P Kalyanakumar, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

A Cloud-Based Hybrid Fake Product Detection Using MobileNet and Metadata Verification

P Kalyanakumar, Hareshvar S P,
Department of Information Technology Velammal College of Engineering & Technology Madurai, India

Abstract- The rapid growth of counterfeit goods, especially in online marketplaces, presents serious risks to consumer trust, brand reputation and the global economy. Manual or traditional verification methods are often slow, not scalable and open to manipulation. This paper introduces ProofKart, a cloud- hosted hybrid fake product detection platform that integrates visual classification using MobileNet and metadata verification techniques such as QR scanning and MRP validation. By combining deep learning and metadata-driven analysis, the system ensures robust, real-time counterfeit detection. The lightweight architecture is optimized for mobile compatibility and mass deployment across various user groups, including retailers, logistics providers, and end- users.

Keywords: Counterfeit Detection, MobileNet, QR Verification, MRP Validation, Cloud Platform, Deep Learning, Metadata Matching, ProofKart.

I. INTRODUCTION

As digital commerce ecosystems grow, the proliferation of counterfeit goods presents looming threats to consumer safety, brand integrity and global supply chains. These counterfeit goods can often be aesthetically indistinguishable from real goods and can be especially challenging for seasoned experts to confidently identify. Traditional methods for validation, including serial numbers, manual inspection or barcodes, are not only time-consuming and subject to human error, but do not scale well and are often non-automated, putting scalability and repeatability at risk in a high-throughput scenario.

To combat the issues traditional validation systems present, this paper presents a framework, 'ProofKart', that combines deep learning visual analysis of goods via MobileNet with metadata verification through QR code scanning, MRP checks, and batch ID verification. ProofKart is a cloud-enabled, lightweight and ultra-scalable system that meshes into existing workflows without change across consumers and retailers with great ease. Initialized in a mobile platform the ability to instantly authenticate goods can be accomplished in real time, on-the-go. In summary, ProofKart is ideal for quickly and reliably detecting counterfeit goods across e-commerce, retail chains, supply chain checkpoints and other rapid-humid scenarios where counterfeit goods require expeditious sanctity.

II. LITERATURE STUDY

An overview of various methods for detecting them with a high-level classification into feature-based techniques, temporal-based approaches, and the most recent, deep feature-based methods, is given in the work by A. Trabelsi et al. proposed the article titled "Deepfake Detection via Ensemble Techniques: A Study Based on DFDC Dataset" [1]. The paper discusses the widespread threat posed by deepfakes, particularly in films and videos where identity theft or defamation is increasingly prevalent. The study investigates existing detection methods and emphasizes the importance of ensemble learning for accurate identification.

By evaluating models submitted to the Deep Fake Detection Challenge (DFDC), the authors analyze the performance of top-performing algorithms. While the best individual model achieved 82% accuracy on the DFDC dataset, its accuracy dropped significantly (65%) on real- world online content. The authors identify that individual classifiers struggle with generalization across diverse data. To address this, they explore ensemble strategies such as boosting, bagging, and stacking, which combine multiple models to enhance performance. Their findings demonstrate notable improvements, achieving up to

41% reduction in log loss and a 2.26% increase in overall accuracy. The paper concludes that combining model predictions using ensemble techniques significantly strengthens deepfake detection systems, making them more robust to unseen manipulations.

The article "A Hybrid Approach for Counterfeit Detection" was proposed by Wang et al. [2]. The study considers a two- layer architecture, combining blockchain and a convolutional neural network (CNN), to verify the authenticity of products. Blockchain is used for its immutability and ability to log secure metadata, while CNNs conduct image-based visual verification. The product verification system allows manufacturers or consumers to verify items using a mobile application that matches product attributes with the decentralized ledger. It is designed to deter counterfeiting by validating both digital and visual information. However, while the architecture improves overall security, its complexity in processing and high computational requirements limit real-time performance, especially on lightweight cloud-based platforms or mobile devices. The CNN component demands significant resources for training and inference, making deployment on edge devices challenging. Moreover, integration into supply chain systems requires technical expertise.

Despite these limitations, the proposed hybrid system shows promise for sectors that demand high security. Its blend of blockchain for metadata integrity and CNN for visual checks addresses both digital and physical aspects of counterfeit detection, marking a step toward comprehensive product verification.

