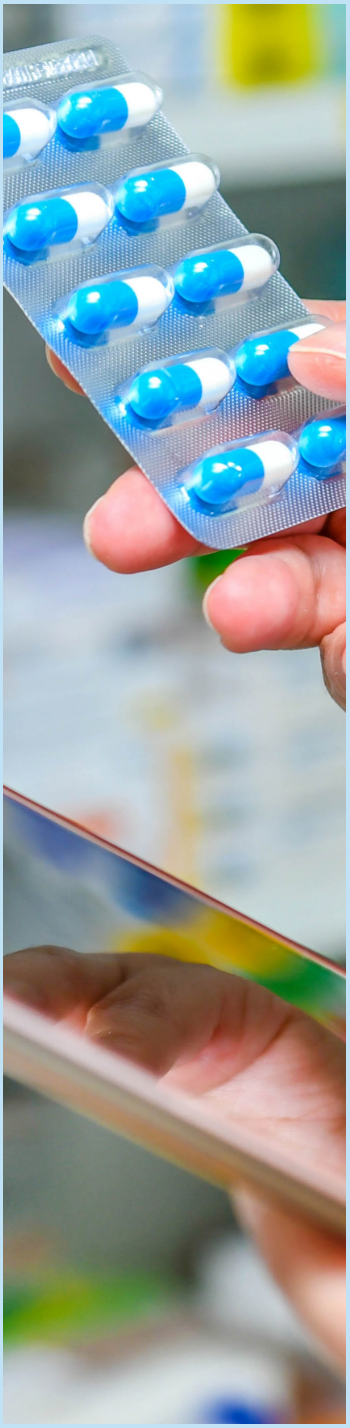
VIEW POINT



COMPARING COUNTERFEIT DETECTION APPLICATIONS AND AI-DRIVEN MONITORING: EVALUATING EFFECTIVENESS

Abstract

Counterfeiting has become a global crisis, threatening consumer safety, brand trust, and revenue across industries like luxury goods, electronics, pharmaceuticals, and auto parts. Sophisticated fraud tactics now mimic even digital verification, making detection harder. Traditional solutions often lack scalability, while AI-powered monitoring offers real-time visibility, automation, and adaptability. With rising regulatory and consumer pressure, businesses must choose the right tools to safeguard their value chains. As supply chains grow complex, understanding the strengths of AI-led detection is key to staying ahead of counterfeiters and protecting both reputation and customer trust.

Infosys®
Navigate your next

The growing challenge of counterfeit goods

Counterfeit goods are unauthorised imitations of genuine products, which the fraudsters create with the intent to deceive buyers. They mimic branding, packaging, and product design but lack the quality, safety, and reliability of the original. These fake items affect nearly every industry and create serious risks for consumers and businesses alike.

Some of the most common examples of counterfeit products include:

- Fake cosmetics and skincare items
- Imitation designer clothing and handbags
- Fraudulent automotive parts
- Knock-off consumer electronics and batteries
- Counterfeit medicines and dietary supplements

Beyond financial losses, counterfeit goods cause real harm. Faulty electronics, for example, contribute to deaths and serious injuries, often due to fires or electric shocks. The pharmaceutical industry also suffers, with counterfeit pills leading to overdoses, allergic reactions, and long-term health consequences.

The scale of the issue is staggering. Counterfeiting has grown into a huge criminal enterprise. In the luxury sector alone, brands lose billions each year, while fake fashion items account for nearly a majority of all counterfeit seizures globally.

What makes this threat more concerning is the technology that fraudsters now use to replicate authentic labels, QR codes, and packaging details. As these fakes become harder to identify, the need for advanced counterfeit product detection has become both urgent and unavoidable.

Common counterfeit detection techniques

As counterfeit operations grow more sophisticated, many businesses continue to rely on outdated methods, unable to match the speed or scale of the threat. While the traditional approach of manual visual inspection has its advantages, advanced technologies now offer far more effective tools for counterfeit product detection.

Traditional counterfeit detection techniques rely heavily on surface-level checks and require skilled human judgement. These methods leave room for error, especially when counterfeiters replicate genuine packaging with precision. Manual physical inspection methods involve:

- Inspectors relying on personal experience to spot subtle inconsistencies in labels, colours, or construction
- Checking packaging materials or holograms under UV lights or tactile tests
- Looking for material differences, missing seals, or incorrect markings for quality assessment.

While these checks work in controlled environments, they do not scale across high-volume or global operations, and counterfeiters use this limitation to slip fakes through undetected. To improve speed, accuracy, and coverage, organisations are now shifting toward digital tools that enhance counterfeit product detection across the supply chain. These tools leverage technologies like:

External Document © 2025 Infosys Limited

Blockchain systems

To create tamper-proof, verifiable records for each product, enabling full traceability from source to sale

AI and machine learning algorithms

To analyse images and flag anomalies faster than human reviewers

IoT sensors

To monitor product condition and movement, helping verify authenticity and prevent tampering in transit

Forensic tools

To examine material composition and molecular structures to identify even the most convincing fakes

These technologies not just overcome the limitations of manual methods, but they also allow businesses to anticipate counterfeit threats and respond in real time. As the counterfeit landscape becomes more complex, integrating smart counterfeit detection tools is essential.

Counterfeit detection applications

With the rise of smartphones and affordable internet, mobile apps and web-based applications are playing a growing role in helping both businesses and consumers verify the authenticity of products quickly. These platforms bring counterfeit detection close to the point of sale and into the hands of everyday users.

