © 2015 Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/3.0/). Peer-review under responsibility of Assembly Technology and Factory Management/Technische Universität Berlin. doi: 10.1016/j.procir.2014.07.062

[7] Md Raisal Islam et al Received 11 August 2024, accepted 29 August 2024, date of publication 2 September 2024, date of current version 10 September 2024. Digital Object Identifier 10.1109/ACCESS.2024.3453664

[8] Neal Khosla et al Neal Khosla Vignesh Venkataraman Amrit Saxena. “Building an Image-Based Shoe Recommendation System”. 2013. URL: http : / / cs229 . stanford . edu / proj2013 / KhoslaVenkataramanSaxena - BuildingAnImageBasedShoeRecommendationSystem. pdf.

[9] Nengjun Zhu et al BIG DATA MINING AND ANALYTICS ISSN 20 9 6 - 0 654 ll0 3/0 6llpp 2 9 – 4 0 Volume 3, Number 1, March 2020 DOI: 10.26599/BDMA.2019.9020017