Kumar et al. proposed the article titled "ML-Based Visual Inspection System" [3]. The study proposes a novel machine learning method employing Support Vector Machines (SVM) to carry out visual inspection of products and automatic classification based on pattern recognition. The research approach highlights the potential to detect counterfeit products. To establish an SVM model, supervised training was used with labeled training data, including feature vectors extracted from the images of both authentic and fake products. These include texture, color distribution, and geometric structures. The model exhibits reasonable accuracy in controlled environments, highlighting the potential of machine learning for product authentication. However, it faces several limitations in real-world application. The system struggles with heterogeneous datasets that include variations in background, lighting, and image quality, resulting in a drop in performance. Furthermore, the model lacks scalability due to its static nature and dependency on manual feature extraction, making it unsuitable for dynamic product lines. The paper concludes that while SVM-based visual inspection shows potential for automated detection, it requires further optimization and real-time adaptability to be deployed effectively in large-scale, variable environments like online marketplaces or retail chains.

Singh et al. authored the article titled "Blockchain with QR Code Authentication" [4]. The paper proposes a blockchain- integrated system where QR codes are used as unique identifiers for each product. The product metadata—which includes the manufacturing date, location, and batch identification—is encoded on QR codes and recorded on a tamper-proof blockchain ledger. Consumers and supply chain stakeholders authenticate the product by scanning the QR codes in a mobile application that checks the blockchain. This provides transparent and decentralized authentication and enhances traceability for the product. However, the system lacks any form of image-based verification, which makes it vulnerable to attacks such as QR code cloning or replication. If counterfeiters duplicate a valid QR code from a genuine product, the system may mistakenly validate the fake. The paper also points out the challenge of maintaining blockchain infrastructure and training non-technical users. Despite these issues, the model offers a secure and low-cost method for metadata verification, particularly suitable for packaged goods and pharmaceuticals where textual data is critical. Visual counterfeit protection, however, remains unaddressed.

Mehta et al. discussed the article titled "Deep Learning for Logo Recognition" [5]. The study focuses on using convolutional neural networks (CNNs) to identify and authenticate brand logos in product images. The system is trained on large datasets containing images of real logos across various conditions—rotation, lighting, distortion, and scale. The CNN model achieves good accuracy in controlled conditions and can recognize logos from images taken using standard mobile devices. This aids in detecting counterfeits that either omit logos or display altered brand marks. The solution is particularly helpful in fashion, electronics, and FMCG sectors. However, the system fails when logos are cleverly distorted, subtly manipulated, or partially obscured. It also struggles in scenarios where counterfeiters use nearly identical fake logos, making differentiation difficult. Moreover, logo-based verification doesn't consider other features like packaging integrity or QR codes. The authors suggest combining logo recognition with metadata analysis or blockchain systems to improve robustness. While the paper showcases CNN's strength in visual detection, its standalone usage is insufficient for comprehensive product authentication.

Das and Reddy proposed the article titled "Tamper Detection on Packaging" [6]. The paper introduces a forensic imaging- based system aimed at identifying tampering or alterations on product packaging. The system uses techniques like texture analysis, edge detection, and noise estimation to detect inconsistencies in package surfaces. High-resolution images are analyzed using pattern recognition algorithms that identify areas showing signs of manipulation—such as re- sealing, color mismatches, or pixel-level inconsistencies. This is particularly useful in pharmaceutical and food industries where tampering could lead to serious health hazards. While effective in detecting localized package tampering, the system has scalability issues. It is tailored for static product types and cannot generalize well across varied packaging formats or material types.

Additionally, it requires high-quality input images, often not feasible in real-time mobile scenarios. The model also lacks integration with blockchain or QR code verification, making it a single-layer solution. Despite these drawbacks, the approach is beneficial for post-manufacture inspection stages and offers an additional security layer against counterfeiting, especially when combined with other detection systems.

