Tracing the Source:
Using AI to Unmask Counterfeiters in Real Time

Counterfeiting is no longer a crude affair. Today's fake products can closely mimic legitimate ones, infiltrating supply chains with concerning precision. Yet, for all their sophistication, counterfeiters often leave digital fingerprints behind. By harnessing the power of artificial intelligence, it's now possible not just to block fake goods – but to trace them back to their source.

This white paper outlines how AI-driven certificate tracking, behaviour analysis, and anomaly detection form a comprehensive framework for identifying the origin of counterfeit goods. Drawing on years of experience and advanced data systems, this methodology goes beyond protection: it becomes an investigation tool capable of dismantling criminal supply networks.

Unique Certficates and AI Recognition

Each product protected by Cypheme's technology carries a unique certificate featuring both a unique ID code and a chemically unique « fingerprint ». The codes are algorithmically generated in an encrypted format, while the fingerprints are recorded in a database alongside their associated codes. When a user takes a photo of a Cypheme certificate, the AI looks up the code, retrieves the corresponding fingerprint from the database, and verifies whether the fingerprint in the image matches.

But that's just the beginning. When a counterfeiter attempts to clone a label, the system doesn't just detect the fake – it starts building a case.

Since every scan of a certificate is logged, AI can detect anomalies immediately. If copies appear in the supply chain, they are instantly flagged. The system recognises both the legitimate origin of a code and the irregularities of a fake. Distribution patterns, scan behavior, and even the timing of verification attempts provide strong forensic indicators.

Tracing the Source of the Fake

Cypheme is fully compliant with the strictest laws in the world when it comes to privacy: European GDPR. As such, all scan data is perfectly anonymised. Yet even without personal data, useful insights can be drawn from behavioural patterns. For instance, someone who scans a single product over a long period is likely a consumer, while someone scanning dozens of items is likely a shop owner. Similarly, we can figure out with a high degree of confidence which individual nod on the network is a distributor, or a logistics partner.

This behavioural distinction allows the system to infer which parts of the distribution chain are operationally relevant. A counterfeit detected by a consumer may simply be an endpoint failure; it offers no actionable trace. An individual scan is never relevant. But a fake found during a high-frequency scan suggests a professional node – and a possible entry point for further investigation.

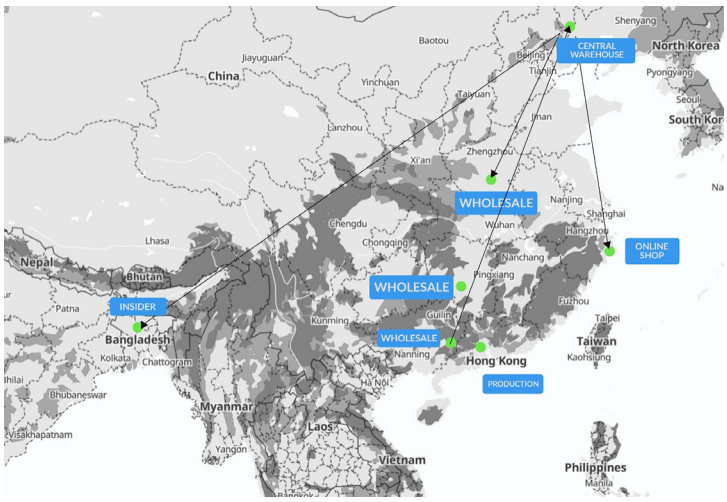
Linkage Through Duplication and Batch PaBerns

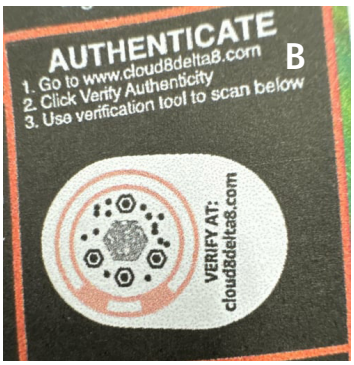
Because each certificate is unique, any duplicated code can be traced to its original source. When a fake uses a copied code, investigators can identify who originally received that code and when. This data helps pinpoint the breach – whether it's a missing batch, a compromised factory, or an insider leak.

In many cases, counterfeit products are distributed alongside genuine ones, often through the same channels. By examining the overlap between real and fake shipments, the investigation can narrow down potential culprits. Early detection of a fake, especially before the legitimate product is released, suggests insider access – valuable intelligence for targeting internal threats.

Geospatial and Behavioural Mapping

With enough scan data, AI can generate a





Example of authentic certificate (A) Example of fake certificate. (B) Defining trait for this family of certificate: – Printed directly on the package rather than as separate stickers – Low resolution – Colour printed in quadrichromy – "Certificate" is 95° sideways

geographic 'cloud' showing where fakes appear first. The denser the cluster, the closer investigators are to the origin. Even without identifying individual users, anonymous usage data can show regional distribution trends and suspicious activity zones.

Combined with batch information and shipment records, this spatial mapping allows authorities to zero in on likely sources – whether a warehouse, a rogue reseller, or a clandestine print operation.

Forensic Signatures and the Families of Fakes

Every counterfeiting operation leaves behind a signature. This could be the type of ink used, the resolution and method of printing, or the physical materials applied. These subtle indicators are difficult to fake consistently – and serve as valuable forensic clues.

Over time, Cypheme's AI has learned to classify these markers and cluster fakes into "families" based on their similarities. A particular kind of ink, print grain, or adhesive behaviour might indicate that multiple counterfeit items were produced by the same entity, using the same process or equipment. These families often emerge across geographic areas, and by identifying the overlapping distribution of such products, investigators can triangulate the source – whether it's a factory, an insider operation, or a subcontractor.

In some cases, deeper forensic analysis – such as identifying whether the print technique is flexographic, digital, or offset – can suggest the scale and professionalism of the counterfeit operation. Industrial printing methods imply a large, organised effort. In contrast, low-end inkjet counterfeits may indicate a more amateur, decentralised attempt. Each clue narrows the search.

Conclusion: Counterfeiting as a Traceable Crime

What was once an invisible crime has become traceable. With AI-powered systems like Cypheme's, the presence of counterfeit goods is no longer a passive threat but an active investigative lead. Each scan, each anomaly, and each inconsistency becomes a data point that sharpens the focus on counterfeit networks.

The future of anti-counterfeit protection lies in proactive intelligence – not only stopping fake products but unmasking the operations behind them. Through a combination of certificate verification, behavioural analytics, geographic mapping, and forensic evidence, modern systems can transform product security from a reactive protocol to a forensic science and finally be able to fight back.

Charles Garcia

Charles Garcia is a technologist and entrepreneur. Since graduating 2011, he has lived in four countries and co-founded several ventures in the emerging smart-tech space. In 2015, he co-founded Cypheme, an AI-powered product authentication company. Cypheme has since become a leader in the European anti-counterfeiting space, receiving recognition from Station F and the European Union's Horizon 2020 programme.