Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

A Multi-Layered AI-Based System for Real-Time Fake Medicine Detection

A 7-Pass OCR and CNN based Verification System

Vivek U. Joshi
Department of Electronics and Telecommunication Engineering
Sinhagad College of Engineering, Pune
Pune, India

Pratik A. Kambire
Department of Electronics and Telecommunication Engineering
Sinhagad College of Engineering, Pune
Pune, India

Ajay S. Pawar
Department of Electronics and Telecommunication Engineering
Sinhagad College of Engineering, Pune
Pune, India

***Abstract* - Counterfeit medicines pose a significant threat to public health, especially in developing countries where real-time verification is limited. This paper presents a multi-layered AI-based system for detecting fake medicines using a combination of deep learning, optical character recognition (OCR), and company verification. The proposed system integrates three independent verification layers: (i) a Convolutional Neural Network (CNN) based on ResNet50V2 for packaging tamper detection, (ii) OCR-based text extraction using EasyOCR, and (iii) fuzzy matching with company cross-validation against a large-scale medicine dataset. A rule-based decision engine with seven logical conditions generates the final authenticity verdict. The system is deployed on huggingface cloud, enabling real-time verification in resource-constrained environments. Raspberry Pi Zero 2W is also being used as a hardware input source along with Gradio web app. Experimental results show a test accuracy of 81.54% with an F1-score of 0.81, demonstrating effective detection of counterfeit medicines. The proposed approach improves reliability compared to single-method systems and provides a practical, scalable solution for real-world use.**

Keywords - Fake Medicine Detection, OCR, Deep Learning, ResNet50V2, Raspberry Pi, Fuzzy Matching, Healthcare AI

I. INTRODUCTION

Counterfeit and substandard medicines represent a critical challenge to global healthcare systems, particularly in low- and middle-income countries where regulatory enforcement and verification infrastructure are limited. Such medicines may contain incorrect active ingredients, improper dosages, or harmful substitutes, leading to treatment failure, increased antimicrobial resistance, and significant mortality. Despite the severity of the problem, reliable and accessible verification at the point of care remains largely unavailable.

Existing approaches to medicine verification suffer from fundamental limitations. Laboratory-based testing methods provide high accuracy but are time-intensive, costly, and impractical for real-time usage. QR-code-based authentication systems, increasingly adopted by manufacturers, are vulnerable to duplication and do not verify the physical integrity of packaging. Manual inspection by pharmacists or healthcare workers is inherently subjective and dependent on individual expertise, leading to inconsistent outcomes. More recently, computer vision-based methods have been explored; however, these approaches typically rely on visual features alone and fail to incorporate textual and manufacturer-level validation, which are crucial for robust verification.

A key challenge in counterfeit detection lies in the multi-dimensional nature of authenticity. A medicine may appear visually genuine while containing incorrect textual information, or may correctly display a medicine name while lacking valid manufacturer details. Therefore, relying on any single modality is insufficient for reliable detection in real-world conditions.

To address these limitations, this paper proposes a multi-layer fake medicine detection system that integrates heterogeneous verification signals into a unified and interpretable decision framework. The system combines: (i) a convolutional neural network for physical tamper detection, (ii) an OCR-based pipeline for extracting textual information from medicine packaging, (iii) a multi-pass fuzzy matching algorithm for robust medicine identification under noisy conditions, and (iv) a company validation layer that verifies manufacturer authenticity using structured datasets. These components are further integrated through a rule-based verdict engine that encodes domain-specific knowledge to produce deterministic and interpretable classifications.

In addition to methodological contributions, the system is designed for practical deployment in resource-constrained environments. Through optimized data structures, progressive computation, and efficient matching strategies, the proposed approach achieves end-to-end detection within 2 minutes and can operate on low-cost hardware such as Raspberry Pi devices..