Most counterfeit detection applications follow a simple procedure:

Users scan the product's QR code or barcode using their smartphone to initiate an authenticity check

The app connects to a secure database to verify the code against registered product information

Some apps also allow users to manually report suspicious items, with the report often requiring photos and location details for further investigation

This streamlined approach gives businesses a quick way to empower their employees and customers with immediate access to verification tools. It also offers several practical benefits, especially in retail and consumer-facing environments, such as:

The intuitive interface allows users to scan and verify products without any technical training.

Running on standard smartphones, these counterfeit detection apps are often widely accessible without the need for specialised equipment.

Instant verification enables users to make informed purchase decisions on the spot.

Although mobile authentication applications provide a fast and accessible way for counterfeit detection, they often struggle with scale, complexity, and evolving counterfeit tactics. For businesses dealing with high-volume risks and global distribution challenges, counterfeit detection applications serve only as a first layer of defence. However, more intelligent, adaptive systems are essential to stay ahead of the evolving threat.

External Document © 2025 Infosys Limited

Counterfeit detection challenges

Even with growing investments in technology, businesses continue to face several challenges when it comes to building reliable counterfeit product detection strategies. These often limit the effectiveness of detection efforts, particularly across global and complex supply chains. Addressing them requires a clear understanding of where current systems fall short.

Key limitations that often reduce counterfeit detection impact include:

Most counterfeit detection tools focus on specific product lines or categories, making it difficult to scale across diverse inventories.

Many solutions depend heavily on updated, accurate manufacturer data, which may not always be available or consistent.

Global supply chains involve multiple touchpoints, creating gaps where counterfeit goods can enter unnoticed.

Fraudsters increasingly use advanced techniques to replicate genuine labels, serial numbers, and security features, making counterfeit detection harder.

Businesses often struggle to create awareness among customers and internal teams on why and how to verify product authenticity.

The high cost of implementing and maintaining advanced detection tools can hinder widespread adoption, especially for smaller brands.

These challenges highlight the need for smarter, more adaptive counterfeit detection systems that can operate in real time and learn from evolving threats. This is where AI-powered monitoring offers a more scalable and proactive approach to counterfeit product detection.

AI-powered monitoring for counterfeit product detection

Counterfeit detection applications can no longer match the speed and scale at which counterfeit operations operate today. Businesses need intelligent, flexible, and forward-looking solutions to close the growing gap between detection and prevention. Advanced monitoring offers just that, combining machine learning, blockchain, and automation to transform how organisations tackle counterfeit product detection across physical and digital channels.

Here is how AI-powered monitoring is facilitating counterfeit detection:

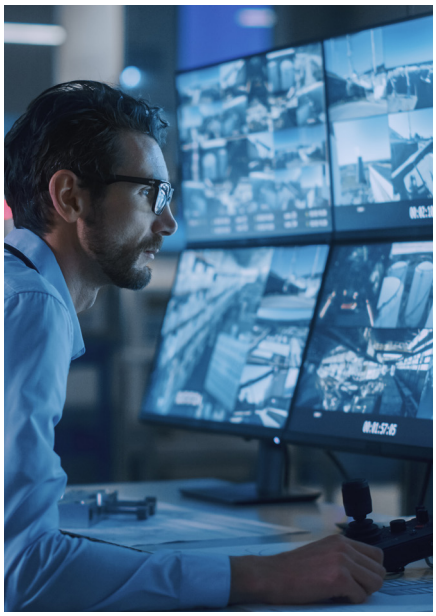
Making supply chains traceable and tamper-resistant

AI systems enhance supply chain visibility by pairing real-time tracking with blockchain's immutable records. Businesses can monitor product movement across sourcing, manufacturing, and distribution stages. With this level of transparency, they can instantly identify unauthorised diversions or tampering.

Detecting fake products through visual AI

Computer vision models use image recognition and object detection to identify inconsistencies that humans often miss. These include logo misalignment, packaging irregularities, or missing security features. AI can also verify serial numbers, QR codes, and product-specific identifiers against authentic databases. These models become smarter with every scan, continuously learning to spot more subtle or sophisticated forgeries.

External Document © 2025 Infosys Limited



Turning fragmented data into strategic intelligence

AI not only detects fakes but also helps prevent them by making sense of unstructured data. Machine learning models analyse scan patterns, transaction histories, and buyer behaviours to spot unusual trends. Natural language processing engines scan online reviews, forums, and marketplaces to flag suspicious sellers or complaints in multiple languages. These insights allow businesses to identify threats earlier and act faster.

Scaling online surveillance and enforcement

AI-powered platforms monitor eCommerce websites, social media, and digital marketplaces around the clock. They scan thousands of listings, flag unauthorised sellers, and trigger takedown requests in real time.

Although AI-driven counterfeit detection systems require upfront investment and careful integration, the long-term gains far outweigh the initial effort. They reduce the need for manual inspections, lower the cost of dealing with counterfeit-related issues, and increase customer trust by maintaining consistent product integrity. More importantly, these systems adapt with time, learning from every data point to improve precision and stay ahead of counterfeiters.

As businesses face growing pressure to safeguard their brands and customers, AI-first counterfeit detection offers a proactive, scalable path forward – one that supports both present needs and future resilience.

End note

As counterfeit goods continue to evolve, so must the counterfeit detection tools. AI-first trust and safety solutions are redefining how businesses respond to counterfeiting threats, turning reactive counterfeit product detection into proactive protection. These intelligent systems do more than detect fake products; they adapt, scale, and evolve to safeguard supply chains, build consumer trust, and preserve brand integrity.

While counterfeit detection applications provide a useful starting point, they fall short against today's complex fraud networks. AI-powered monitoring closes this gap, offering enhanced accuracy, speed, and long-term resilience. As counterfeiting grows more sophisticated, businesses that embrace data-led, AI-first counterfeit product detection will lead the way in protecting value, reputation, and safety across industries.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next

© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.