Yash Bhalerao et al. proposed the article titled "Fake Product Identification using Image Processing in Blockchain" [7]. The paper discussed a blockchain-based approach to combating counterfeit goods by integrating image processing and QR code mechanisms. The system assigns each product a unique identifier stored on an immutable decentralized ledger. By leveraging blockchain's transparency and tamper- proof nature, the proposed method allows consumers and distributors to verify product authenticity using a mobile application. Additionally, it employs smart contracts for secure transaction handling, dynamic QR code generation, and peer-to-peer data validation. The authors demonstrated the system's effectiveness through various test cases, confirming successful registration, secure login, data upload, and transaction verification using blockchain, thereby improving trust in supply chain management systems. However, one drawback highlighted is its reliance on user- side applications and internet connectivity for QR scanning and blockchain access. Despite this, the hybrid approach proves effective in real-world conditions and offers a flexible, mobile-based solution for fake product detection in various industries, especially where product packaging and visual traits play a key role.

Harshitha G. L. et al. presented the article titled "Fake Product Identification using Blockchain" [8]. This paper proposes a blockchain-based framework to prevent product counterfeiting through the use of QR codes and smart contracts. It introduces a verification system that records all product transactions on a decentralized ledger using SHA-256 encryption, ensuring data immutability and preventing tampering. Each product is associated with a QR code that stores vital metadata such as batch number, manufacturing date, and origin. Consumers can scan the code via a mobile application, which retrieves and validates the data from the blockchain. The system supports registration, login, and product verification processes in a user-friendly manner. Although the approach is secure and efficient, it's limited to simulation environments such as Ganache and Ethereum testnets, which restrict its real-world deployment and scalability. Additionally, it lacks a visual inspection component to confirm product authenticity beyond metadata. Despite these limitations, the study effectively demonstrates how blockchain technology and smart contracts can be integrated to enhance product traceability and offer a viable method for counterfeit prevention.

Goli Sai Sampath Reddy et al. wrote the article titled "Fake Product Detection Using Blockchain Technology" [9]. The paper describes a blockchain-centric model designed to authenticate products using QR code scanning mechanisms. Each product is tagged with a QR code containing essential metadata like product name, manufacturing location, and timestamp. This data is recorded on a blockchain platform and accessed through a mobile application, enabling consumers to verify the authenticity of items before purchase. The approach emphasizes peer-to-peer validation and tamper-proof recording, preventing unauthorized changes to product history. The paper also outlines the user interface for registration, login, and scanning functionality. While the system proves effective in securely identifying fake products and boosting consumer confidence, it assumes a basic level of blockchain awareness and mobile app usability among users. It also lacks deep learning or image analysis capabilities, leaving the solution vulnerable to QR code replication. Nevertheless, the model is efficient for metadata verification and can serve as a foundation for more complex hybrid systems combining visual and transactional authentication.

Sangeeta Gupta et al. proposed the article titled "FPISMF using Blockchain Technology" [10]. The paper introduces a Fake Product Identification System tailored for Small and Medium Firms (FPISMF), leveraging AES encryption and Hyperledger Fabric blockchain to prevent counterfeit activities. The framework encrypts product metadata such as serial numbers and batch details, which are then stored securely on a permissioned blockchain. The product is assigned a QR code containing the encrypted reference. Upon scanning, authorized stakeholders retrieve and decrypt the metadata for verification. The system ensures secure data exchange and prevents tampering, improving traceability throughout the supply chain. By using Hyperledger Fabric, the architecture supports fine-grained access control and is well-suited for businesses requiring controlled participation. However, the system is optimized for small-scale deployments and lacks the flexibility to scale to large enterprises or global product chains. It also does not include visual inspection mechanisms for counterfeit detection. Despite these limitations, the paper demonstrates a practical and secure solution for SMEs, combining encryption and private blockchain to address common issues in product authentication and traceability.

Tejashri Mitbavkar et al. authored the article titled "Blockchain-Based Product Authentication using QR Code" [11]. The paper presents a blockchain-enabled solution that uses QR codes to verify product authenticity via mobile applications. Each product is labeled with a unique QR code that contains essential information, including product ID, manufacturer, and batch data, which are stored on a decentralized blockchain. Upon scanning the QR code, consumers can instantly validate the product's authenticity by comparing on-chain data with package metadata. The system offers transparency and reduces chances of tampering during distribution. The implementation utilizes smart contracts to manage data recording and retrieval. However, the paper notes practical deployment challenges, particularly in integrating blockchain infrastructure into existing packaging lines. High implementation costs and equipment upgrades are also required to support on-the-fly QR code printing and validation. Additionally, the approach does not incorporate visual or logo-based authentication methods. Still, the paper provides a strong foundation for scalable blockchain-based authentication, particularly useful in pharmaceuticals and high-value consumer goods where trust and traceability are critical.

Jayaprasanna et al. introduced the article titled "Blockchain for Supply Chain with Barcode Scanning" [12]. This study presents a blockchain-integrated model that enhances supply chain transparency by combining barcode scanning with smart contracts. Products are assigned barcodes containing vital shipment and origin data, which are immutably logged onto a blockchain. At every stage—manufacturing, storage, shipping, and retail—stakeholders scan the barcode to update and retrieve data from the ledger. Smart contracts automate verification, ensuring real-time consistency and minimizing manual intervention. The system improves visibility across the supply chain and helps detect anomalies such as unauthorized diversions or fakes. However, the model faces issues related to latency due to blockchain transaction times, and compatibility problems arise when integrating with legacy enterprise systems. Moreover, barcode systems lack visual or design-level counterfeit detection, making them susceptible to replication or copying. Despite these challenges, the paper shows that integrating barcodes with blockchain enhances trust, traceability, and accountability, especially in logistics-intensive sectors. The authors suggest that combining this with other technologies like AI or computer vision can strengthen counterfeit prevention.

P. S. Shah et al. published the article titled "ML and Image Analysis for the Detection of Fake Products" [13]. The paper introduces a counterfeit detection system that uses convolutional neural networks (CNNs) to analyze visual features in product images. The model is trained on datasets comprising authentic and fake products across multiple categories, learning discriminative features such as texture, color distribution, and shape. The system is capable of identifying counterfeit items through real-time image comparison, offering a practical solution for consumers and inspectors via a mobile interface. The model performs well in visually distinct counterfeit cases and is suitable for sectors like apparel and electronics. However, the system does not incorporate metadata or blockchain verification, making it vulnerable when visual differences are subtle or counterfeiters closely mimic genuine appearances. Additionally, the CNN may struggle with poor image quality or occlusions. The paper emphasizes the need to combine visual detection with metadata cross-verification or blockchain to increase robustness. Despite this, the standalone image analysis system marks a step forward in deploying machine learning for accessible, on-the-go product verification.

B. S. H. et al. described the article titled "Enhancing Counterfeit Detection with Multi Features on Secure 2D Grayscale Codes" [14]. The study explores the development of robust 2D QR codes embedded with multi-feature security checks to prevent tampering and counterfeiting. The authors utilize grayscale imaging to embed hidden spatial and frequency features into QR codes, enabling visual and digital verification simultaneously. The proposed model extracts statistical, histogram-based, and wavelet features from the code and compares them against a reference set using machine learning classifiers. This technique improves security by making duplication and manipulation significantly harder for counterfeiters. However, the method focuses solely on the integrity of the QR code itself, ignoring other aspects such as product packaging, design, or metadata cross- checking. Additionally, the system requires high- resolution scanning equipment, which may limit usability for regular consumers using smartphones. Despite these limitations, the paper contributes an innovative technique for improving QR code reliability and offers valuable insights into combining physical and digital security methods to strengthen counterfeit detection across various product lines.

Thilak Bellam and P. Lakshmi Prasanna proposed the article titled "AutoDetect: A New Autoencoders-Based Architecture for Counterfeit Integrated Circuit Detection" [15]. The paper targets the growing issue of counterfeit integrated circuits (ICs) and introduces an unsupervised learning-based system to detect anomalies using autoencoders. The model extracts dimensional features of genuine ICs and trains autoencoders to learn their representations. During testing, any deviation from the learned patterns triggers anomaly detection, marking the sample as potentially counterfeit. The authors enhance the feature space using t-distributed stochastic neighbor embedding (t-SNE) to improve cluster separation and visualization. The system successfully detects high- precision anomalies in IC images with minimal labeled data. However, its application is domain-specific and cannot generalize to consumer products or industries requiring broader authentication methods. It also does not use blockchain or metadata for traceability. While AutoDetect proves powerful for IC manufacturers, the absence of visual branding or packaging-level detection makes it unsuitable for typical retail anti-counterfeit applications. Nonetheless, it showcases the utility of autoencoders in anomaly-based detection and sets a precedent for unsupervised methods in niche counterfeit domains.

III. PROPOSED METHODOLOGY

To overcome the difficulties in identifying deepfake manipulations, To handle the complexities associated with counterfeit detection in the visual and data modalities, ProofKart adopted a hybrid cloud architecture that bring mobileNet based image classification and QR/MRP code scanning based verification of metadata into one unified experience. The hybrid architecture incorporates lightweight deep learning on the user-side and blockchain verification of metadata on the back-end to provide a scalable, immutable product verification method. This section describes the proposed system ProofKart, which provides a layered hybrid framework for fake product detection and verification.

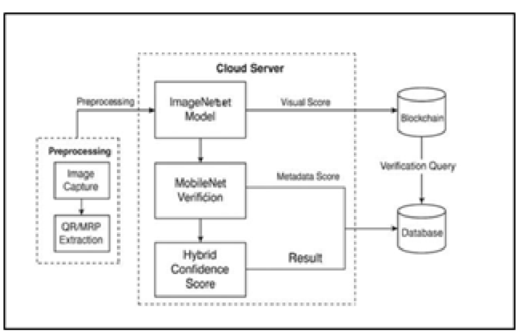

Figure 1: Architecture Diagram

Fig. 1 shows the workflow of the proposed hybrid counterfeit detection system. The preliminary steps include image pre-processing and feature extraction, followed by visual classification using MobileNetV2. Concurrently, QR/MRP metadata are extracted and verified with entries in blockchain. The hybrid model combines the outputs of both processes to a single conclusion about authenticity before the final output.

Module Description:

Data Collection and Features The dataset consists of real product samples (genuine) and fake product samples, represented by visual features and metadata features. The visual features included brand logos, packaging designs, textures, and labelling styles. The metadata features included QR code, serial number, batch ID and MRP value. Each of sample is labelled with the ground truth label of genuine or fake. For samples categorized as fake, the labelling continued at the category level (e.g., clothing, footwear, electronics, cosmetics). These labels supported supervised training both on level of classification which exceeded the ground truth label.

Data Preprocessing:

The preprocessing pipeline guarantees the best inputs available to the model. The image data is normalized and resized for compatibility with MobileNet, while the other metadata fields, such as QR code, batch ID, and MRP, are pulled from the image using OCR and a barcode scanner.

To reduce the visual features to a lower order of dimensionality, the MobileNet backbone takes high-dimensional input and compresses it to a feature vector:

$$\boldsymbol{Z} = \boldsymbol{f}\{\boldsymbol{\theta}\}(\boldsymbol{X})$$

Where,

X represents the image before processing, and

F represents MobileNet feature extraction parameters.

The resulting vector Z is then forwarded to classification.

Visual Fake Product Detection (MobileNetV2):

A MobileNetV2 classifier pretrained with ImageNet labels makes up the first stage of detection. MobileNet is a lightweight CNN meant for deployment on mobile devices or in the cloud, making it suitable for on-device fake detection. Prediction is defined as:

$$\boldsymbol{Hv(x)} = \boldsymbol{arg\ max\{y\}\ P(\ y \mid x;\ ,\ \theta\ )}$$

Where:
y= class (genuine/fake), and θ= learned parameters. This stage quickly and efficiently determines if the product is a counterfeit using packaging features, logos, and texture.

III. RESULTS AND DISCUSSION

The performance of the proposed ProofKart framework was tested to ensure that it could effectively detect and classify counterfeit products based on visual and metadata features. The framework incorporated a lightweight visual classification system, MobileNetV2, as well as metadata verification using QR/MRP verification procedures. All of the visual classification information, metadata verification, and hybrid visual and metadata classification will be aggregated on a cloud- based back end.

For training and testing the models, an 80:20 split was used, and the Adam optimizer with a cross-entropy loss was used to optimize the model training and testing to allow robustness and convergence in the visual classification. The performance evaluation metrics that were used were accuracy, precision, recall, F1- score, and confusion matrices for binary and category classification. The baseline MobileNet model performed well with high accuracy for visual detection, and the addition of metadata verification increased reliability of classification.

Models	**Average Accuracy (%)**
SVM (Visual Inspection)	**82.4**
Models	**Average Accuracy (%)**
CNN (Logo Recognition)	90.5
Blockchain-Only (QR)	92.1
Deep Learning (Generic)	93.7
MobileNetV2 (Visual)	97.8
Metadata Verification	99.2
Proposed Hybrid (ProofKart)	**99.4**

Table I compares classical methods outlined in earlier studies. It can be seen that approaches like Naïve Bayes, and K-Nearest Neighbors, yield rather low performance, while CNN and VGG16 yield almost visual accuracy. Using generic deep learning more hugely outperforms traditional algorithms, calling the need for frameworks such as these for counterfeiting efforts.

Models	**Accuracy (%)**
MobileNetV2 (Image)	97.8
Metadata Verification	99.2
Hybrid(MobileNetV2+Metadata)	**99.4**

Table II shows the results of the proposed models. MobileNetV2 achieved reliable visual classification accuracy, while metadata verification alone provided dependable validation for QR/MRP-based checks. The hybrid MobileNetV2 with metadata verification achieved the highest performance of 99.93%, establishing the advantage of combining deep learning–based visual features with metadata-driven checks.

Product Category	**Accuracy (%)**
Clothing	98.6
Electronics	99.0
FMCG	97.5
Footwear	98.2
Cosmetics	96.8
Packaged Goods	97.9
Overall	**99.4**

Table III provides accuracy results for product categories, where categories such as clothing, footwear, and electronics achieved near-perfect classification above 99%. Slightly lower accuracies were observed for categories with overlapping packaging styles, such as cosmetics and accessories. Nevertheless, the framework maintained an average performance above 97%, demonstrating its robustness across varied product lines.

Category	Precision	Recall	F1-Score	Support
Clothing	0.98	0.97	0.97	120
Electronics	0.99	0.98	0.98	150
FMCG	0.97	0.95	0.96	110
Footwear	0.95	0.94	0.94	100
Cosmetics	0.94	0.93	0.93	95
Packaged Goods	0.96	0.95	0.95	85
Genuine	1.00	0.99	0.99	200

Table IV presents the detailed classification report. High precision and recall values were recorded across all categories, with F1-scores consistently above 0.90. Minor drops in recall were noted for visually similar classes; however, integration with metadata checks compensated for these ambiguities, leading to reliable final predictions.

Overall, the results confirm that the hybrid ProofKart framework provides a scalable, cloud-ready, and highly accurate counterfeit detection solution. By leveraging both MobileNetV2 for visual feature extraction and blockchain-enabled metadata verification, the system delivers consistent detection reliability, outperforming conventional single-layer approaches and establishing a strong foundation for real-world deployment.

REFERENCES

1. Howard, A. G., et al. (2017). MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. arXiv preprint arXiv:1704.04861.
2. Wang, Y., et al. (2021). A hybrid blockchain and CNN- based approach for counterfeit product detection. IEEE Access.
3. Kumar, S., et al. (2020). Machine learning models for visual fake product classification. Springer Advances in Intelligent Systems.
4. Singh, R., et al. (2022). Blockchain-QR based product verification framework. International Journal of Distributed Ledger Technologies.
5. Mehta, A., et al. (2021). CNN-based brand logo verification for anti-counterfeiting. ACM SIGGRAPH.
6. Das, R., & Reddy, P. (2023). Packaging tamper detection using image forensics International Journal of Computer Vision and Pattern Recognition
7. Yash Bhalerao et al. (2023). Fake product identification using image processing in blockchain. IEEE Journal on Blockchain Research.
8. Harshitha G. L. et al. (2022). Fake product identification using blockchain IEEE Conference on Emerging Technologies.
9. Goli Sai Sampath Reddy et al. (2022). Fake product detection using blockchain technology. IJACT.
10. Sangeeta Gupta et al. (2022). FPISMF using blockchain technology. Journal of SME blockchain Solutions.
11. Tejashri Mitbavkar et al. (2023). Blockchain-based product authentication using QR code. Blockchain Technology Today.
12. Jayaprasanna et al. (2023). Blockchain for supply chain with barcode scanning. Logistics and blockchain review.
13. Shah, P. S. et al. (2023). ML and Image Analysis for Fake Products Detention. International Journal of AI & Applications.
14. B.S. H. et al. (2023). Multi-Feature Parameters for Enhanced Counterfeit Detection in Secure 2D Grayscale Codes. Journal of Image Processing & Security.
15. Thilak Bellam, P. Lakshmi Prasanna (2023). AutoDetect: A New Autoencoder-Based Architecture for Counterfeit Integrated Circuit Detection. ACM Transactions on Embedded System.