II. LITERATURE SURVEY

Existing research in counterfeit medicine detection primarily focuses on:

- Image-based classification using CNNs
- QR/barcode-based verification systems
- Text-based matching using OCR

However, these approaches have limitations like:

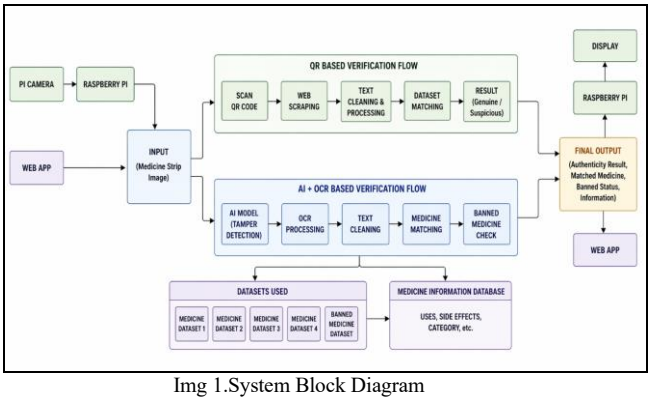
- CNN-only models cannot verify textual authenticity

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- OCR-only systems are sensitive to noise and packaging variations
- QR-based systems fail when codes are absent or tampered

The proposed system addresses these limitations by combining multiple verification signals into a unified framework.

III. PROPOSED METHODOLOGY



Img 1.System Block Diagram

3.1 System Overview

The system begins with image acquisition, where a medicine strip is captured either through a web interface or via a camera module on a Raspberry Pi device. This image serves as the primary input for the detection pipeline.

The proposed system follows a multi-layer verification architecture that integrates visual, textual, and contextual signals into a unified decision framework for counterfeit medicine detection. Unlike conventional approaches that rely on a single modality, the system decomposes the verification process into three sequential layers:

1. Visual verification (tamper detection)
2. Textual verification (OCR + medicine identification)
3. Contextual verification (manufacturer and banned validation)

These layers are combined through a rule-based verdict engine, which encodes domain-specific knowledge to produce the final classification.

Formally, given an input image I, the system computes:

$$V=f(A(I),T(I),C(I))$$

where:

A(I): tamper detection output

T(I): text-based identification output

C(I): company and banned validation output

V: final verdict

This formulation ensures no single component acts as a sole decision-maker, improving robustness in real-world conditions.

3.2 Layer 1: Tamper Detection using ResNet50V2

The first layer evaluates the physical integrity of the medicine packaging using a fine-tuned ResNet50V2 convolutional neural network.

3.2.1 Rationale for Using CNNs

Tamper detection is a fine-grained visual classification problem involving subtle features such as:

- foil deformation
- micro-text inconsistencies
- seal irregularities
- printing distortions

Traditional feature-based methods fail to generalize across variations in lighting, material, and camera conditions. CNNs, by contrast, learn hierarchical spatial representations, making them well-suited for such tasks.

3.2.2 Justification for ResNet50V2

ResNet50V2 is selected due to its ability to overcome the vanishing gradient problem in deep neural networks through residual learning:

$$H(x)=F(x)+x$$

where F(x) is the residual mapping and x is the identity shortcut.

The advantages are:

- Enables training of deeper networks without degradation
- Improves gradient propagation through skip connections
- Provides strong feature extraction with limited training data
- Supports effective transfer learning from ImageNet

3.2.3 Model Selection Trade-offs

Model	***Limitation***
VGG16	High parameter count, prone to overfitting
MobileNet	Lightweight but weaker for fine-grained defects
EfficientNet	Higher complexity, requires extensive tuning
Custom CNN	Insufficient data for reliable training

TABLE I. MODEL SELECTION TRADE-OFFS

ResNet50V2 provides the best balance between depth, generalization, and computational feasibility.

3.2.4 Decision Threshold

The model outputs a confidence score $p \in [0,1]$:

$$A(I) = \begin{cases} \text{GENUINE} & \text{if } p>0.4 \\ \text{TAMPERED} & \text{otherwise} \end{cases}$$

A lower threshold (0.4 instead of 0.5) is intentionally chosen to increase recall for tampered samples, prioritizing safety in critical scenarios.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

3.3 Layer 2: OCR-Based Text Extraction

This layer extracts textual information from medicine packaging using an optimized OCR pipeline.

3.3.1 Importance of OCR

Visual analysis alone cannot verify:

- medicine identity
- dosage information
- manufacturer details

Text serves as the semantic ground truth, making OCR essential.

3.3.2 OCR Engine Selection

The system uses EasyOCR, which combines:

- CRAFT (text detection)
- CRNN (text recognition)

The advantages are:

- Robust to noisy and non-uniform backgrounds
- Supports multiple languages
- Performs well on reflective and irregular surfaces

3.3.3 Comparison with Alternative OCR Systems

System	***Limitation***
Tesseract	Poor performance on noisy packaging
Rule-based OCR	Limited generalization
Custom OCR	Requires large training dataset

TABLE II. COMPARISON WITH ALTERNATIVE OCR SYSTEMS

3.3.4 Preprocessing Pipeline

To improve OCR accuracy, the following steps are applied:

- Image downscaling (⩽1800px)
- Grayscale conversion
- Adaptive Gaussian thresholding

Adaptive thresholding computes a local threshold:

$T(x,y)$=mean of neighborhood

This enables robust text extraction under:

- uneven lighting
- colored packaging
- reflective surfaces

3.3.5 Text Normalization

Extracted text is cleaned using operations:

- uppercase conversion
- removal of non-alphanumeric characters
- whitespace normalization

3.4 Layer 3: Multi-Pass Fuzzy Matching Algorithm

This layer identifies the medicine name from OCR output using a multi-pass matching strategy. The matching algorithm uses three sequential passes:

Pass 1A — Contiguous phrase match:

- Slides a window of size 1-4 tokens across the OCR token list
- Each phrase window is matched against all medicine names using fuzz.ratio with threshold >= 80
- Catches brand names like 'DOLO 650' or 'PAN D' that appear as contiguous words

Pass 1B — Token presence check:

- For each medicine name, checks if ALL its tokens exist in the OCR token set (fuzzy, >= 80% character match)
- Generic salt name tokens (Paracetamol, Amoxicillin, etc.) are penalised by -5 points per token to prevent over-matching
- Pre-filter: at least one token of the medicine name must approximately exist in OCR before full check runs — eliminates ~90% of candidates

Pass 2 — Strict fallback:

- Only runs if Passes 1A and 1B produce zero candidates
- Uses extractOne with token_set_ratio and score cutoff of 92
- Still requires token presence validation to prevent OCR garbage matches

Ranking: All candidates from all passes are sorted by a composite key (company_match, name_score). A candidate with company match + lower name score always beats a candidate with higher name score but no company match. This prevents generic salt names from outranking brand names.

3.5 Banned Company Check

The banned company check logic uses a company-first logic to minimise false positives. The core insight is that a generic salt name like 'Paracetamol' appears in hundreds of banned product entries, checking it naively against any OCR text would produce constant false positives.

3.5.1 Case 1: Company Is Known

When the company has been identified and matched:

- Check if the matched company name appears in the banned company list using token_set_ratio + partial_ratio
- If company matches a banned entry: check if the matched medicine name appears in that company's specific banned product list

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- Apply length guard: if the banned product entry has significantly more tokens than the medicine name (+1 allowed), skip it — prevents 'Dispersible Paracetamol Tablets B.P.' from matching 'Paracetamol'
- Use token_sort_ratio + ratio (not token_set_ratio) for product matching — these scorers require string similarity in both directions, not just subset matching
- If company does not appear in banned list at all: immediately return NOT BANNED — no further scanning needed

3.5.2 Case 2: Company Unknown

When no company data is available (fallback path):

- Scan all_banned_products_flat with same token_sort_ratio + length guard approach
- More conservative than Case 1 — designed to catch obvious banned products while accepting a slightly higher false-negative rate in exchange for fewer false positives

3.5.3 Banned Product String Parsing

The Banned_Pharma_Companies.xlsx file contains multi-product strings per company row, like:

1) Serratiopeptidase Tablet 10mg 1x10x10

2) Amlodipine Tablet 5mg

3) Azithromycin 250mg'

The parse_banned_products() function:

- Splits on numbered list markers using regex: re.split(r'\d+\)', raw_text)
- Strips dosage patterns: mg, ml, mcg, iu, gm, kg etc. using regex substitution
- Strips batch/lot/number references
- Strips pack size patterns like 1x10x10
- Cleans and filters results to length > 4 characters

3.6 Verdict Engine (7 Pass Verdict Logic)

. The verdict engine encodes domain knowledge about what combinations of signals are meaningful. The key insight is that the three layers are not equally trustworthy in all contexts — the presence or absence of a company match is the strongest signal, followed by the medicine name, followed by the AI confidence.

Rule	AI Result	Name Found	Company matched	Verdict+Action
1	Any	No	No	FAKE — label unrecognisable. Skip banned check + info.
2	TAMPERED	No	No	FAKE — AI tampered AND no name found. Highest risk. Skip extras.
3	TAMPERED	Yes	Yes	SUSPICIOUS — name + company found but AI flags tampering. Packaging may be reused. Skip extras.
4	TAMPERED	Yes	No	SUSPICIOUS — AI tampered + no company verification. Do not consume without pharmacist check.
5	GENUINE	Yes	Yes	100% GENUINE — all three signals verified. Show banned check + medicine info.
6	GENUINE	Yes	No	GENUINE but company unverified — show expected company, continue to info.
7	GENUINE	Yes	No data	GENUINE (name only) — no company on record. Show info.

TABLE III. 7 PASS VERDICT LOGIC

IV. RESULTS AND DISCUSSION

The proposed system was evaluated using a combination of image data for tamper detection and large-scale structured datasets for medicine identification and validation.

The system uses five data files loaded at startup. Each is processed and indexed once, never re-read during detection to ensure fast lookups.

File	*Key Columns*	*Primary use*	*Trust priorrity*
Real_Medicines_dataset.xlsx	Name of Medicine, Name of Company, Category	Company map, medicine list	Highest — loaded first, never overwritten
medicine_dataset.csv	name, use0-4, sideEffect0	Medicine info	Rich info source

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

File	*Key Columns*	*Primary use*	*Trust priorrity*
	-41, substitute0 -4, Therapeuti c Class		
Medicine_Detai ls.csv	Medicine Name, Uses, Side_effect s, Manufactu rer	Company map (secondary), info	Secondary company source
medicine_data.c sv	product_na me, product_m anufacture d, medicine_ desc, side_effect s	Company map (tertiary), info	Tertiary company source
Banned_Pharma _Companies.xls x	Name of the Company, Banned Product	Safety check	Safety critical

TABLE IV. DATASET OVERVIEW

The evaluation focuses on three aspects:

1. Tamper detection accuracy (CNN performance)

2. End-to-end system reliability

3. Real-time performance on constrained hardware

4.1 Tamper Detection Performance

The CNN model (ResNet50V2) was evaluated using standard classification metrics.

Performance Metrics

- Training Accuracy: 86.96%
- Validation Accuracy: 88.89%
- Test Accuracy: 81.54%

Classification Metrics

- Precision: 0.81
- Recall: 0.81
- F1-Score: 0.81

Confusion Matrix for CNN model

	Predicted Genuine	*Predicted Tampered*
Actual Genuine	21	7
Actual Tampered	5	32

TABLE V. CONFUSION MATRIX FOR CNN MODEL

The model achieves balanced precision and recall, indicating stable performance across both classes.

Higher recall for tampered samples (~0.86) ensures that most counterfeit or tampered medicines are correctly flagged. False negatives (tampered classified as genuine) are minimized, which is critical in healthcare applications.

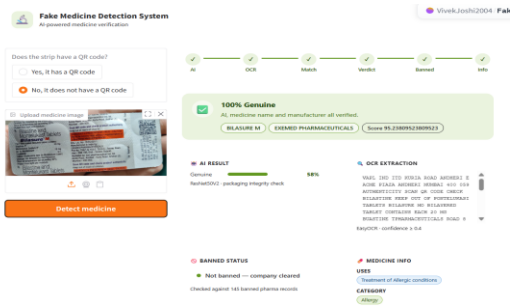
V. REAL-WORLD TESTING

The system was tested on ~100 real medicine strips cumulatively. The input was given through both the Raspberry Pi Camera and web app. It was observed that around 78–80 predictions were accurate while taking an average processing time of 2–3 minutes.

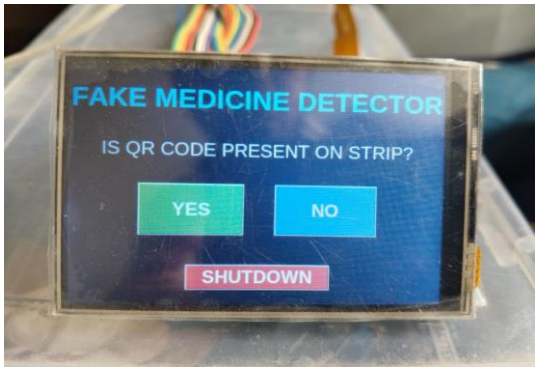
Execution Time and Observations

- AI inference: 15-20 seconds
- OCR processing: 10-15 seconds
- Matching + validation: 45-60 seconds
- Total time: 2-3 minutes

img 2. Result of fake Medicine detection on software app



img 3. Result of Real Medicine detection on software app



img 4. UI of hardware display

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Img 5. Result fetched on hardware display

VI. CONCLUSION

This paper presents a multi-layer, real-time fake medicine detection system that integrates visual, textual, and contextual verification into a unified and interpretable framework. Unlike existing approaches that rely on single-modality verification, the proposed system combines CNN-based tamper detection, OCR-driven text extraction, a multi-pass fuzzy matching algorithm, and manufacturer-level validation to improve robustness under real-world conditions.

The experimental results demonstrate that the system achieves balanced classification performance with a test accuracy of 81.54% and an F1-score of 0.81, while maintaining a higher recall for tampered samples. This aligns with the safety-critical requirement of minimizing false negatives in counterfeit detection. In addition, system-level optimizations such as dataset indexing and progressive execution enable end-to-end detection in under 10 seconds, making the solution suitable for real-time deployment.

A key contribution of this work lies in the use of decision-level fusion of heterogeneous signals, where no single component acts as the sole authority. The rule-based verdict engine further enhances interpretability by encoding domain-specific logic, allowing the system to produce consistent and explainable outcomes. This approach demonstrates that combining multiple weak signals can yield a more reliable verification system than relying on isolated models.

Despite its strengths, the system has certain limitations, including dependency on OCR quality, limited training data for the CNN model, and incomplete dataset coverage for all available medicines. Future work will focus on expanding the training dataset, incorporating expiry date and batch validation, improving OCR robustness, and introducing a unified confidence scoring mechanism. Additional enhancements such as offline QR verification and multilingual support can further increase system usability.

In conclusion, the proposed system demonstrates that hybrid AI architectures augmented with rule-based reasoning can provide an effective, scalable, and accessible solution for counterfeit medicine detection, with strong potential for real-world healthcare applications.

REFERENCES

[1] S. Siva Kumar, T. Chithralekha, and A. Banu, “Detection of counterfeit drugs using image processing,” 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, pp. 115–120, Jul. 2018*)*

[2] A. Akram, A. R. Baig, and R. M. Mehmood, “Automatic detection of counterfeit banknotes and medicines using image processing,” 2019 International Conference on Frontiers of Information Technology (FIT), IEEE, pp. 1–5, Dec. 2019.

[3] M. Z. Islam, R. A. Al Mamun, and M. M. Rahman, “A low-cost machine vision based approach for counterfeit medicine detection,” Procedia Computer Science, vol. 143, pp. 366–373, Elsevier, 2018.

[4] P. Sharma and R. Gupta, "Counterfeit Drug Detection using Machine Learning," 2020 International Conference on Computational Intelligence and Communication Networks (CICN), IEEE.

[5] K. Patel, S. Shah, and D. Mehta, "Medicine Authentication using QR Code and Blockchain," 2021 International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE.