

Review

Combating the Counterfeit: A Review on Hardware-Based Anticounterfeiting Technologies

Suvadeep Choudhury ¹, Filippo Costa ², Giuliano Manara ² and Simone Genovesi ^{2,*}

¹ The Department of Electronics and Communication Engineering, The LNM Institute of Information Technology, Jaipur 302031, India; suvadeepchoudhury@gmail.com

² The Dipartimento di Ingegneria dell'Informazione, University of Pisa, 56122 Pisa, Italy; filippo.costa@unipi.it (F.C.); giuliano.manara@unipi.it (G.M.)

* Correspondence: simone.genovesi@unipi.it

Abstract

Counterfeiting poses a significant threat to global commerce, causing economic damage and jeopardizing consumer safety. This report addresses the critical need for advanced anti-counterfeiting measures. While often confused, authentication verifies an item's genuineness, whereas anticounterfeiting is a broader strategy that includes authentication to deter counterfeit production. This report explores such technologies, which are primarily based on tangible objects and can be used as an anticounterfeiting measure. Such technologies, referred subsequently as “hardware-based anticounterfeiting techniques”, provides a critical line of defence in the fight against imitation of goods. This review covers diverse methods: electronic, mechanical, chemical, and marking techniques. The report emphasizes that no single technique is sufficient, advocating for a multi-layered approach. By combining these hardware solutions with complementary measures like supply chain monitoring, we can create a more resilient defense against counterfeiting.

Keywords: anticounterfeiting; chemical-based; contact chips; electronic; marking-based; mechanical-based; Radio Frequency Identification



Academic Editor: Ephraim Suhir

Received: 31 July 2025

Revised: 18 September 2025

Accepted: 19 September 2025

Published: 22 September 2025

Citation: Choudhury, S.; Costa, F.; Manara, G.; Genovesi, S. Combating the Counterfeit: A Review on Hardware-Based Anticounterfeiting Technologies. *Appl. Sci.* **2025**, *15*, 10298. <https://doi.org/10.3390/app151810298>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The global prevalence of counterfeit goods, estimated to reach a staggering \$326.3 billion by 2029 [1,2], poses significant threats across diverse industries. These threats encompass consumer safety hazards, brand reputational damage, and economic instability [3]. These illicit goods not only deprive legitimate manufacturers of rightful revenue but also inflict harm upon brand integrity, potentially jeopardizing consumer trust and loyalty. In recent years, the issue of counterfeiting has increased public attention, fueled by the escalation of sophisticated technologies employed by counterfeiters in their pursuit of their profit [4]. This concerning trend is further escalated by factors such as uneven wealth distribution, intricate global trade arrangements, and complex social and economic developments, all of which contribute to the increasingly occurrence of counterfeiting activities.

This review paper embarks on an in-depth examination of the multifaceted landscape of hardware-based anti-counterfeiting technologies. The term “hardware” in this context refers to any tangible object which can be used as an anticounterfeiting measure. By delving into their functionalities, potential applications, and inherent limitations, a comprehensive overview is provided for diverse stakeholders across industries. This includes empowering manufacturers, brand owners, and policymakers with the knowledge necessary to select

the most suitable hardware solutions aligned with their specific needs. A multi-pronged approach has been undertaken to comprehensively analyze the landscape of hardware-based anti-counterfeiting technologies, with the thrust areas being:

- **Taxonomic Framework:** Establishment of a robust classification system, categorizing and defining diverse methodologies based on their underlying principles and functionalities.
- **Comparative Analysis:** Rigorous evaluation of prominent technologies, appraising their strengths and weaknesses across key metrics such as security level, cost-effectiveness, implementation ease, and scalability, empowering stakeholders to make informed choices based on their specific needs.
- **Practicality and Integration in the System:** Discussion on the practicalities of implementation, crucial factors to consider when selecting hardware-based solutions. This includes product type, target audience, and integration with existing systems, ensuring the chosen technology seamlessly fits within existing infrastructure.
- **Real-World Impact:** To showcase the effectiveness of hardware-based solutions, certain case studies and real-world applications from diverse industries have been discussed. These examples demonstrate the tangible impact of these technologies in combating counterfeiting across various domains.

Prima-facie, one needs to understand the figures of merit which are associated with hardware-based anticounterfeiting techniques. They include:

- *Unclonability/Security Level*, which includes the difficulty in replication, robustness of attack, randomness/uniqueness.
- *Identification states/data capacity*, which involves calculation of the number of unique identifiers.
- *Readability/Reliability*, which is associated with the read range and speed, accuracy, error rate, orientation with respect to the reader.
- *Cost effectiveness*, which includes the tag and the reader/overall deployment cost.
- *Integration and Compatibility* with the current systems, and the associated environmental impact.

While often conflated, authentication and anticounterfeiting are distinct concepts. Authentication is the specific process of verifying an item's genuineness by checking a unique feature against a known standard [5]. In contrast, anticounterfeiting is a comprehensive strategy that includes authentication as a component, aiming to prevent and deter the creation and distribution of counterfeit goods [6]. The aim of this work is to explore anti-counterfeiting techniques and the associated hardware used for authentication to combat counterfeit products.

Table 1 presents a visual categorization of the state-of-the-art hardware-based technologies in use. These technologies are classified according to several key criteria, including their size and location within the final product, their visibility to the naked eye, any requirement for dedicated readers or server connections, their typical use case, associated cost, and their target industry. Given the specific focus of this review on hardware-based approaches to product authentication, software-based detection techniques have not been explicitly analyzed or reviewed. This paper is organized as follows: Electronic anticounterfeiting techniques involving hardware based approaches are elaborated in Section 2. This mostly encompasses techniques involving NFC, RFIDs and chips. Section 3 deals with mechanical based techniques, which includes security films, engravings, seals and labels. Chemical anticounterfeiting techniques are elaborated in Section 4, which mostly deals with coding on a chemical levels, viz. DNA based, glue coding, and surface analysis. Section 5 discusses various marking techniques used in anticounterfeiting which includes microtexts, holograms, watermarks, and inks, with Section 6 providing the concluding remarks.

Table 1. A roadmap on the hardware based anticounterfeiting techniques. **Target Industry** (Pharmaceuticals: PH, Electronics: EL, Luxury Goods: LG, Food Supply Chain: FS, Others: OT), **Product/ Package size** (Very Small (~medicines): VS, Small (~Smartwatch): S, Medium (~Laptop): M, Large (others): L).

Anticounterfeiting Technique (Section Number)	Technology (Section Number)	Target Industry	Product/ Package Size	Visible to the Naked Eye (Y/ N)	Requirement of a Reader (Y/ N)	Usage		Hardware Cost (on a Scale of 1–5) 1: Cheap 5: Costly	Server Connectivity (Y/ N)	
						In Package (PA)/ Product (PR)	For Authentication (AU)/ Track and Trace (TT)/ Anti-alteration (AA)			
Electronic (Section 2)	NFC (Section 2.1)	LG	VS, S, M, L	N	Y	PA, PR	AU, TT	2	Y	
	Magnetic stripes (Section 2.2)	EL	S	N	Y	PR	AU, TT, AA	1	Y	
	Contact chips (Section 2.3)	PH, LG	S	Y	Y	PR	AU, TT, AA	2	Y	
	Electronic seal (Section 2.4)	FS	M, L	N	Y	PA, PR	AU, TT, AA	1	Y	
	RFID (Section 2.5)	Active Section 2.5.1	LG, EL, LG, FS	M, L	N	Y	PA, PR	AU, TT	3	Y
		Passive Section 2.5.2		VS, S, M, L	N	Y	PA, PR	AU, TT	1	Y, N
		Battery assisted passive Section 2.5.3		M, L	N	Y	PA, PR	AU, TT	2	Y
		Chipless Section 2.5.4		VS, S, M, L	N	Y	PA, PR	AU, TT	1	N
		Physically Unclonable Functions Section 2.5.5		VS, S, M, L	N	Y	PA, PR	AU, TT	2	Y
Mechanical (Section 3)	Security films (Section 3.1)	EL	S, M, L	Y	Y, N	PA, PR	AA	2	N	
	Engravings (Section 3.2)	LG	VS, S, M, L	Y	N	PA, PR	AU, TT	5	N	
	Seals (Section 3.3)	FS	S, M, L	Y	N	PA, PR	AA	1	N	
	Labels (Section 3.4)	Adhesive based	OT	S, M, L	Y	Y, N	PA, PR	AU, TT, AA	1	Y, N
		Fabric based	OT	VS, S, M, L	Y	Y, N	PA, PR	AU, TT, AA	2	Y, N
		Micro-engraved	OT	VS, S, M, L	Y	N	PA, PR	AU	2	N
		Void	OT	VS, S, M, L	Y	Y	PA, PR	AU	1	Y
Chemical (Section 4)	DNA coding (Section 4.1)	PH, EL	S	N	Y	PA, PR	AU, TT, AA	5	Y	
	Chemical encoding (Section 4.2)	PH, EL, FS	VS, S, M	N	Y	PA, PR	AU, AA	4	Y	
	Surface analysis (Section 4.3)	LG	VS, S, M, L	N	Y	PA, PR	AU, AA	4	Y	
	Glue coding (Section 4.4)	EL	S	N	Y	PA, PR	AU, TT, AA	4	Y	
Marking (Section 5)	Optical memory stripes (Section 5.1)	OT	S, M, L	Y	Y	PA, PR	TT	4	Y	
	Microtext (Section 5.2)	OT	VS, S, M	N	Y	PA, PR	AU	2	N	
	Watermark (Section 5.3)	PH	VS, S, M	Y	N	PA, PR	AU	3	N	
	Copy detection patterns (Section 5.4)	FS	VS, S, M, L	Y, N	Y	PA, PR	AU, TT	1	Y	
	Guilloche printing (Section 5.5)	OT	VS, S, M	Y	N	PA, PR	AU	2	N	
	Security holograms (Section 5.6)	Traditional	PH, EL, LG	VS, S, M, L	Y	N	PA, PR	AU	1	N
		Complex	PH, EL, LG	VS, S, M, L	Y, N	Y, N	PA, PR	AU	2	N

Table 1. Cont.

Anticounterfeiting Technique (Section Number)	Technology (Section Number)		Target Industry	Product/ Package Size	Visible to the Naked Eye (Y/ N)	Requirement of a Reader (Y/ N)	Usage		Hardware Cost (on a Scale of 1–5) 1: Cheap 5: Costly	Server Connectivity (Y/ N)
							In Package (PA)/ Product (PR)	For Authentication (AU)/ Track and Trace (TT)/ Anti-alteration (AA)		
Marking (Section 5)	Machine readable codes (Section 5.7)	1D Section 5.7.1	PH, FS	VS, S, M, L	Y, N	Y	PA, PR	TT	1	Y
		2D Section 5.7.2	PH, FS	VS, S, M, L	Y	Y	PA, PR	AU, TT	1	Y
	Inks (Section 5.8)	UV Sensitive Section 5.8.1	PH	VS, S, M, L	Y, N,	Y	PA, PR	AU, AA	5	N
		IR Sensitive Section 5.8.2	PH	VS, S, M, L	N	Y	PA, PR	AU, AA	5	N
		Magnetic Section 5.8.3	PH	VS, S, M, L	N	Y	PA, PR	AU, AA	5	N
		Thermochromic Section 5.8.4	PH	VS, S, M, L	Y	N	PA, PR	AU, AA	5	N
		Reactive Section 5.8.5	PH	VS, S, M, L	Y	N	PA, PR	AU, AA	4	N
		Penetrating Section 5.8.6	PH	VS, S, M, L	Y	N	PA, PR	AU, AA	5	N

2. Electronic Anticounterfeiting Techniques

Electronic anticounterfeiting technologies utilize electronic data devices to establish a unique association with physical goods. This association serves two primary functions: first, it enables the individual identification and authentication of each item through direct access to embedded product information or by providing a bridge to external databases containing the relevant data. Second, the association facilitates the tracking and monitoring of the goods throughout their life-cycle. The technologies in use will be discussed in the subsections to follow.

2.1. Near Field Communication—NFC

Near Field Communication (NFC) technology is now widely integrated into smart devices (smartphones and smartwatches), enabling a variety of user-friendly applications. One prominent use case is contactless payment, where users can link their credit cards to their devices and authorize transactions by simply bringing the device near an NFC-enabled reader at payment terminals [7]. Additionally, NFC technology facilitates fare payments on public transportation systems and plays a crucial role in product authentication, enhancing security and combating counterfeiting.

Unlike Radio Frequency Identifiers (RFID) based readers (to be discussed later), which are capable of simultaneously reading numerous tags, a characteristic that proves valuable in applications like logistics, NFC readers are designed for one-to-one communication with a single tag at a time. This unique feature renders NFC technology particularly well-suited for securing transactions, such as credit card payments, where individual authentication and data integrity are of paramount importance. Implementing NFC technology requires initial monetary investments for development of the management systems and in possible changes to the production process. The tag costs are within a few euros, but depends mostly on the specific target application and the associated level of authenticity required.

2.2. Magnetic Stripes

Magnetic stripes, which are mostly associated with credit cards, ID cards, and even some product packaging, offer a surprisingly robust layer of security against counterfeiting. While relatively low-tech compared to more advanced solutions like RFID chips, magnetic stripes still hold merit because of the following advantages:

- **Simplicity:** Require minimal infrastructure to read and write data, making them cost-effective and accessible.
- **Durability:** Resistant to wear and tear, lasting for years under regular use.
- **Versatility:** Can be integrated into various objects, from cards to packaging, offering broad applicability.

The hardware components which are conventionally used include:

- **Magnetic material:** The core of the strip is a thin layer of ferromagnetic material, typically iron oxide, capable of storing data encoded as a series of magnetized zones. This standard tape strip contains three magnetic tracks, containing magnetic resins that are used to store the card's data, in encoded format [8].
- **Substrate:** The magnetic material is embedded within a flexible substrate, usually polyvinyl chloride (PVC), for protection and handling.
- **Encoding/Reading Head:** A specialized device which writes/reads data by magnetizing or sensing the magnetic fields of the zones. These heads can be integrated into card readers, point-of-sale terminals, or even handheld verification devices.

The core component of the encoding head is a laminated electromagnet which is typically constructed from permalloy or soft ferrite, with an air gap $\approx 0.3 \mu\text{m}$ and substrate

thickness $\approx 25 \mu\text{m}$. As the magnetic tape moves across this electromagnet, the fringing field generated by the magnet alters the spin orientation of the magnetic particles within the tape in a manner directly proportional to the current flowing through the head's coil. This process induces a permanent writing of the encrypted signal onto the tape. While reading, the card with the tape is swiped, which induces an alternating emf in the coil and the data is read successfully [9].

Some modern recording heads utilize conventional ferrites whose gap surfaces are coated with a micrometer-thick metal layer composed of aluminum, iron, and silicon (normally referred to as *Sendust* [10]). This metal-in-gap (M-I-G) technology has better high-frequency behavior and good wear and tear properties of ferrites with the higher coercivity of ferromagnetic metals. Thus, fields two or three times as intense as that offered by pure ferrites can be supported. Such high fields are necessary to record high density (i.e., on high coercivity) data, in which tiny regions of alternating magnetization are closely spaced and should not mutually demagnetize each other. The latest encoding technology utilizes a thin magnetoresistive element, made out of permalloy, which senses the slight variation in resistance (about 2%) that occurs as the angle of magnetization is changed when the magnetized data bits pass beneath the encoding head, thus achieving 1.8 Mbits/mm².

While most commonly employed on financial cards, magnetic stripes offer broader applicability beyond financial transactions, because of its low cost margins. Under suitable physical characteristics and operational conditions, they can be directly affixed to objects to serve several purposes: assuring authenticity, enabling post-sale customer service through item tracking and verification of genuineness.

2.3. Contact Chips—Smart Cards

The concept of embedded microchips in plastic cards, now known as *Smart Card*, first emerged with the 1968 patent application filed by German inventors Jürgen Dethloff and Helmut Grötrupp. Subsequent developments included a Japanese iteration patented in 1970, culminating in Roland Moreno's 1974 French patent filing for the *IC card*, awarded priority status in France in 1975 and the United States in 1978 [11].

Physically analogous to contemporary plastic payment cards, the smart card incorporates a microprocessor or memory chip. This embedded technology, harnessed in conjunction with a dedicated reader, grants the card significant processing power, enabling diverse applications [12]. In the realm of access control, smart cards function as gatekeepers, ensuring that sensitive personal and business data remains accessible solely to authorized personnel. Furthermore, with a storage capacity of 32 kbytes, they empower users to engage in financial transactions and value exchange with enhanced security and ease. In essence, smart cards offer a triumvirate of benefits: data portability, robust security, and unparalleled convenience.

The composition of a smart card comprises three key elements: an integrated circuit (IC), an interface facilitating communication with the card reader, and a physical body. Differentiating characteristics of smart cards vary from the type, size, and communication methodology employed by the embedded IC. These integrated circuits serve as the core computational engine, executing the logic programmed for specific applications, which can be functionally classified into the following two categories [13]:

- **Memory cards:** These category of smart card incorporates a non-volatile memory chip embedded within its structure. This memory component facilitates both data reading and writing operations embedded within a pre-programmed logic circuit etched directly onto the chip during the manufacturing process. This embedded logic circuit safeguards the stored data through a security mechanism that typically

leverages access permission protocols. Consequently, these cards offer exclusively secure data storage functionalities.

- **Microprocessor cards:** This category of the smart card integrates a microprocessor, granting it computational capabilities akin to those of portable slow computing devices. Consequently, these smart cards possess the ability to process, store, and secure information through the utilization of sophisticated cryptographic algorithms.

Based on the chip-to-reader communications, smart cards can be classified into the following three categories [14]:

- **Contact cards:** Contact card communicates utilizing an eight-pin micromodule to establish a physical connection with the card reader, as shown in Figure 1a. Each of the five designated pins serves a specific function: V_{CC} (+5 volts – DC) supplies power, *reset* initializes the module, *clock* regulates timing, *ground* provides a reference potential, and the input/output (I/O) pin facilitates data exchange.
- **Contactless cards:** As illustrated in Figure 1b, contactless smart cards rely on antennas with an approximate 10-cm range to establish communication with readers. These memory chip devices, physically comparable to credit cards, acquire power and exchange information with the reader through an Radio Frequency (RF) field generated by the reader module. Contactless smart cards are commonly utilized for employee identification badges in building access systems of large organizations.
- **Combination cards:** Multipurpose combination smart cards represent a strategic integration of contact and contactless technologies. These hybrid cards incorporate an eight-pin contact interface for communication with card readers employing physical connections, and additionally feature an antenna that facilitates wireless data exchange with RF readers. This dual functionality expands the application scope of the card, catering to a wider range of use cases.

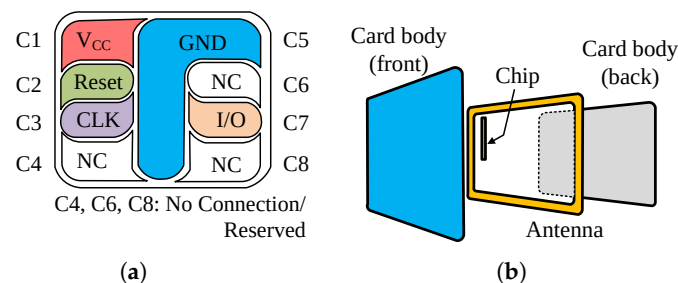


Figure 1. Schematic arrangement of the (a) contact card, (b) Contactless card modules.

Driven by the diverse applications demanding unique solutions within the smart card technology landscape, several standards emerged to ensure compatibility and functionality. The ISO 7816-X series of specifications serves as the cornerstone, comprehensively defining the technical characteristics of this technology.

2.4. Electronic Seal

Electronic seals (also known as eSeals) are integrated within mechanical seals of the packaging system, and are an enhanced version of the traditional seal. In contrast to traditional seals, eSeals incorporate an encrypted chip, thereby enabling them to fulfill anti-counterfeiting functions. They build upon RFID technology to augment their physical anti-tampering properties with functionalities for digital data capture, storage, and readability. Although e-seals find its major applications in secure and authenticating legal documents and official certificates, including contracts, invoices, tax declarations, etc, they are more often used along with RFID technologies to build secured anticounterfeiting systems. Such systems are used in elevating security in logistics [15], container terminal management

system [16], real-time tamper detection [17], inventory and asset management [18], to name a few. This enhanced capability translates to superior security and control compared to traditional mechanical seals, as they enable self-monitoring and real-time monitoring capabilities. A comparative overview between an e-seal and a traditional seal is portrayed in Table 2.

Table 2. Comparison of E-Seal and Traditional Seal [19,20].

Feature	E-Seal	Traditional Seal
Physical form	Digital	Physical object (stamp, wax, seal, etc.)
Application	Electronic documents	Physical documents
Security	Cryptographic methods	Physical security (ink, wax, etc.)
Verification	Digital	Visual
Storage	Digital	Physical
Transfer	Electronic	Physical
Tamper evidence	Digital signatures, timestamps	Visual inspection for tampering
Environmental impact	Minimal	Potential environmental impact from materials and production
Accessibility	Remote access	Requires physical presence
Legal recognition	Varies by jurisdiction, but gaining legal recognition in many countries	Generally recognised and accepted

To generate an eSeal, a legal entity must undergo a rigorous vetting and authentication process conducted by a third party or through a remote identity verification system. An eSeal can then be utilized to digitally sign large quantities of documents (bulk signing), such as invoices or educational transcripts, via an accredited digital signing solution. Electronic seals serve to authenticate both the identity of the signing entity and the document's integrity, which serves as its two major objectives. An evaluation of an eSeal's quality can be assessed based on the following characteristics:

- **Non-duplicability:** The electronic seal must resist replication, ensuring its uniqueness.
- **Reliability:** The seal should be designed to prevent resealing after being opened, and the act of opening should be readily discernible.
- **Verifiability:** An operator must be able to readily confirm both the authenticity and integrity of the seal, either through visual inspection or by employing a dedicated device.

Such a technology is increasingly being used by the domestic and international customs, wherein it significantly reduces the time and potential for errors associated with manual inspections. Active eSeals further employ real-time positioning monitoring technology, enabling continuous tracking of container transportation routes. Within the domestic tax area, electronic seals are utilized to supervise the movement of high-risk, unreleased containers. This supervision encompasses the movement of import containers from port to warehouse, re-export containers between controlled ports, and export containers

from warehouse to port [21]. Some other potential users of the eSeal technology are the medicine/pharma industry [22,23], agriculture and food industries [24–26], e-procurement of goods [27], and e-registration of documents [28], to name a few.

2.5. Radio Frequency Identification—RFID

Radio Frequency Identification (RFID) tags are low-cost, ubiquitous devices designed to uniquely identify and track goods. Within supply chain management, RFID tags facilitate product tracking across various stages and locations. Additionally, diverse applications are emerging that leverage the data extracted from these tags, including:

- Automated inventory management: Streamlining stock control and reducing manual intervention.
- Automated quality control: Enabling real-time monitoring and ensuring product integrity.
- Access control: Enhancing security by granting or restricting entry based on tag identification.
- Payment systems: Facilitating contactless and secure transactions.
- General security applications: Providing additional layers of security and preventing unauthorized access.

The cost of the tags, currently ranging from a few cents to some euros, remains a crucial factor for widespread adoption of RFID-based systems. This affordability is essential for achieving large-scale implementation and maximizing the technology's potential.

The RFID technology dates back to the radar technology, and was primarily used to detect backscattered radiowaves, its evolution being articulated in Figure 2. Currently, RFID tags are extending their reach beyond product identification to tackle counterfeiting challenges [29]. This involves verifying a product's authenticity by locating an RFID tag containing specific product and reference information. Despite various existing variants, all Radio Frequency Identification (RFID) systems share three core components, as depicted in Figure 3:

- **Tags:** Attached to objects, these contain an antenna and/ or a microchip storing product data such as unique identifiers or informational website URLs. Security against reproduction and tampering relies on:
Communication protocols: Governing data exchange between tags and readers.
Information protection methods: Securing tag data through codes, passwords, or encryption algorithms.
- **Readers:** Specific to the utilized tag type, these devices query tags, receive response information, and transmit it to a data processing system.
- **Data Processing System:** Connected to readers via the internet, this system utilizes tag identification codes to access and manage relevant object information.

During a communication protocol with the reader, the tag's information is checked for both presence and certified authenticity. Products with verified information are deemed genuine, while others are flagged as potentially counterfeit.

Based on the operating mechanism, RFID tags are sub-classified into the following four categories:

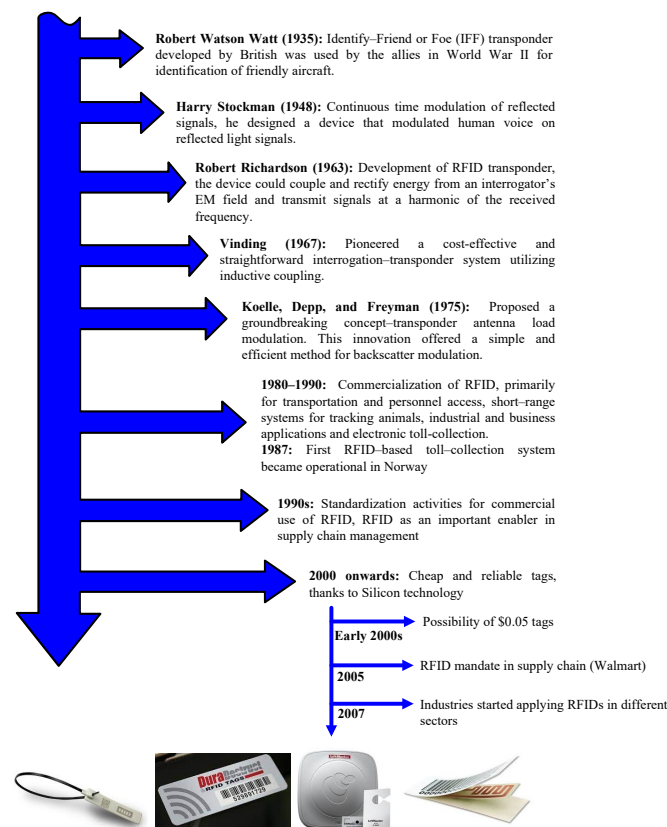


Figure 2. Evolution of the RFID technology [30].

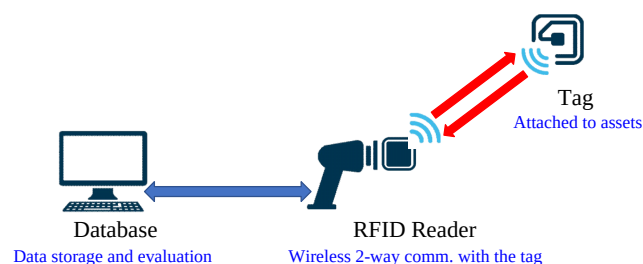


Figure 3. Schematic of a basic RFID-based system.

2.5.1. Passive Tags

Such category of RFID tags are small devices comprised solely of an antenna and an integrated circuit (microchip). In the absence of an internal power source, passive RFID tags harness the electromagnetic field generated by the reader. This coupled energy undergoes rectification and voltage multiplication to activate the internal circuits of the tag. A prevalent technique for this process is the utilization of a multi-stage Greinacher rectifiers [31] or its derivatives. One such two-stage modified Greinacher full-wave rectifier is shown in Figure 4. Subsequently, upon receiving this signal, the tag awakens and transmits its identification data back to the reader. Subsequently, the reader relays the data to a computer for processing and verification. The stored identification data typically consists of a unique identifier, similar to an Electronic Product Code (EPC), which offers additional details beyond barcode information, such as product type and manufacturer. Notably, some passive tags are read-only, while others offer read-write functionality, allowing for data modification and updates.

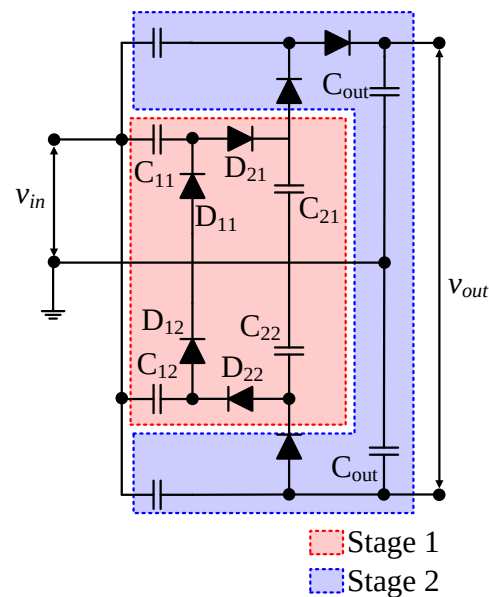


Figure 4. Two-stage modified-Greiner full-wave rectifier.

Two different coupling techniques are commonly used by passive tags, namely:

- **Near-Field Coupling:** Within the near field region, the prevailing characteristic of the electromagnetic field is its reactive nature. This signifies that the electric and magnetic fields are spatially orthogonal (perpendicular) and exhibit quasi-static behavior, meaning they experience minimal change over time. The dominant field, electric with a dipole antenna, or magnetic with a coil antenna, depends upon the specific antenna type employed. Most near-field tags utilize the magnetic field to achieve inductive coupling with the tag's coil, following Faraday's principle of magnetic induction (illustrated in Figure 5). In essence, current flowing through the reader's coil establishes a magnetic field in its vicinity. This field, in turn, induces a small current within the coil of a nearby tag.

The interaction between a reader and a tag leverages a technique known as load modulation [32]. This method works on the principle of mutual inductance, where a change in current within the tag's coil induces a corresponding, albeit smaller, current variation in the reader's coil. The reader detects these subtle variations. To achieve this, the tag modulates the current by deliberately altering the load presented by its antenna coil. This deliberate manipulation of the load underlies the term load modulation. Owing to its inherent simplicity, inductive coupling was the initial technology embraced for passive RFID systems due to its ease of implementation.

As the phenomenon is a nearfield one, such tags are restricted to the use of low carrier frequencies, being mostly restricted at 128 kHz (low-frequency, LF) and 13.56 MHz (high-frequency, HF). This limitation is exemplified by the operational boundary distances, which are significantly shorter for higher frequencies: 372 m for 128 kHz and 3.5 m for 13.56 MHz. An inherent drawback of near-field tags is their inherently low bandwidth, which translates to a correspondingly low data rate [33].

- **FarField Coupling:** In contrast to the near-field region, the EM field within the far-field exhibits a radiative nature. In this regime, coupling involves the capture of EM energy at a tag's antenna as a potential difference. However, a portion of the incident energy reflects back due to an impedance mismatch between the antenna and the load circuit. This mismatch, or deliberate alterations to it, can be exploited to vary the amount of reflected energy, a technique commonly known as backscattering [34] (illustrated in

Figure 6). Such a methodology serves as the foundational principle for communication in far-field tags.

Far-field coupling is the preferred method for long-range (5–20 m) RFID applications, as it is not subject to the restrictive field boundaries encountered in near-field systems. Far-field tags typically operate within the 860–960 MHz Ultra-High Frequency (UHF) band or the 2.45 GHz Microwave band.

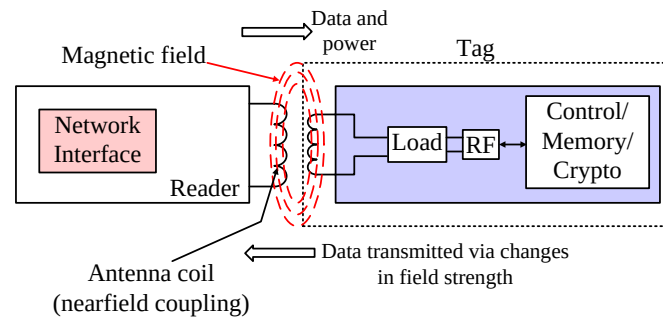


Figure 5. Near-field communication using inductive coupling.

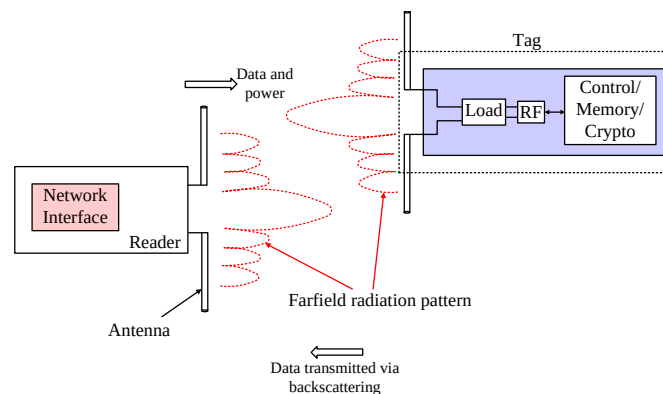


Figure 6. Far-field communication via backscattering, with antennas placed at farfield distances.

2.5.2. Active Tags

Active RFID tags incorporate an internal battery, a transmitter, a receiver, an antenna, and an integrated circuit. This internal power source allows them to possess several advantages over passive tags. Active tags can be equipped with extensive, frequently rewritable memory capacities and may also include integrated sensors. They typically operate at high frequencies, viz the 433 MHz or 2.45 GHz bands. The higher frequency operation enables them to function at significantly greater reading distances compared to passive and semi-passive tags, reaching up to 200 m from the reader depending on antenna configuration and battery strength [35]. The high-frequency operation facilitates the additional functionalities offered by active tags. Essentially, two types of active tags are currently available:

- **Transponders:** Functioning similarly to passive RFID systems, active transponder tags operate in a reader-initiated mode. The reader transmits a signal, prompting the active transponder to respond with a corresponding signal containing the encoded data. This interrogation-response mechanism fosters efficient battery utilization for the transponder. When out of the reader's range, the transponder remains inactive, thus preserving battery life. Active RFID tags utilize a low-power LC-oscillator (depicted in Figure 7) as a wakeup radio. This oscillator is specifically designed to function in the weak inversion region (subthreshold) to minimize power consumption. The oscillator operates near its oscillation threshold, and an incoming radio signal received by the

2.5.3. Battery Assisted Passive (BAP) Tags

BAP tags, also known as semi-passive tags, occupy a niche between passive and active RFID technologies, their architecture being shown in Figure 9. While they share the internal battery characteristic with active tags, BAP tags lack a dedicated transmitter. This functionality aligns with passive tags, where a reader's signal triggers a response. The internal battery in BAP tags serves to power the microchip, enabling features comparable to active tags. These features include integrated environmental sensors and potentially larger, rewritable memory capacities. Additionally, BAP tags boast a significantly extended read range compared to passive tags, functioning at distances of up to several dozen meters from the reader.

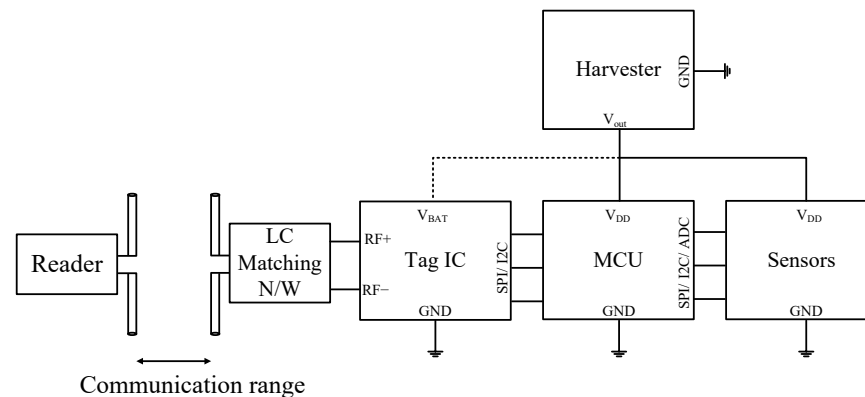


Figure 9. RFID Sensor tag architecture in BAP configuration.

Similar to active tags, the primary drawbacks associated with BAP tags are their finite battery life and the environmental concerns arising from battery replacement and disposal.

Recent advancements in BAP tag technology target these two key limitations, namely the limited battery life and communication range. To address the first challenge, research is exploring the use of energy harvesting modules as a potential replacement for batteries. This approach could offer indefinite operational autonomy, eliminating the need for battery replacement and its associated environmental concerns. Secondly, improvements in tag integrated circuit (IC) design have introduced a concept known as BAP mode. This mode leverages an additional input voltage pin (V_{BAT})—as illustrated in Figure 9. By supplying external power to the internal blocks of the MSP430 low-power microcontroller unit (MCU) [39] and the tag IC through this pin, BAP mode allows for enhanced sensitivity. This, in turn, leads to a significant improvement in the overall communication range of the system [40].

2.5.4. Chipless RFID

Chipless RFID offers a promising solution for anti-counterfeiting, particularly for high-volume, low-cost items where traditional chip-based RFID would be cost-prohibitive. The price of an RFID tag depends on several factors:

- **Order volume and functionality:** The cost of RFID tags varies significantly based on the number of tags ordered and the specific functions they need to perform.
- **Item cost:** The value of the item being tagged influences the required security level, which in turn affects the tag's price. For example, a high-value item like a luxury watch requires a more secure and expensive tag than a standard item like a book.
- **Deployment environment:** The environment where the tag will be used also affects its cost. Tags deployed in harsh environments, such as for asset management in a yard or livestock tracking, must be more durable and rugged, which increases their price.

For chip-based tags, the price can range from 5–30 cents per tag for passive tags when ordered in bulk, and \$10–\$100 per unit, based on its functionality for active ones. Conversely, for smaller order quantities, the chipless ones cost around 1–20 cents, which reduces to below 1 cent for bulk orders [41]. Unlike its chipped counterparts, chipless RFID tags embed unique electromagnetic signatures through patterned conductive materials or specialized inks. When interrogated by a reader, these tags reflect specific radio frequencies, creating a distinct “fingerprint” that can be authenticated, as shown in Figure 10. An Ultrawideband signal impinges on the chipless tag, which backscatters/reflects back parts of the signal, based on its structural characteristics, hence providing an unique digital fingerprint. This inherent uniqueness, combined with their low manufacturing cost (often printable directly onto products or packaging), makes them difficult to replicate by counterfeiters [42]. While chipless RFID typically has lower data capacity and a shorter read range than traditional RFID [43], its affordability, flexibility, and enhanced sustainability [44,45] are driving its adoption in various sectors, including retail [46], pharmaceuticals [47], and secure document applications [48], to name a few, effectively complementing or even replacing barcodes for robust product authentication.

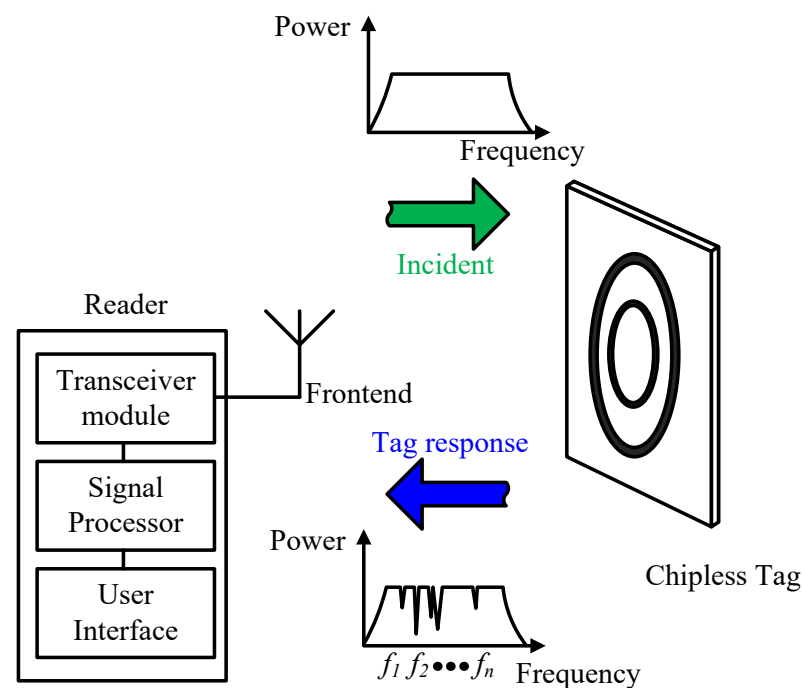


Figure 10. Schematic diagram of operation of Chipless RFID tag.

2.5.5. Physically Unclonable Functions

Physically Unclonable Functions (PUFs) are a compelling anti-counterfeiting solution. These are created during manufacturing through random variations, generating a unique digital “fingerprint” [49]. This inherent randomness makes PUFs impossible to clone, even by the original manufacturer, establishing them as a robust anti-counterfeiting tool [50–52].

In practice, a manufacturer scans a product’s PUF to create challenge-response pairs (CRPs), which are stored in a secure cloud database. An authenticator can then scan the PUF and cross-reference the response with the database to verify the product’s authenticity.

- **Optical vs. Silicon-based PUFs:** Although silicon-based PUFs are widely used, they can be vulnerable to modeling attacks and often lack reliability [53,54]. Optical PUFs offer a promising alternative, providing high complexity and accessible readout. This is particularly true for chemically engineered optical PUFs, which can be highly robust and efficient [55–57].

- **Fluorescent Taggants in Optical PUFs:** Optical PUFs use various fluorescent taggants, including quantum dots, nanocrystals, organic dyes, and carbon dots [58–61]. Recently, silicon quantum dots have also emerged as a viable option [62]. However, semiconducting polymer nanoparticles (SPNs) are a strong alternative, surpassing most fluorescent materials in brightness and photostability [63,64]. SPNs have been shown to be over 30 times brighter than inorganic quantum dots and antibody-dye conjugates [65] and are more photostable than typical fluorescent dyes.
- **Hybrid PUFs:** Hybrid PUFs enhance security by combining physical randomness with a more robust digital system, often an RFID chip [66,67]. This makes them significantly more secure than static identifiers like barcodes, as it is impossible to clone both the physical structure and the cryptographic response simultaneously.

Recent research has explored using semiconducting polymers in anti-counterfeiting by printing unique patterns [68–70]. Similar approaches using photoswitches in paper and gels have also been demonstrated [56,57]. However, these photoswitch-based methods can degrade with repeated use or under harsh conditions [60] and are vulnerable to replication once their active materials are identified. PUF devices based on semiconducting polymer nanoparticles have not yet been explored but have the potential to outperform current fluorescent optical PUFs.

Performance benefits of hybrid PUFs over traditional methods

- Exceptional Security and Unclonability
- Robustness to Environmental Variations
- Enhanced Traceability and Supply Chain Security

Drawbacks and Limitations

- Complexity and Implementation Costs
- Dependency on reader
- Potential for Modeling Attacks

Compared to traditional hardware security methods, PUFs offer a different approach. Traditional methods, such as eFuses and secure memory, store cryptographic keys in dedicated, non-volatile memory [71–73]. While tamper-resistant, these keys are static and can be extracted through costly, invasive physical attacks [74].

In contrast, a PUF’s “secret” is not stored but is derived on-demand from the chip’s physical structure. The key exists only when the device is powered on and disappears when it’s off. Any attempt to physically probe the PUF will likely damage it, making it tamper-evident [75].

Integration Potential

PUFs are well-suited for integration into resource-constrained devices like IoT systems.

- **On-Chip Integration:** Many PUF designs use existing components, such as Static RAM (SRAM), eliminating the need for dedicated hardware. This makes them a cost-effective alternative to other security methods that require separate memory modules or cryptographic co-processors [76,77].
- **Lightweight Authentication:** PUF-based authentication is “lightweight,” replacing complex cryptographic operations with a simpler challenge-response mechanism. This reduces computational and communication overhead, making it ideal for devices with limited power and processing capabilities [78,79].

PUFs offer a significant advantage by providing high security at a low cost. Many PUF types, like SRAM PUFs, use existing on-chip components, resulting in negligible hardware overhead [76]. This makes them a more attractive alternative to expensive, dedicated security chips.

Challenges and Solutions

A key challenge for PUFs is reliability. Environmental factors such as temperature can cause minor response errors, which are typically managed with error correction codes (ECCs), adding some implementation complexity. Additionally, some “strong” PUFs with a large challenge-response space are vulnerable to machine-learning attacks that can predict responses without physical access [80,81].

Ongoing research is focused on addressing these vulnerabilities through new hybrid PUF architectures and protocols [82]. For example, designs may combine PUFs with cryptographic hash functions or use obfuscation techniques to make them more resistant to modeling attacks. Despite these challenges, PUFs remain a robust and cost-effective security solution compared to the risks of hardware counterfeiting or IP theft.

Regardless of the specific system configuration, the inclusion of a dedicated tag-programming layer remains essential. This layer facilitates the seamless integration of RFID equipment and computer control systems within manufacturing lines. This enables real-time processing of tag data and updates to the back-end database, all without compromising production efficiency. Some practical issues associated with RFID tags are as follows [83]:

- Optimal tag programming performance necessitates the appropriate attachment of the tag to the product. This selection process requires careful consideration of two key factors: antenna orientation and the material’s skin depth at the tag’s operational frequency.
- Following product purchase or consumption, the product-bound tag should be deactivated to mitigate the risk of unauthorized reuse by counterfeiters.
- An efficient mechanism for tag programming and database synchronization is crucial to ensure seamless product tracking within the manufacturing line. However, incomplete or erroneous tag programming, potentially caused by inadequate configuration of RFID equipment (encompassing both hardware and software control parameters), can compromise the uniqueness of tag data and consequently, the integrity of the product’s provenance.
- A robust exception-handling mechanism is necessary to identify and manage products with defective tags, including those with duplicate or incomplete programming. This mechanism should facilitate the segregation of such products for either rework (if cost-effective) or disposal.
- Optimization of product transfer speed on a manufacturing or packaging line must balance production throughput with reliable RFID tag programming.

3. Mechanical Anticounterfeiting Techniques

Mechanical anti-counterfeiting solutions leverage the inherent physical characteristics of materials to deter the production of imitations and establish reliable tamper-evident safeguards. While these methods function primarily for basic authentication purposes when employed independently, their integration with complementary technologies allows for enhanced identification and tracking capabilities. A detailed overview of the techniques used for anticounterfeiting using mechanical components are discussed in the sections to follow.

3.1. Security Films

This technology is primarily employed to safeguard data printed on documents and packaging. The protective mechanism involves the application of a plastic film, utilizing pressure or heat, to the designated surfaces (Figure 11). Security features, such as printed elements, tactile textures, or color variations, are directly integrated into the plastic film during its application process, offering an additional layer of protection [84]. The following processes are used to build security in films:

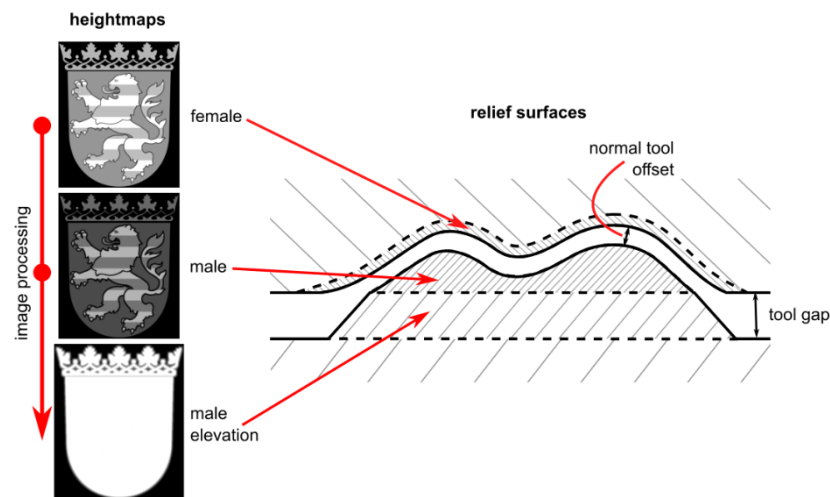


Figure 11. Image processing chain from female to male and male elevation heightmap (left) and schematic cross sectional view of the embossing tool, where representative female, male and male elevation relief surfaces derived from these heightmaps are highlighted (right) [85].

- **Overprinting:** Security elements are strategically positioned for optimal protection within the security film's structure. This typically involves placement on the reverse side (interior) of the film or within the intermediary layer between the adhesive and the film itself. This approach safeguards these elements from potential damage or tampering attempts [86]. Screen printing, or flexographic printing techniques are commonly employed for their application.

Screen printing operates on the principle of selective ink transfer through a mesh screen. Ink permeates the open areas of the screen, corresponding to the desired graphic elements, while the non-printing areas are rendered impermeable by a blocking stencil. This technique can be employed in color film printing using a three-step process: application of a glossy bottom layer, followed by a white base, and finally the addition of specific colors [87]. The factors which affect the printing include (but are not limited to) oil ink, paper, ink knife, cleanliness of the printer heads, speed of screen printing, scraper, the orientation/way of placing paper, tension of network board, pressure adjusting of scraper, angle adjusting of scraper, and human errors [88]. There has also been substantial research for ecologically sustainable alternatives, which includes the use of starch as the printing ink in security films [89–92], to name a few. Although starch is a bio-compatible, cheap, and renewable solution, the disadvantages that limit their usage as packaging films: moisture sensitivity and low mechanical strength and stability.

- **Embossing:** In embossing, the security film incorporates tactile elements for enhanced protection. These elements may include fine lines, intricate patterns composed of thin lines, or microscopic printed features [85,93,94].
- **Embedding through binding:** This technique is primarily utilized to safeguard photographs and printed personal identification data within passports. To deter tampering attempts, the security film is seamlessly integrated into the passport's binding during construction. This integration process results in a narrow extension of the film material onto the subsequent page at the document's rear, creating a tamper-evident margin [86].
- **Iridescent film:** Such films are characterized by an iridescent sheen that exhibits color variations depending on the viewing angle. They are mostly applied for validation of banknotes [95,96].

- Back-reflecting film: Such a film is detectable only under specific viewing equipment by utilizing coaxial illumination, which changes its color [97–99].

3.2. Laser Engravings

This technology leverages a specialized laser to create intricate engravings on various substrates (paper and paperboard, labels, leather, film, rubber, foam, wood, fabrics, PET, PVC, glass, stone, iron, nickel, steel, stainless steel, aluminium, electrical components, etc.). These engravings consist of closely spaced grooves with variable depths. The process allows for the addition of superimposed images, logos, text, or identification codes. These elements exhibit a unique property—their color appears to change depending on the viewing angle. Often mistaken for holograms, these features are highly resistant to replication due to their complexity. A significant advantage of this technology lies in the inherent permanence of the markings. Their inseparable nature from the underlying material makes them highly tamper-proof [100,101]. Conventionally, there are three techniques to achieve laser engraving:

- Annealing: This process, also known as *laser surface stamping*, utilizes a targeted laser beam to permanently mark ferrous metals and titanium. The laser induces localized heating on the surface, triggering a controlled oxidation reaction beneath. This selective oxidation results in a permanent discoloration of the metal, replicating the desired marking design [102].
- Laser engraving: This technique employs a material ablation process to create the desired marking. The laser beam selectively removes material from the surface of the product, replicating the marking design. This method finds particular application with metals, plastics, and ceramics [103,104].
- Deep laser marking: A highly specialized technique for permanent marking on metallic substrates, that utilizes a controlled process to create markings at a predetermined depth within the material's surface [105–108].

3.3. Seals

A seal constitutes a closure mechanism that secures a package, thereby safeguarding its contents from unauthorized alteration. These seals can be crafted from either plastic or metal, and their design can range from a basic and economical screw cap on a bottle to more intricate configurations. While generally straightforward to apply and remove, the efficacy of these seals in deterring tampering hinges considerably upon the expertise and attentiveness of the inspector.

They are characterized by three fundamental properties:

- Unique Identification: Each seal possesses a distinct identifier, allowing for its unambiguous verification.
- High Tamper Evident Security: Seals are designed to be exceedingly difficult to replicate, offering a clear indication of tampering if any attempt is made.
- Enhanced Security: By virtue of their unique identification and tamper-evident nature, seals contribute significantly to the overall security of a package, over which they are the usual choice.

Conventionally, their integrity is established through visual inspection, which reassures the user as to the security of a product by providing visual evidence of any tampering. Some pertinent disadvantages with such seals are the following:

- Limited Tamper History: Unlike some electronic seals, physical seals cannot record the specific time or location of a tampering event. This may limit the ability to pinpoint the exact time and place of a breach.

- **Passive Security:** Physical seals lack the ability to actively monitor their own integrity. Therefore, unlike electronic seals that can trigger alarms upon tampering, physical seals rely solely on visual inspection for detection.

3.4. Labels

Identification labels are physical attachments containing data that uniquely identifies a product and conveys relevant information. These labels are affixed to the product itself or its packaging, regardless of material. Common applications include cardboard boxes, glass bottles, plastic containers, and directly on items like clothing or footwear. During implementation, integrating identification data directly into existing packaging artwork (cardboard, plastic, or shrink sleeves) can be a cost-effective approach, minimizing disruption to production processes.

Furthermore, identification labels can be enhanced with security features through the incorporation of various technologies. When combined with RFID tags or NFC devices, these labels transform into *smart labels*, offering additional functionalities. Based on the type of material and technology used, they can further be categorized into the following subgroups:

- **Fabric based labels:** Fabric labels exhibit remarkable versatility by integrating with various security features, resulting in a spectrum of label complexity. The most basic labels serve the primary function of displaying product information and identification codes, typically barcodes. As complexity increases, labels incorporate more sophisticated security measures, including holograms, security threads, and tracer in fibers. The most intricate labels, known as smart labels, encompass RFID tags or even NFC devices, catering to particularly valuable goods. Standard label dimensions generally range from 20 mm–70 mm, determined by the product type and marketing considerations. Woven labels, the most common choice for apparel and accessories, utilize fine threads to incorporate intricate details in text and patterns. Printed labels, another common option for clothing, are typically attached to or directly printed on the garment's interior.
- **Adhesive based labels:** Adhesive labels demonstrate material adaptability, being constructed from a diverse range of materials and adhering to various surfaces. Similar to fabric labels, they can be enhanced with advanced security features like custom holograms, optical variable ink (OVI), tracer in fibers, and RFID tags. The selection of adhesive material depends on the product and its environmental exposure [109]. Adhesives are further categorized based on their bond strength, offering permanent or removable options. Rubber-based adhesives offer broad surface compatibility but exhibit lower resistance to temperature and UV light compared to other options. Acrylic adhesives, while less suitable for plastics, boast superior solvent resistance and extended lifespan. Self-adhesive labels are composed of a five-layer structure. From top to bottom, they are facestock, bottom coating, adhesive, silicone coating, and base. Self-adhesive label materials offer a variety of surface finishes to choose from, including high-gloss paper, semi-gloss paper, and matte paper. Finally, acrylic blend adhesives provide the strongest adhesion but are susceptible to degradation under heat and UV light.
- **Micro engraving:** It is a printing technique which utilizes a heated die to transfer a detailed design onto a metallic foil placed between the die and the label substrate. This process not only enhances the label's visual appeal but also offers a significant level of anti-counterfeiting protection. The intricate texture engraved is difficult to replicate, making it a valuable security feature. The resulting effect is visually similar to a hologram, albeit with a distinct appearance and tactile sensation [110]

- (Figure 12). Micro-engraved patterns can be either random or incorporate customized logos, further bolstering their ability to deter counterfeiting attempts [111] (Figure 13).
- **Tags:** While tags serve as a reliable method for product identification and verification of authenticity, particularly when coupled with more sophisticated technologies like holograms, RFID tags, OVI inks, or tracer fibers, their effectiveness is ultimately limited by the tensile strength of the attachment threads. They are typically affixed to the product using resilient threads, such as nylon strings or chains. In this context, the 3D electro-mechanical tag also needs some highlight. Such chipless tags have mechanical void inclusions within them, which changes the electromagnetic behaviour and are useful in anticounterfeiting applications, serving as a digital fingerprint. They are mostly printed by the additive manufacturing process involving rapid and hassle-free prototyping. The chipless tag takes the form of a solid dielectric cylinder, presenting a homogenous exterior. However, the information is embedded within the object's internal structure. This is achieved by strategically placed voids that encode the data. This design offers a promising solution for anti-counterfeiting and security applications. It eliminates the vulnerability of information theft during the reading process or through visual inspection, a common weakness in other chipless systems. Furthermore, the data encoding method departs from the conventional on-off or amplitude schemes used in chipless RFID. Instead, it leverages a strategy that maximizes available states or non-overlapping uncertainty regions [112].



Figure 12. Micro engraving on a champagne bottle [110].

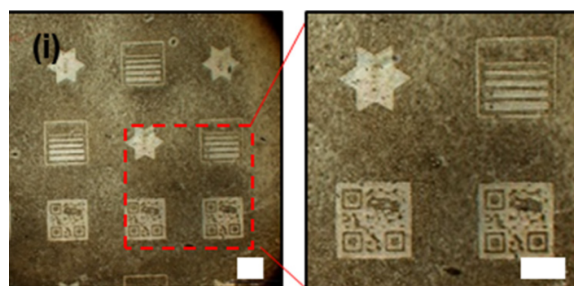


Figure 13. Image of a silver nanowire pattern fabricated using UV dicing tape, with the zoomed view [111].

4. Chemical-Based Anticounterfeiting Techniques

Chemical-based anticounterfeiting technologies rely on the incorporation of specialized materials to authenticate objects. These materials exploit the inherent randomness generated during specific processes or chemical applications, creating unique and verifiable markers. The primary function of these technologies is product authentication, not necessarily unique identification. Verification, however, often requires specialized equipment or laboratory analysis, hindering immediate on-site confirmation. While the cost of implementation for these markers is generally low, specialized reading devices can

be expensive. Consequently, verification timelines may be extended due to the need for laboratory analysis. Such techniques can further be sub-divided into the following categories:

4.1. DNA Coding

Deoxyribonucleic acid (DNA), the fundamental genetic material of all living organisms, comprises four distinct nucleobases: adenine (A), guanine (G), thymine (T), and cytosine (C). These bases form a specific sequence that encodes the genetic information. Advancements in biotechnology and molecular biology enable the controlled synthesis of DNA with a predetermined base sequence. This technology presents a novel approach for anti-counterfeiting applications. By arranging the DNA bases in unique combinations, a highly secure and verifiable identifier can be created. Additionally, encryption techniques can be employed on the DNA sequence to further enhance the security of the anticounterfeiting tag [92,113–116]. Beyond its amenability to encryption, DNA possesses a remarkable information density [117]. A single gram can theoretically store petabytes of data, making it a highly miniaturized data carrier. This characteristic, coupled with its microscopic size, renders DNA an ideal candidate for covert anti-counterfeiting tags.

A key advantage of DNA authentication labels lies in their inherent replication difficulty. Unlike conventional methods, which may be readily reproduced, the complex structure of DNA sequences poses a significant challenge to counterfeiters. Traditional techniques like Sanger sequencing and its variants, while effective for sequence determination, are often cost-prohibitive and necessitate specialized expertise. This complexity serves as an additional barrier against counterfeiting endeavors [118].

DNA coding has various practical applications, including integration into printing ink for secure barcodes and QR codes [119]. DNA can also be incorporated into degradation units to stain currency [120] or combined with blockchain for enhanced product security and offline verification [121].

DNA sequences have been attached to magnetic nanoparticles and added to liquid products like milk and oil, enabling easy retrieval and analysis [122]. Additionally, a method for labeling pharmaceutical products has been developed, with the DNA remaining stable for at least two years [123].

While DNA offers promising potential for data storage, current reading methods present a challenge. Techniques such as sequencing can be time-consuming, exceeding several hours, thus hindering practical implementation. Environmental factors like heat, pH, UV radiation, and microbial activity can degrade DNA, reducing its yield [124]. It is reasonable to assume these factors would similarly impact the performance of DNA-based coding systems. Additionally, although replicating DNA sequences is generally difficult, it becomes potentially achievable with access to specific primer pairs. A synergistic approach combining DNA with other technologies, such as nanoparticles and RFID tags, may prove advantageous. This would allow for immediate verification using RFID followed by a more definitive confirmation through DNA sequencing [125,126]. The advantages of such a methodology are pictorially depicted in Figure 14. But such a technology also comes with certain disadvantages:

- Association with products: Strategic Incorporation of DNA with important goods
- Conjugation with other technologies: Combining DNA with 1D/ 2D codes, RFID, etc.
- DNA stability and protection: Coating DNA with a protective layer
- Detection methodology: The detector should be fast, reliable and low cost

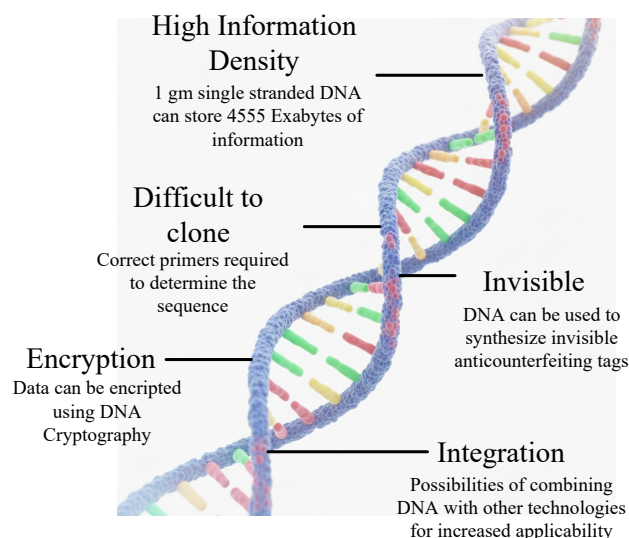


Figure 14. Primary advantages with using DNA for anti-counterfeiting applications.

4.2. Chemical Encoding

Chemical encoding and tracers offer a method for product authentication by incorporating unique and readily identifiable microscopic chemical particles into raw materials or finished goods [127]. The presence of these particles serves as a verifiable indicator of a product's legitimacy. Detection and subsequent decoding of these markers are typically performed within a laboratory setting.

There are various approaches within the domain of chemical encoding and tracing. Some methods employ chemical compounds possessing specific optical properties, such as luminescent particles, for product authentication. In this context, the use of Carbon dots (CDs) have been of particular interest to the researchers. CDs offer promising contributions to product security, environmental sustainability, and the circular economy [128]. Conversely, other techniques utilize compounds with distinct physical properties, like magnetically susceptible particles, to achieve the same objective [129–131].

4.3. Surface Analysis

Surface analysis involves surface fingerprint technologies and laser surface analysis, which offer a method for generating unique product identifiers. This approach leverages the inherent randomness of physical processes, resulting in identifiers that are inherently difficult to replicate. These technologies analyze the surface topography and structural variations of a material utilizing laser-based techniques. By identifying these distinctive surface features, a unique identifier is generated, allowing for unambiguous product authentication [132].

This principle is based on a method for generating unique identifiers encoded in readily machine-readable labels. The process involves coating a substrate with nanoparticles and subsequently applying a silicon polymer layer. As the substrate dries, it shrinks, inducing the formation of unique structural variations, or “wrinkles,” on the polymer surface. These random wrinkles are then analyzed to generate a unique identification code. Decoding necessitates a dedicated device that reads the wrinkle pattern and compares it to a reference database containing previously stored codes for verification purposes [133,134].

4.4. Glue Coding

Glue coding is combination of physical and chemical processes to generate highly secure, unique identifiers, the process being similar to ‘Adhesive based Labels’ discussed be-

fore. These identifiers manifest as intricate three-dimensional patterns formed by randomly shaped and sized miniscule polymer bubbles, generating unique digital fingerprints [135].

The versatility of glue coding allows for its application to minuscule polymer substrates, measuring only a few millimeters in size [55]. These substrates are then securely affixed to the product or its packaging, functioning as a unique and tamper-evident seal of authenticity. For verification purposes, all the polymer bubble signatures are meticulously recorded within a secure reference database. To ascertain a product's legitimacy, a specialized reading device meticulously analyzes the signature in both two and three dimensions, followed by a comparison with the signatures stored within the reference database.

In this regard, Polymer Substrate Fingerprinting (PSF) is of importance, which is mostly used to authenticate banknotes. This technique leverages the inherent randomness of the opacity coating process, a critical step in polymer banknote production. The stochastic nature of this process results in uneven coating thickness and the dispersion of ink impurities, leading to the formation of unique, random translucent patterns when the banknote is backlit [136]. During the printing process on a rotary press, the substrate makes contact with the inked cylinder while positioned between a backing roller and a gravure cylinder. The gravure cylinder features microscopic, recessed cells etched onto its surface. These cells function as ink reservoirs, collecting ink from a dedicated liquid pool as the cylinder rotates through a partial immersion. A precisely positioned, flexible blade, meticulously removes any excess ink from the gravure cylinder's surface. This ensures that ink remains solely within the recessed cells, containing unique identifiers.

5. Marking Technologies for Anticounterfeiting

Marking technologies safeguard products by applying unique security features, typically graphic patterns or encoded data, directly onto the item. These features function as verifiable identifiers that can be read with specialized tools, allowing for authentication and confirmation of a product's legitimacy, thereby protecting brands from counterfeiting and ensuring consumers receive genuine goods. The primary objective of marking technologies lies in authentication, not necessarily individual product identification. The security they offer against replication and tampering stems from two key aspects:

- The inherent properties of the technology: This encompasses the chemical and physical characteristics of the materials used, such as specialized inks with unique properties that are difficult to replicate accurately. Visual indications of tampering may also be a factor for technologies relying on overt markings.
- The encoded information within the marker: This can include complex data embedded within a graphic pattern or encrypted information within a code. The difficulty of cloning or reproducing this encoded information provides an additional layer of security.

Several different marking technologies exist, with the most prevalent being those suitable for visual inspection. This preference arises due to several factors:

- Versatility: Visual inspection allows for the application of these technologies to a wide range of products.
- Cost-effectiveness: The technology itself and verification procedures are often relatively inexpensive on a per-item basis.
- Ease of verification: In many cases, verification can be achieved through a simple visual inspection or by utilizing readily available technology such as smartphones.

5.1. Optical Memory Stripe

An optical memory stripe is a data storage technology employing a laser reading device. This technology offers high-density storage capabilities, typically up to 4 MB, for

data and images. The data is permanently etched onto the stripe using the WORM (Write Once, Read Many) method, rendering it read-only. This immutability ensures the data cannot be deleted, replaced, or tampered with after initial inscription. Due to its inherent security features, the optical memory stripe finds its most prominent application in document authentication. The technology can be integrated into plastic cards, similar to identity cards, or directly affixed to the product itself, offering a versatile solution for various authentication needs. Such a technology falls under the subset of Optical Counterfeiting.

Optical anti-counterfeiting technology leverages the interaction of light with specially designed elements embedded within a product. These elements, termed “optical reporters,” exhibit specific optical phenomena upon light interaction. These phenomena can include light scattering (e.g., Rayleigh [137,138] and Raman tags [139,140]), light emission (e.g., fluorescent marks [141]), or manipulation of light phase and interference [142].

The information encoded within a product utilizes these optical responses. The reporters are strategically distributed to create a unique “fingerprint” for the product. This fingerprint is then digitized and converted into a binary code, representing the presence or absence of specific optical features at designated locations. This binary code can then be further processed and stored within an image or label associated with the product.

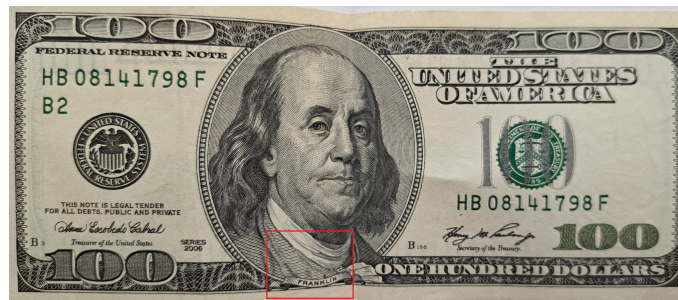
By analyzing the optical response of the product reporters and comparing it to the stored digital representation, the authenticity of the product can be verified. This approach offers a robust and secure method for combating counterfeiting. In this context, diamond forms a very versatile candidate, which can be probed in a wide-excitation wavelength range from deep-ultraviolet to infrared regimes scalable with excitation power [143–147].

5.2. Microtext

Microprinting, also known as microtext, is a covert security measure employed in various printed materials. This technique involves the reproduction of human-readable text or graphic elements at a minuscule scale, rendering them invisible to the naked eye. Detection necessitates the use of magnifying devices such as loupes. While user awareness of the feature’s presence and proper training are prerequisites for identification, advancements in printing technology have facilitated the creation of even smaller, truly invisible microstructures. This invisibility property can be leveraged as a security mechanism, as reproductions obtained through conventional copying methods fail to replicate these minute details.

Despite the availability of digital scanning and printing technologies for over two decades, microprinting remains a relevant, albeit basic, security feature. While its replicability exists, specialized knowledge is necessary for successful detection. Notably, microprinting offers several advantages: it incurs minimal production costs, can be readily implemented on a global scale, and maintains a visually unobtrusive presence.

In instances where microprinting is already in use, its continued application is justifiable due to the negligible cost factor. However, for a more robust security posture, the incorporation of cryptographic elements is highly recommended. Cryptography offers a more sophisticated layer of protection, simplifying counterfeit detection processes. Microprinting/Microtexts finds application in various security-sensitive documents and products, including banknotes [148] (shown in Figure 15), identification documents, packaging materials, labels, and pharmaceutical goods [149].



(a)



(b)

Figure 15. Microtexts on Benjamin Franklin's collar in a 100 \$ bill (a) Full, (b) Cropped, showing the microtext.

5.3. Watermark

In the field of digital communication, information hiding, also known as data embedding, refers to the process of imperceptibly modifying a carrier signal to conceal a secondary message, termed the watermark. This technique can be applied to various signal types, including audio, images, and videos.

Image watermarking, a specific application of information hiding, focuses on embedding a watermark image within a host (or cover) image. The embedded watermark is designed to be undetectable and inaccessible to unauthorized users.

Several key requirements govern the successful implementation of digital image watermarking:

- **Imperceptibility:** The watermark should not introduce noticeable degradation to the host image.
- **Invisibility:** The watermark should be visually indistinguishable from the watermarked image.
- **Robustness:** The watermark must be resistant to various attacks, such as compression, cropping, geometric distortions, noise addition, filtering, and blurring. This robustness criterion is particularly important for robust watermarks, as opposed to fragile watermarks that are designed to be easily detectable upon tampering.
- **Security:** The watermark should be secure and challenging for unauthorized individuals to extract or access.

In the Fourdrinier watermark [150] process, a specialized device known as the dandy roll facilitates the creation of watermarks within machine-made paper. This lightweight, hollow cylinder features a raised design precisely etched onto its surface. As the newly formed paper sheet travels along a conveyor belt, it encounters the dandy roll which gently

presses its design into the wet fibers. This localized pressure displaces and thins the fibers, resulting in a permanent variation in paper density that corresponds to the design.

Following the drying stage, the watermark becomes an integral part of the paper and cannot be altered. This inherent permanence imbues watermarks with security and authentication functionalities.

Amongst watermarking techniques, *Cylinder Mould watermarks* [151] are recognized for their exceptional security. These watermarks possess a three-dimensional nature, characterized by remarkable clarity and high image definition. The unique characteristic of cylinder mould papermaking lies in the creation of the watermark during the formation of the paper sheet itself. This integration results in a watermark with exceptional multi-tonal detail, as the variations in thickness become an inherent property of the paper.

5.4. Copy Detection Patterns

Printable graphic codes (PGCs), a recently developed anti-counterfeiting scheme, have gained significant traction in both industry and academia due to their affordability and robust counterfeiting deterrence capabilities. A specific type of PGC, the copy detection pattern (CDP) [152,153], derives its name from its exceptional sensitivity to unauthorized copying. CDPs typically consist of intricate pseudo-random micro-textures designed to undergo significant alterations in their textural features during illegal copying processes. These alterations can be effectively captured and analyzed through machine learning algorithms, enabling CDP-based authentication.

To combat counterfeiting of printed materials, researchers have devised innovative anti-counterfeiting patterns. These patterns can be embedded within Quick Response (QR) codes, utilizing textures or micro-features sensitive to copying processes. By incorporating additional authentication data or leveraging mobile app analysis of these patterns, they offer a robust layer of security for print matter, as exemplified by the two-level QR code, low-cost anti-copying barcode, and visually integrated QR code systems [154–157].

This technology leverages the inherent information loss that occurs during the printing and scanning of digital images. Regardless of the copying method or scanner quality, some detail inevitably degrades with each reproduction cycle. CDPs are meticulously designed to amplify this information loss during the copying process. Since a counterfeit CDP will have undergone at least one additional copying cycle compared to the original, the resulting image will contain a noticeably lower level of information compared to the authentic version.

Conventionally, the CDP-based authenticity identification methods suffer from several limitations:

- **Reliance on Traditional Machine Learning:** Existing approaches typically rely on traditional machine learning algorithms. These methods require manual feature extraction and selection by experts, often based on experience. This process necessitates the collection of vast datasets containing genuine and forged CDP images. Subsequently, features that best differentiate authentic from forged patterns are manually chosen. However, such traditional features are limited in their ability to represent complex information. Designing robust and highly discriminative manual features becomes increasingly challenging due to the rapid advancements in electronic equipment and increasingly sophisticated counterfeiting techniques. The inability to anticipate all potential forgery methods during design can lead to a decline in the effectiveness of traditional feature differentiation.
- **Limited Mobile Integration:** Most current identification methods require specialized equipment, hindering their accessibility for mobile device use. Dedicated and user-

friendly anti-counterfeiting pattern authentication solutions for mobile platforms remain underdeveloped.

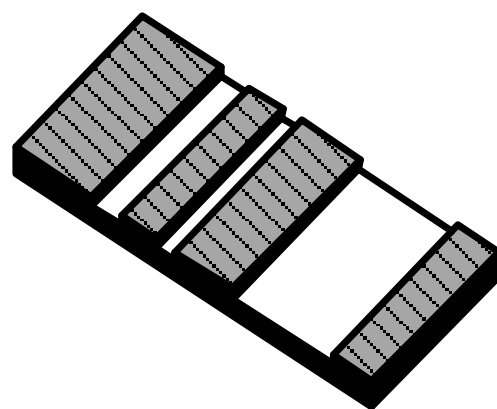
- **Impact of Image Blur on Mobile Capture:** Blur degradation frequently occurs in CDP images captured using mobile devices. This degradation stems from factors such as relative motion between the camera and the pattern, focusing errors, and other limitations inherent to mobile device photography. The resulting image quality reduction can negatively impact the accuracy of CDP authenticity identification. Consequently, the design of identification algorithms for mobile platforms needs to address the challenges posed by image blur and minimize its influence on authentication outcomes.

5.5. Guilloche Printing

The term “guilloche” originates from the French word denoting an ornamental design created through the engraving of metal plates. Guilloches are intricate designs characterized by the meticulous interweaving of fine lines, frequently encountered as a security feature on banknotes. Guilloche printing represents one of the longest-standing industrial security measures employed in the printing industry. Traditionally, authentic guilloches are produced using the *intaglio printing method*, a process known for its high cost and reliance on specialized printing equipment typically reserved for high-security documents. The vast majority of intaglio plates utilize a standardized printing method involving a roller press. This press consists of horizontally positioned bearing roller with a movable flatbed situated between them. A viscous ink is applied to the plate’s recessed areas using a roller, followed by the removal of excess ink. The inked plate is then positioned face-up on the press bed. A damp sheet of paper is placed on top, and a blanket is subsequently draped over both to ensure even pressure distribution. The printing process commences with the rotation of the upper roller, drawing the bed through the press. During this stage, immense pressure, measured in several tons, is exerted through the blanket. This forceful compression drives the damp paper into the ink-filled grooves of the plate, transferring the image and creating the final print (shown pictorially in Figure 16).

A less expensive alternative exists in the form of *offset lithography* (mass-production printing) in which the images on metal plates are transferred (offset) to rubber blankets or rollers and then to the print media. This method yields guilloches that are significantly easier to replicate. Additionally, the inherent visibility of offset-printed guilloches poses a limitation. However, the cost-effectiveness of this approach makes it a viable option for creating a visual deterrent against counterfeiting in applications such as security documents, tickets, and certificates.

Essentially, guilloches are assessed by close visual inspection: mechanical copies lose the fine-line structure of the original, and hence can be used for anticounterfeiting.



(a)

Figure 16. Cont.

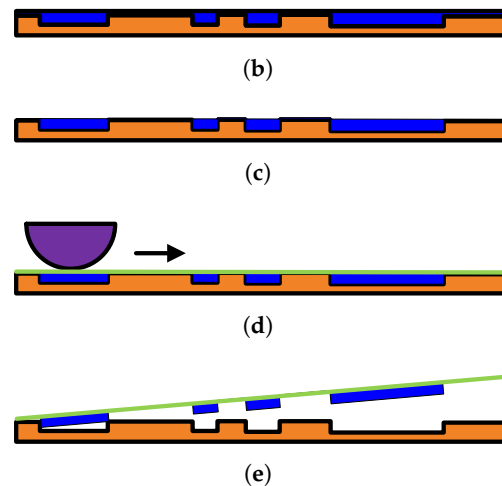


Figure 16. Traditional intaglio printing method (a) Depressions cut in the printing plate, (b) Plate covered by ink (blue), (c) Removal of excess ink, while keeping only inside the grooves, (d) Paper (green) placed on top and run with a heavy roller (violet), and (e) paper is removed with the ink being transferred to the paper.

5.6. Security Holograms

The invention of rainbow holography by Stephen Benton [158] marked a turning point in security technology. This innovation, coupled with the subsequent development of hologram micro-embossing [159], paved the way for the mass production of holograms.

Beyond traditional holography, a diverse range of diffractive microstructures [160] have been developed. These are commonly referred to as diffractive optically variable image devices (DOVIDs). DOVIDs are now manufactured not only through holographic and laser interference techniques, but also by employing advanced electron beam lithography.

In addition to diffractive security structures, advancements have been made in microstructures based on thin film interference [161]. Many of these interference structures, known as interference security image structures (ISIS), are currently produced using sophisticated vacuum deposition technologies [162].

5.6.1. Diffractive Optically Variable Image Devices—DOVIDs

DOVIDs are based on the principle of first/ higher order diffraction. These devices, also referred to as first-order DOVIDs (FODs), utilize gratings with line periods comparable to the wavelength of light. In contrast, zero-order DOVIDs (ZODs) employ gratings with an even smaller line period, leading to significantly different optical properties compared to FODs [163].

The production of DOVIDs involves the exposure of a photosensitive material, typically a photoresist. Subsequently, electroplating is used to generate embossing masters from the exposed and developed micro-relief structures. The specific method employed for photoresist exposure plays a critical role in determining the security value of the resulting DOVID. Two primary techniques dominate this process: traditional light interference and advanced lithographic methods.

In the traditional method, the photo-resist is exposed by two laser beams, incident at different angles, to create a line pattern. Consequently, DOVIDs manufactured through such a technique exhibit an identical appearance when viewed under both positive and negative first-order diffracted light.

In contrast, advanced lithographic techniques, such as electron beam lithography, enable the line-by-line exposure of gratings directly into suitable photoresists [164]. This approach facilitates the creation of blazed gratings, characterized by an asymmetric cross-section. Blazed gratings exhibit the property of diffracting light significantly more efficiently

into the positive first order compared to the negative first order [165–167]. Consequently, DOVIDs incorporating blazed gratings display a marked contrast difference between the positive and negative first-order diffracted light.

5.6.2. Interference Security Image Structures (ISISs)

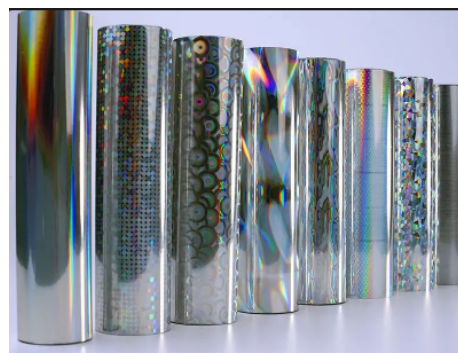
DOVIDs and ISISs serve as counterparts to each other, while DOVIDs are composed of adjacent fringes, ISIS consists of one or more thin films, thus resulting in volume reflection. They are built up of single layers, displaying a colour shift with angle of observation, but having low reflectivity; or multilayered geometry, comprising of refractive-type multilayers [168] and Bragg-type multilayers [169].

Conventionally, traditional holography is more in use for anticounterfeiting, and the methods to fabricate them can briefly be enumerated as:

- **2D/3D holograms (multilayered):** Two-dimensional and three-dimensional (2D/3D) holograms achieve a three-dimensional appearance by employing a series of visually layered two-dimensional diffractive elements. These elements contain holographic images carefully positioned behind one another to create a perceived depth, utilizing multiple layers. This technique offers substantial depth perception between the layers, often accompanied by a distinct shine on the topmost layer. Due to its established nature of over 20 years and proven effectiveness in generating high-quality security features, 2D/3D holography remains the dominant technology for most commercially available holographic stickers. These holograms exhibit a distinctive multilayered and multicolored appearance. One or two levels of two-dimensional graphics appear to ‘float’ above or reside on the surface of the hologram. The background elements seemingly lie beneath or behind the hologram, creating a convincing illusion of depth (as shown in Figure 17a).
- **3D holograms:** These holograms possess a three-dimensional quality, encompassing length, breadth, and depth. This illusion of depth arises from the utilization of a three-dimensional physical model that appears to project from the holographic plane. In essence, the holographic image captures the complete set of data pertaining to the wavefront emitted by an illuminated object.
- **Dot-Matrix:** In this technique, computer-controlled manipulation arranges microscopic dots into a well-defined relief structure. These precisely positioned dots act as a diffraction grating, selectively scattering light to reconstruct a holographic image. The computer generates a vast array of these dots, forming an intricate structure with diffractive properties. Dot-matrix holograms utilize multiple laser beams to create a pattern of minute, engraved dots. Each dot possesses a unique diffraction pattern, contributing to the hologram’s security features. The resulting visual effect is aesthetically pleasing, often exhibiting dynamic kinetic effects and displaying variable images with a high-quality finish.
- **Hot Stamping Foil (HSF):** In this method, pre-dried inks or foils are adhered to a target surface using high temperatures. Dry lithography finds extensive application in securing paper and plastic products, although its versatility allows for its use with various other materials (Figure 17b).
- **De-metallized holograms:** In this process, a layer of aluminium is deposited onto the hologram. Subsequently, specific regions are selectively removed to create a desired graphic pattern. This technique enables the creation of printouts containing both metallized and transparent areas on a single film, offering enhanced security features or improved design aesthetics [170].



(a)



(b)

Figure 17. Traditional holograms (a) 2D/3D holograms in Indian Railways for transport, (b) HSF foils for anticounterfeiting and cosmetic packaging.

Complex holograms offer a layered approach to authentication, encompassing both overt and covert elements. The readily apparent holographic image provides a first level of immediate verification. Embedded within this visible image lies a layer of covert information invisible to the naked eye. This hidden data can take the form of microtext, encoded messages (cryptograms), or other security features. Reading this concealed information necessitates the use of specialized tools such as magnification lenses, microscopes, lasers, etc.

5.7. Machine Readable Codes

Machine-readable identification codes, often referred to as barcodes, are symbolic representations of data intended for automated capture and processing by machines, typically utilizing optical scanning technologies. They can be classified into the following two categories:

5.7.1. One-Dimensional Code

One-dimensional barcodes exist in a variety of standardized symbologies. These symbologies typically include a corresponding plain text representation for human readability. Each barcode type possesses a defined character set (e.g., numeric only, alphanumeric, or including special characters) and may have limitations on the total number of encoded characters. For instance, Code 128 allows for the encoding of up to 128 unique symbols, while Code 39 is limited to 39. Conversely, certain barcode types have predetermined code lengths, such as EAN-13 [171] with its fixed 13-digit format and UPC-A [172] with its fixed

12-digit format. Such barcodes can easily be attached to products either via adhesive labels or by printing them directly onto the products or packaging.

5.7.2. Two-Dimensional Code

Unlike one-dimensional barcodes, which necessitate access to a corresponding database for the retrieval of encoded product data, two-dimensional barcodes possess the capability to store internally all information necessary for product identification. This enables them to directly deliver a data file containing the encoded information upon scanning. Additionally, two-dimensional barcodes can encode a unique web address (URL), facilitating the retrieval of pertinent product-level or, in the case of serialized codes, item-level data from cloud storage. The most widely used 2D codes are the quick response (QR) code and the 2D datamatrix.

It is worth noting here that machine readable codes (1D or 2D) doesnot offer protection against duplication. However, can be integrated with supplementary authentication technologies, including holograms, copy detection patterns, or unique identifiers facilitating the implementation of automated authentication processes via a smartphone scan.

5.8. Inks

Security inks are a valuable tool in the fight against counterfeiting in various industries. They are used to protect pharmaceutical packaging, add covert markings to documents, and include tamper-evident features in food, textiles, artwork, and other products. These inks come in different colors and use complex authentication methods, making it difficult for counterfeiters to replicate or forge products. In addition to product authentication, ink-based technologies can also be used for identification and tracking by including unique product codes/identifiers in the markings. They can be classified into the following categories:

5.8.1. UV Sensitive

This technology uses special ink that can be seen under regular light but changes color or it appearance when exposed to ultraviolet (UV) light. This effect is due to the ink containing fluorescent pigments, which appear different colors under visible light versus UV light. Detecting these markings requires equipment that emits electromagnetic radiation mainly in the UV spectrum, with possibly some emission in the visible range as well. In the recent years, there has also been considerable research on organic compounds (vegetable oils) based UV-luminescent ink [173–176].

There has also been research on color-coded microcapsules with UV-sensitive ink [177]. These tiny capsules are applied on the surface or embedded within the product and can only be seen under an electron microscope. Finding specific UV-sensitive inks like photochromic and “white” multispectral inks [178] is quite tough. As a result, the markings made with these inks are extremely hard to copy, providing excellent protection against counterfeiting.

5.8.2. IR Sensitive

Offering both transparent and opaque formulations, infrared-sensitive inks provide a versatile security measure. A particularly intriguing type within this category is the “metamaterial” ink [179]. These inks consist of paired colors that appear identical under normal light, but reveal a hidden mismatch when viewed under infrared illumination.

Infrared inks, unlike their UV-sensitive counterparts, boast impressive longevity. This makes them ideal for a wide range of applications, from securing banknotes and important documents to safeguarding any valuable paper-based item.

5.8.3. Magnetic

A prominent example of magnetic ink technology is Magnetic Ink Character Recognition (MICR). Employed in numerous countries, MICR encodes a set of characters, typically found on the bottom of cheques, for efficient machine reading. Defined by the ISO 1004 standard [180], MICR characters are magnetized within the plane of the paper, facilitating reliable identification by character recognition systems even when obscured by conventional inks.

5.8.4. Thermochromic

Thermochromic inks exhibit a remarkable property: they alter color in response to temperature fluctuations [181–184]. Various types exist, with some inks responding to heat, others to cold. The color change can be temporary or permanent. Notably, some thermochromic inks utilize microcapsules containing a colorant. Upon exceeding a specific temperature threshold, these microcapsules become transparent, revealing the underlying background. Conversely, a temperature decrease triggers a return to the original color. The transparency point depends on a combination of factors including temperature, chosen color, concentration, and ink thickness. Standardized inks typically lose 95% of their color at either 6 °C or 31 °C.

Thermochromic inks find application in a wide array of products and packaging. However, it is crucial to note that prolonged exposure to high temperatures (exceeding 50 °C), UV light, specific fluorescent lights, or even excessive sunlight can diminish or even eradicate their color-changing sensitivity.

5.8.5. Reactive

Reactive inks offer a robust method for deterring and detecting document counterfeiting [185]. These inks exhibit an immediate and visually discernible response upon exposure to tampering liquids or chemicals. For instance, a document printed with ink that vanishes or changes color upon contact with specific reagents would readily reveal any attempt to alter its content through chemical manipulation.

Further on, such ink can be sub-categorized as:

- **Erasable:** Erasable inks are often employed in a background capacity for specific documents. Their functionality becomes apparent when an attempt is made to erase information, as the ink readily succumbs to friction and disappears [186]. This characteristic makes them particularly valuable for safeguarding documents like checks and certificates against unauthorized alterations. Notably, erasable inks are best suited for dry and wet offset printing methods and are incompatible with laser printing technology.
- **Solvent-sensitive:** Designed to thwart forgery attempts, solvent-sensitive inks exhibit a marked reaction upon exposure to specific solvents or chemicals commonly used for tampering, such as bleach, alcohol, or acetone. This reaction manifests as a visible transformation of the ink, including running, color change, or stain development, thereby exposing any attempt to alter the document.
- **Fugitive:** Fugitive inks offer a security measure by readily revealing tampering attempts. These inks are formulated to react with water-based solutions (aqueous solutions) or other inks, causing visible smudging within the printed area [187]. This characteristic makes them particularly useful for safeguarding documents like checks, where any effort to alter the content with ink or a liquid solution would be readily apparent due to the resulting smudges.

5.8.6. Penetrating

Penetrating inks possess a high degree of fluidity and readily permeate the underlying material upon contact. This infiltration process creates a faint stain surrounding the printed image, visible on the reverse side of the document as well. These inks are typically employed in the letterpress printing technique. An alternative method involves incorporating a colored oil into the ink formulation. This oil, possessing similar penetrative properties, migrates deep into the paper's pores, generating a colored halo around the printed number. Any attempt to tamper with the number, such as scraping or correction, would leave the stain behind, rendering the counterfeiting of the serial number readily apparent.

Some other varieties of ink, which are less commonly used include:

- **Optically Variable Ink—OVI:** This ink incorporates a unique feature—microscopic metallic film flakes. These flakes endow the ink with a remarkable optical property—its color exhibits variation depending on the viewing angle [188,189].
- **Biometric Taggants:** These inks incorporate covert security elements in the form of DNA taggants [119]. These microscopic markers react to designated solvents or require specialized equipment for detection. This technology facilitates the authentication of a wide range of products and documents. In essence, DNA taggants function as a hidden layer of security that necessitates technical expertise to verify the genuineness of an item.
- **Bleeding Ink:** This security ink offers a convenient method for document authentication. While appearing black upon printing, it undergoes a chromatic shift to red when exposed to a water-based solution (aqueous solution). This transformation allows for straightforward verification without the need for specialized reagents. The application process is simple, requiring only a moistened fingertip to be drawn across the printed area, initiating the color change to red. It is important to note that this ink is specifically suited for dry offset printing.
- **Metameric Ink:** These inks leverage the principle of metamerism, where the combination of two colors creates a resultant appearance that varies under different lighting conditions. This phenomenon allows for the covert integration of security features, such as numbers only visible when viewed under a particular coloured filter [190].

6. Discussion

Battling against fakes demands robust security layers. Hardware technologies offer strong protection. This review examines various techniques contributing unique authentication elements, including electronic techniques, mechanical techniques, chemical techniques, and marking based techniques.

However, no single method is flawless. Counterfeiters adapt continuously, demanding multi-layered strategies. Combining these hardware-based technologies with complementary measures becomes crucial:

- **Tamper-evident Packaging:** Packaging with self-destructing seals or unique identification codes discourages tampering and provides additional layers of verification.
- **Supply Chain Management:** Robust tracking systems from manufacturing to distribution can identify and eliminate potential vulnerabilities within the supply chain.
- **Digital Authentication:** Implementing product serialization and track-and-trace systems provide a digital layer of verification. Products with unique identifiers can be authenticated through online databases, further strengthening the anti-counterfeiting strategy.

Table 3 provides a normalized comparison of different anti-counterfeiting technologies based on key metrics. The scores, from 1 (low) to 5 (high), illustrate the trajectory toward

more robust and integrated solutions. It should be noted here that the values in the table are based on the outcome of the research provided as references.

Table 3. Comparative Analysis of Anti-Counterfeiting Technologies. * 1 (high error rate) to 5 (extremely low error rate).

Technology	Economical	Read Range	Robustness (Unclonability)	Error Rates *	Ease of Integration	Industry Applicability	Effectiveness over Time
NFC	4	1	2	4–5	2	5 (Versatile)	3–4
Magnetic Stripes	5	1	1	2	2	3 (Banking and credit cards)	1
Contact chips	4	1	3–4	4–5	2	4 (Credit cards)	5
Electronic seals	5	3–5	3–5	4–5	1	2 (Document authentication)	5
RFID	5	1–5	2–5	3–5	2	5 (Versatile)	2–5
Security films	4	1–2	3–5	4	3	2 (Packaging)	4
Engravings	1	1	1–4	4	1	3 (High value goods)	2–4
Mechanical Seals	5	1	1–2	4	3	1 (Highly specialized tech.)	1
Labels	5	1–2	2–5	3–4	5	5 (Versatile)	2–4
DNA coding	1	1–2	5	5	1	2 (Pharma and luxury goods)	5
Chemical encoding	2	1–2	4–5	5	1	2 (Pharma and luxury goods)	5
Glue coding	2	1–2	4–5	5	1	1 (Highly specialized tech.)	5
Surface analysis	2	1–2	4–5	5	1	1 (Highly specialized tech.)	5
Microtext	4	1	2–3	4	4	4 (Versatile)	2
Optical memory stripes	3	1	2	3	3	2 (Secured documents, passports)	2
Copy detection patterns	5	1	3–4	4	3	3 (Documents, ID cards, certificates)	3
Watermarks	4	1	2	4	5	3 (Secure documents)	2
Guilloche printing	5	1	3	4	5	3 (Secure documents)	2
Security holograms	4	1	3–4	4	2	4 (Applicable across industries)	4
Machine readable codes	4	1–3	2	4	4	5 (Highly Versatile)	1
Inks	1	1–2	2–3	4	5	5 (Highly versatile)	2–3

To sum up the discussion, it has been segregated into two major categories:

- Our current scenario
 - The market for anti-counterfeiting/secure packaging solutions is large and growing fast as brands and regulators respond to growing counterfeit volumes [191].

- Solutions today are a mix of physical features (holograms, optically variable inks, taggants), authentication layers (NFC/QR with backend verification), and forensic/lab methods (molecular taggants, DNA, isotopic markers)
- High-impact trends
 - Molecular/DNA taggants moving from niche to viable commercial use—New hybrid DNA and polynucleotide tag systems allow microscopic, hard-to-copy markers that can be read with paper/kit-based or lab readers; these are now appearing in high-security trials and patents. This makes authenticity tied to chemistry rather than optics alone [192].
 - Scalability of Smart packaging (NFC + consumer verification)—NFC and tamper-aware chips are increasingly embedded in pharma, luxury, and packaging so consumers (or customs officers) can verify origin or a tamper flag with a smartphone. Expect rapid adoption where consumer trust and safety are critical [193].
 - Blockchain and product-level digital ledgers for provenance—Blockchain (plus IoT anchors) is maturing as a tool for immutable provenance records along supply chains; it is shifting from pilot projects to production deployments for high-value goods and regulated products [194].
 - AI, computer vision and signal analysis for detection—Deep-learning models detect subtle optical, spectral or electrical signatures (e.g., for semiconductor chips or packaging) that humans miss; universities and standards labs have recently published promising prototypes. Expect AI to be used both for automated inspection and for flagging suspicious supply-chain behavior [195].
 - Market growth and industry consolidation—Industry reports show strong CAGR in secure packaging and anti-counterfeit markets as companies buy, integrate, and scale these technologies. Investment into combined physical + digital stacks is increasing [191].

In a nutshell, anti-counterfeiting is shifting from one-off visible tricks to integrated, layered systems that combine molecular forensics, embedded electronics, cryptographic provenance, and AI detection—brands that adopt multiple independent roots of trust and participate in shared provenance networks will be hardest to counterfeit [192,193,195,196].

Author Contributions: S.C. and S.G.: Conceptualization, S.C.: writing—original draft preparation, F.C., G.M. and S.G.: Review and editing, S.G.: Supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Italian Ministry of Education and Research (MUR) in the framework of the Crosslab and Forelab projects (Departments of Excellence).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. The Economic Impacts of Counterfeiting and Piracy—Report prepared for BASCAP and INTA. *Front. Econ.* **2017**.
2. Available online: <https://www.asianage.com/business/counterfeiters-use-e-com-target-larger-audiences-613/> (accessed on 3 April 2024).
3. Angrist, J.D.; Pischke, J.S. *Mostly Harmless Econometrics: An Empiricist's Companion*; Princeton University Press: Princeton, NJ, USA, 2009.
4. Available online: <https://www.trustconcept.com/en/newsroom/news/whitepapers/white-paper-how-counterfeit-proof-is-your-product/> (accessed on 3 April 2024).

5. Sola, A.; Sai, Y.; Trinchì, A.; Chu, C.; Shen, S.; Chen, S. How can we provide additively manufactured parts with a fingerprint? A review of tagging strategies in additive manufacturing. *Materials* **2021**, *15*, 85. [CrossRef] [PubMed]
6. Butt, I.; Al Balushi, M.K.; Lee, S.H.; Mohan, M.; Ahmad Khan, N.; Haines, S. Four decades of counterfeit research: A bibliometric analysis. *Cogent Bus. Manag.* **2023**, *10*, 2284814.
7. Subramaniam, R.; Azzuhri, S.R.; Wah, T.Y.; Mahmood, A.; Balakrishnan, V. A Holistic Anti-Counterfeiting Platform Using NFC and Blockchain Technologies. *Comput. Mater. Contin.* **2025**, *83*, 4257–4280.
8. Smith, C.L.; Brooks, D.J. Chapter 7—Integrated Identification Technology. In *Security Science*; Smith, C.L., Brooks, D.J., Eds.; Butterworth-Heinemann: Boston, MA, USA, 2013; pp. 153–175. [CrossRef]
9. Hummel, R.E. Applications in Electronic Properties of Materials. In *Electronic Properties of Materials*; Springer: New York, NY, USA, 2011; pp. 385–401. [CrossRef]
10. Inoue, A.; Kong, F. Soft Magnetic Materials. In *Encyclopedia of Smart Materials*; Olabi, A.G., Ed.; Elsevier: Oxford, UK, 2022; pp. 10–23. [CrossRef]
11. Husemann, D. The smart card: Don't leave home without it. *IEEE Concurr.* **1999**, *7*, 24–27. [CrossRef]
12. Yadav, S.; Verma, S. A Comprehensive Study of Security Features for Modern Payment Services Cards and Identity Cards. *Int. J. Adv. Res. Multidiscip. Trends (IJARMT)* **2025**, *2*, 675–683.
13. Shelfer, K.M.; Procaccino, J.D. Smart card evolution. *Commun. ACM* **2002**, *45*, 83–88. [CrossRef]
14. Rankl, W.; Effing, W. *Smart Card Handbook*; John Wiley & Sons: Hoboken, NJ, USA, 2004.
15. Chin, L.P.; Wu, C.L. The role of electronic container seal (E-seal) with RFID technology in the container security initiatives. In Proceedings of the 2004 International Conference on MEMS, NANO and Smart Systems (ICMENS'04), Banff, AB, Canada, 25–27 August 2004; pp. 116–120.
16. Kadir, E.A.; Rosa, S.L.; Gunawan, H. Application of RFID technology and e-seal in container terminal process. In Proceedings of the 2016 4th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 25–27 May 2016; pp. 1–6.
17. Yeun, C.Y.; Shemali, M.A.B.; Zemerly, M.J.; Mubarak, K.; Yeun, H.K.; Chang, Y.S.; Zafar, B.; Simsim, M.; Salih, Y. ID-based secure real-time tracking system. *Int. J. Adv. Logist.* **2015**, *4*, 100–114. [CrossRef]
18. Lampe, M.; Strassner, M.; Fleisch, E. RFID in movable asset management. In *Ubiquitous and Pervasive Commerce: New Frontiers for Electronic Business*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 53–71.
19. Min, J.U.; Park, M. Electronic cargo seal for safe and secure supply chain traceability. *J. Int. Logist. Trade* **2007**, *5*, 47–56. [CrossRef]
20. Available online: <https://www.entrust.com/sites/default/files/documentation/whitepapers/rss-electronic-and-digital-signatures-wp.pdf/> (accessed on 4 April 2024).
21. Available online: <https://web.customs.gov.tw/en/singlehtml/3428?cntId=242f4a635e4646749f0c46f2cf248901> (accessed on 8 May 2024).
22. Shah, R.Y.; Prajapati, P.N.; Agrawal, Y. Anticounterfeit packaging technologies. *J. Adv. Pharm. Technol. Res.* **2010**, *1*, 368–373. [CrossRef]
23. Bansal, D.; Malla, S.; Gudala, K.; Tiwari, P. Anti-counterfeit technologies: A pharmaceutical industry perspective. *Sci. Pharm.* **2013**, *81*, 1–14. [CrossRef] [PubMed]
24. Soon, J.M.; Manning, L. Developing anti-counterfeiting measures: The role of smart packaging. *Food Res. Int.* **2019**, *123*, 135–143. [CrossRef] [PubMed]
25. Xianyu, B.; Jianzhong, Z.; Qian, F.; Yun, G. Efficient electronic seal system. *Appl. Mech. Mater.* **2014**, *610*, 221–224.
26. Maritano, V.; Barge, P.; Biglia, A.; Comba, L.; Aimonino, D.R.; Tortia, C.; Gay, P. Anticounterfeiting and Fraud Mitigation Solutions for High-value Food Products. *J. Food Prot.* **2024**, *87*, 100251. [CrossRef]
27. Available online: <https://www.agid.gov.it/en/platforms/procurement> (accessed on 10 June 2024).
28. Available online: https://www.thailand.go.th/issue-focus-detail/006_098 (accessed on 10 June 2024).
29. Juels, A.; Weis, S.A. Authenticating pervasive devices with human protocols. In Proceedings of the Advances in Cryptology—CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005; Proceedings 25; Springer: Berlin/Heidelberg, Germany, 2005; pp. 293–308.
30. Hunt, V.D.; Puglia, A.; Puglia, M. History and evolution of RFID technology. In *Pošta, Telekomunikácie a Elektronický Obchod*; Wiley Telecom: Hoboken, NJ, USA, 2007; pp. 17–22.
31. Curty, J.P.; Joehl, N.; Krummenacher, F.; Dehollain, C.; Declercq, M. A model for μ -power rectifier analysis and design. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2005**, *52*, 2771–2779. [CrossRef]
32. Available online: https://sweet.ua.pt/andre.zuquete/Aulas/IRFID/11-12/docs/IRFID_nbc_3.pdf (accessed on 11 June 2024).
33. Sidén, J.; Nilsson, H.E. RFID Antennas—Possibilities and Limitations. *Radio Freq. Identif. Fundam. Appl. Des. Methods Solut.* **2010**, *5*, 324.
34. Nikitin, P.V.; Rao, K.S. Theory and measurement of backscattering from RFID tags. *IEEE Antennas Propag. Mag.* **2006**, *48*, 212–218. [CrossRef]

35. Available online: <https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid/> (accessed on 3 June 2024).
36. Sahin, S.; Ozcan, H.; Kucuk, K. Smarttag: An indoor positioning system based on smart transmit power scheme using active tags. *IEEE Access* **2018**, *6*, 23500–23510. [\[CrossRef\]](#)
37. Molapo, N.A.; Malekian, R.; Nair, L. Real-time livestock tracking system with integration of sensors and beacon navigation. *Wirel. Pers. Commun.* **2019**, *104*, 853–879. [\[CrossRef\]](#)
38. Periša, M.; Cvitić, I.; Peraković, D.; Husnjak, S. Beacon technology for real-time informing the traffic network users about the environment. *Transport* **2019**, *34*, 373–382. [\[CrossRef\]](#)
39. Available online: <https://www.ti.com/sc/docs/products/micro/msp430/39113.pdf> (accessed on 2 May 2024).
40. Solar, H.; Beriain, A.; Berenguer, R.; Sosa, J.; Montiel-Nelson, J.A. Semi-Passive UHF RFID Sensor Tags: A Comprehensive Review. *IEEE Access* **2023**, *11*, 135583–135599. [\[CrossRef\]](#)
41. Available online: <https://www.digikey.com/> (accessed on 3 May 2024).
42. Ali, Z.; Perret, E.; Barbot, N.; Siragusa, R. *Chipless RFID Authentication: Design, Realization and Characterization*; John Wiley & Sons: Hoboken, NJ, USA, 2022.
43. Brinker, K.R.; Zoughi, R. A review of chipless RFID measurement methods, response detection approaches, and decoding techniques. *IEEE Open J. Instrum. Meas.* **2022**, *1*, 1–31. [\[CrossRef\]](#)
44. Lopez-Iturri, P.; Ruiz-Feliú, R.; Guembe, I.P.; Klaina, H.; Francés, F.J.T.; Martinez, P.; Amado, I.N.; Basarte, E.; Morentin, J.; Saenz, A.G.; et al. Implementation of a low-cost chipless RFID system with paper-based substrates printed tags for traceability applications in the packaging sector. *IEEE Sens. J.* **2023**, *23*, 14923–14937. [\[CrossRef\]](#)
45. Karmakar, N.C.; Amin, E.M.; Saha, J.K. Literature Review. In *Chipless RFID Sensors*; John Wiley & Sons: Hoboken, NJ, USA, 2016; pp. 13–28. [\[CrossRef\]](#)
46. Khadka, G.; Feng, J.; Karmakar, N.C. Chipless rfid: A low-cost consumer electronics in the retail marketplace for moving item detection. In Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019; pp. 618–621.
47. Subrahmannian, A.; Behera, S.K. Chipless RFID sensors for IoT-based healthcare applications: A review of state of the art. *IEEE Trans. Instrum. Meas.* **2022**, *71*, 1–20. [\[CrossRef\]](#)
48. Herrojo, C.; Mata-Contreras, J.; Nunez, A.; Paredes, F.; Ramon, E.; Martin, F. Near-field chipless-RFID system with high data capacity for security and authentication applications. *IEEE Trans. Microw. Theory Tech.* **2017**, *65*, 5298–5308. [\[CrossRef\]](#)
49. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030. [\[CrossRef\]](#) [\[PubMed\]](#)
50. Scholz, A.; Zimmermann, L.; Gengenbach, U.; Koker, L.; Chen, Z.; Hahn, H.; Sikora, A.; Tahoori, M.B.; Aghassi-Hagmann, J. Hybrid low-voltage physical unclonable function based on inkjet-printed metal-oxide transistors. *Nat. Commun.* **2020**, *11*, 5543. [\[CrossRef\]](#) [\[PubMed\]](#)
51. Gao, B.; Lin, B.; Pang, Y.; Xu, F.; Lu, Y.; Chiu, Y.C.; Liu, Z.; Tang, J.; Chang, M.F.; Qian, H.; et al. Concealable physically unclonable function chip with a memristor array. *Sci. Adv.* **2022**, *8*, eabn7753. [\[CrossRef\]](#) [\[PubMed\]](#)
52. Yang, M.; Ye, Z.; Pan, H.; Farhat, M.; Cetin, A.E.; Chen, P.Y. Electromagnetically unclonable functions generated by non-Hermitian absorber-emitter. *Sci. Adv.* **2023**, *9*, eadg7481. [\[CrossRef\]](#)
53. Gao, Y.; Al-Sarawi, S.F.; Abbott, D. Physical unclonable functions. *Nat. Electron.* **2020**, *3*, 81–91. [\[CrossRef\]](#)
54. Tarik, F.B.; Famili, A.; Lao, Y.; Ryckman, J.D. Scalable and CMOS compatible silicon photonic physical unclonable functions for supply chain assurance. *Sci. Rep.* **2022**, *12*, 15653. [\[CrossRef\]](#) [\[PubMed\]](#)
55. Tsai, W.K.; Lai, Y.S.; Tseng, P.J.; Liao, C.H.; Chan, Y.H. Dual colorimetric and fluorescent authentication based on semiconducting polymer dots for anticounterfeiting applications. *ACS Appl. Mater. Interfaces* **2017**, *9*, 30918–30924. [\[CrossRef\]](#)
56. Alidaei-Sharif, H.; Roghani-Mamaqani, H.; Babazadeh-Mamaqani, M.; Sahandi-Zangabad, K.; Abdollahi, A.; Salami-Kalajahi, M. Photochromic polymer nanoparticles as highly efficient anticounterfeiting nanoinks for development of photo-switchable encoded tags. *J. Photochem. Photobiol. A Chem.* **2023**, *436*, 114343. [\[CrossRef\]](#)
57. Dong, Y.; Ling, Y.; Wang, D.; Liu, Y.; Chen, X.; Zheng, S.; Wu, X.; Shen, J.; Feng, S.; Zhang, J.; et al. Harnessing molecular isomerization in polymer gels for sequential logic encryption and anticounterfeiting. *Sci. Adv.* **2022**, *8*, eadd1980. [\[CrossRef\]](#)
58. Liu, Y.; Han, F.; Li, F.; Zhao, Y.; Chen, M.; Xu, Z.; Zheng, X.; Hu, H.; Yao, J.; Guo, T.; et al. Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication. *Nat. Commun.* **2019**, *10*, 2409. [\[CrossRef\]](#) [\[PubMed\]](#)
59. Yakunin, S.; Chaaban, J.; Benin, B.M.; Cherniukh, I.; Bernasconi, C.; Landuyt, A.; Shynkarenko, Y.; Bolat, S.; Hofer, C.; Romanyuk, Y.E.; et al. Radiative lifetime-encoded unicolour security tags using perovskite nanocrystals. *Nat. Commun.* **2021**, *12*, 981. [\[CrossRef\]](#)
60. Gao, Z.; Han, Y.; Wang, F. Cooperative supramolecular polymers with anthracene–endoperoxide photo-switching for fluorescent anti-counterfeiting. *Nat. Commun.* **2018**, *9*, 3977. [\[CrossRef\]](#)
61. Zhang, J.; Liu, Y.; Njel, C.; Ronneberger, S.; Tarakina, N.V.; Loeffler, F.F. An all-in-one nanoprinting approach for the synthesis of a nanofilm library for unclonable anti-counterfeiting applications. *Nat. Nanotechnol.* **2023**, *18*, 1027–1035. [\[CrossRef\]](#)

62. Wang, K.; Shi, J.; Lai, W.; He, Q.; Xu, J.; Ni, Z.; Liu, X.; Pi, X.; Yang, D. All-silicon multidimensionally-encoded optical physical unclonable functions for integrated circuit anti-counterfeiting. *Nat. Commun.* **2024**, *15*, 3203. [\[CrossRef\]](#)
63. Rong, Y.; Wu, C.; Yu, J.; Zhang, X.; Ye, F.; Zeigler, M.; Gallina, M.E.; Wu, I.C.; Zhang, Y.; Chan, Y.H.; et al. Multicolor fluorescent semiconducting polymer dots with narrow emissions and high brightness. *ACS Nano* **2013**, *7*, 376–384. [\[CrossRef\]](#)
64. Creamer, A.; Fiego, A.L.; Agliano, A.; Prados-Martin, L.; Høgset, H.; Najer, A.; Richards, D.A.; Wojciechowski, J.P.; Foote, J.E.; Kim, N.; et al. Modular synthesis of semiconducting graft copolymers to achieve “clickable” fluorescent nanoparticles with long circulation and specific cancer targeting. *Adv. Mater.* **2024**, *36*, 2300413. [\[CrossRef\]](#)
65. Wu, C.; Schneider, T.; Zeigler, M.; Yu, J.; Schiro, P.G.; Burnham, D.R.; McNeill, J.D.; Chiu, D.T. Bioconjugation of ultrabright semiconducting polymer dots for specific cellular targeting. *J. Am. Chem. Soc.* **2010**, *132*, 15410–15417. [\[CrossRef\]](#)
66. Ferraro, A.; Lio, G.E.; Bruno, M.D.L.; Nocentini, S.; De Santo, M.P.; Wiersma, D.S.; Riboli, F.; Caputo, R.; Barberi, R.C. Hybrid camouflaged anticounterfeiting token in a paper substrate. *Adv. Mater. Technol.* **2023**, *8*, 2201010. [\[CrossRef\]](#)
67. Tehranipoor, M.; Pundir, N.; Vashistha, N.; Farahmandi, F. Hybrid Extrinsic Radio Frequency PUF. In *Hardware Security Primitives*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 81–95.
68. Chang, K.; Liu, Z.; Chen, H.; Sheng, L.; Zhang, S.; Chiu, D.T.; Yin, S.; Wu, C.; Qin, W. Conjugated polymer dots for ultra-stable full-color fluorescence patterning. *Small* **2014**, *10*, 4270–4275. [\[CrossRef\]](#) [\[PubMed\]](#)
69. Yao, Z.; Wang, X.; Liu, J.; Zhou, S.; Zhang, Z.; He, S.; Liu, J.; Wu, C.; Fang, X. Photoswitchable semiconducting polymer dots for pattern encoding and superresolution imaging. *Chem. Commun.* **2023**, *59*, 2469–2472. [\[CrossRef\]](#) [\[PubMed\]](#)
70. Zuo, M.; Qian, W.; Li, T.; Hu, X.Y.; Jiang, J.; Wang, L. Full-color tunable fluorescent and chemiluminescent supramolecular nanoparticles for anti-counterfeiting inks. *ACS Appl. Mater. Interfaces* **2018**, *10*, 39214–39221. [\[CrossRef\]](#) [\[PubMed\]](#)
71. Yang, C.; Liu, B.; Wang, Y.; Chen, Y.; Li, H.; Zhang, X.; Sun, G. The applications of NVM technology in hardware security. In Proceedings of the 26th edition on Great Lakes Symposium on VLSI, New York, NY, USA, 30 April 2016; pp. 311–316.
72. Wan, M.; He, Z.; Han, S.; Dai, K.; Zou, X. An invasive-attack-resistant PUF based on switched-capacitor circuit. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2015**, *62*, 2024–2034. [\[CrossRef\]](#)
73. Arcenegui, J.; Arjona, R.; Román, R.; Baturone, I. Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs. *Sensors* **2021**, *21*, 3119. [\[CrossRef\]](#)
74. Robson, N.; Safran, J.; Kothandaraman, C.; Cestero, A.; Chen, X.; Rajeevakumar, R.; Leslie, A.; Moy, D.; Kirihata, T.; Iyer, S. Electrically programmable fuse (efuse): From memory redundancy to autonomic chips. In Proceedings of the 2007 IEEE Custom Integrated Circuits Conference, San Jose, CA, USA, 16–19 September 2007; pp. 799–804.
75. Wong, C.W.; Wu, M. A study on PUF characteristics for counterfeit detection. In Proceedings of the 2015 IEEE International Conference on Image Processing (ICIP), Quebec City, QC, Canada, 27–30 September 2015; pp. 1643–1647.
76. Mamat, K.S.; Aung, P.P.; Ooi, C.Y. Systematic Review of Physically Unclonable Functions on SRAMs for Secured Authentication. *J. Electr. Electron. Res. (JEER)* **2024**, *1*, 17–26. [\[CrossRef\]](#)
77. Lin, K.H.; Wang, W.H.; Wang, I.C. The Implementation of the Physical Unclonable Function in a Field-Programmable Gate Array for Enhancing Hardware Security. *Eng. Proc.* **2025**, *92*, 23.
78. Alkanhal, M.; Alali, A.; Younis, M. A distributed lightweight PUF-based mutual authentication protocol for IoV. *IoT* **2023**, *5*, 1–19. [\[CrossRef\]](#)
79. Qureshi, M.A.; Munir, A. PUF-RAKE: A PUF-based robust and lightweight authentication and key establishment protocol. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2457–2475. [\[CrossRef\]](#)
80. Bian, J.; Huang, Z.; Lin, Y.; Yang, Z.; Liang, H.; Ni, T. Reliability analysis and comparison of ring-PUF based on probabilistic models. *Microelectron. J.* **2024**, *144*, 106072. [\[CrossRef\]](#)
81. Saadvikaa, N.; Saketi, K.J.; Gopishetti, A.; Degala, B.; Anumandla, K.K. PUF modeling attacks using deep learning and machine learning algorithms. *Eng. Proc.* **2023**, *56*, 187.
82. AL, A.M.; Mohan, N. Design and Evaluation of Hybrid Physically Unclonable Functions for Enhanced Security. In Proceedings of the 2025 IEEE 5th International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI SATA), Bangalore, India, 23–24 May 2025; pp. 1–6.
83. Cheung, H.; Choi, S.H. Implementation issues in RFID-based anti-counterfeiting systems. *Comput. Ind.* **2011**, *62*, 708–718. [\[CrossRef\]](#)
84. Xu, L.; Yang, K. Security Film and Process for Preparation Thereof. U.S. Patent 8,541,095, 24 September 2013.
85. Feldmann, J.; Spiehl, D.; Dörsam, E. Paper embossing tools: A fast fabrication workflow using image processing and stereolithography additive manufacturing. In Proceedings of the Advances in Printing and Media Technology: Proceedings of the 47th International Research Conference of Iarigai, Athens, Greece, 19–23 September 2021; pp. 19–23.
86. Muke, S.; Fox, P.; Jackson, W.; Victoria, C. Improvements in Document Security—The Next Generation. In Proceedings of the Proc. International Congress of Imaging Science, Portland, Oregon, 16–20 October 2006; pp. 424–427.
87. Kuznetsov, Y.V. *Principles of Image Printing Technology*; Springer: Berlin/Heidelberg, Germany, 2021.

88. He, W.F.; Tan, Z.H.; Chan, D.L.; Lu, Y.Z.; Qiu, J.C. Research to Factors of Screen Overprinting in Color Film Printing. *Appl. Mech. Mater.* **2012**, *200*, 739–742. [\[CrossRef\]](#)
89. Roy, S.; Rhim, J.W. Starch/agar-based functional films integrated with enoki mushroom-mediated silver nanoparticles for active packaging applications. *Food Biosci.* **2022**, *49*, 101867. [\[CrossRef\]](#)
90. Ghizdareanu, A.I.; Banu, A.; Pasarin, D.; Ionita, A.; Nicolae, C.A.; Gabor, A.R.; Pătroi, D. Enhancing the Mechanical Properties of Corn Starch Films for Sustainable Food Packaging by Optimizing Enzymatic Hydrolysis. *Polymers* **2023**, *15*, 1899. [\[CrossRef\]](#)
91. Żółek-Tryznowska, Z.; Piłczyńska, K.; Murawski, T.; Jeznach, A.; Niczyporuk, K. Study on the Printability of Starch-Based Films Using Ink-Jet Printing. *Materials* **2024**, *17*, 455. [\[CrossRef\]](#)
92. Li, Z.; Chen, Z.; Qian, J.; Ke, X.; Liu, X. Superior fluorescent ‘Color Paper-based Displayer’ for advanced anti-counterfeiting and multi-layer information encryption. *Chem. Eng. J.* **2025**, *507*, 160047. [\[CrossRef\]](#)
93. Lee, R. Micro-technology for anti-counterfeiting. *Microelectron. Eng.* **2000**, *53*, 513–516. [\[CrossRef\]](#)
94. Fujikawa, M.; Takayama, K.; Fuchi, S. Anti-counterfeiting Technique for Molded Resin Articles. In Proceedings of the 3rd International Conference on Industrial and Business Engineering, Sapporo, Japan, 17–19 August 2017; pp. 46–50.
95. Meng, Y.; Liu, F.; Umair, M.M.; Ju, B.; Zhang, S.; Tang, B. Patterned and iridescent plastics with 3D inverse opal structure for anticounterfeiting of the banknotes. *Adv. Opt. Mater.* **2018**, *6*, 1701351. [\[CrossRef\]](#)
96. Dietemann, P. Security Sheet Including an Iridescent Security Mark. U.S. Patent 10,259,247, 16 April 2019.
97. Fan, Y.; Jin, X.; Wang, M.; Gu, Y.; Zhou, J.; Zhang, J.; Wang, Z. Multimode dynamic photoluminescent anticounterfeiting and encryption based on a dynamic photoluminescent material. *Chem. Eng. J.* **2020**, *393*, 124799. [\[CrossRef\]](#)
98. Li, M.; Feng, Y.; Tian, Q.; Yao, W.; Liu, L.; Li, X.; Wang, H.; Wu, W. Tunable and ultra-stable UV light-switchable fluorescent composites for information hiding and storage. *Dalton Trans.* **2018**, *47*, 11264–11271. [\[CrossRef\]](#) [\[PubMed\]](#)
99. Sripradit, A.; Theeradejanichkul, T. A self-color-changing film with periodic nanostructure for anti-counterfeit application. *Appl. Sci.* **2022**, *12*, 6776. [\[CrossRef\]](#)
100. Zhu, C.; Tao, L.Q.; Peng, Z.; Wang, G.; Huang, Y.; Zou, S.; Sun, H.; Zhao, Y.; Chen, X.; Ren, T.L. An integrated luminescent information encryption–decryption and anticounterfeiting chip based on laser induced graphene. *Adv. Funct. Mater.* **2021**, *31*, 2103255. [\[CrossRef\]](#)
101. Lazaro, A.; Cujilema, M.R.; Villarino, R.; Lazaro, M.; Girbau, D. A novel approach for wine anti-counterfeiting using laser-induced graphene chipless RFID tags on cork. *Sci. Rep.* **2025**, *15*, 12750. [\[CrossRef\]](#)
102. Ha, B.H.; Ahn, S.; Bae, H.S.; Kang, H.S.; Kim, J.o.; Noh, J. Fast and direct engraving of iridescent lettering on original product surface using laser interference to prevent counterfeiting. *Opt. Lasers Eng.* **2018**, *107*, 214–220. [\[CrossRef\]](#)
103. Hoveida, P.; Phoulady, A.; Choi, H.; May, N.; Shahbazmohamadi, S.; Tavousi, P. Terahertz-readable laser engraved marks as a novel solution for product traceability. *Sci. Rep.* **2023**, *13*, 12474. [\[CrossRef\]](#)
104. Tomescu, R.; Parvulescu, C.; Cristea, D.; Comanescu, B.; Pelteacu, M. Low cost technology for the fabrication of anti-counterfeiting microtaggants. *J. Micromech. Microeng.* **2021**, *31*, 035008. [\[CrossRef\]](#)
105. Shariati, S.; Standaert, F.X.; Jacques, L.; Macq, B.; Salhi, M.A.; Antoine, P. Random profiles of laser marks. In Proceedings of the 31st WIC Symposium on Information Theory in the Benelux, Rotterdam, The Netherlands, 11–12 May 2010; pp. 464–478.
106. Available online: <https://www.triumphlaser.com/> (accessed on 14 August 2024).
107. Available online: <https://www.permanentmarking.com/applications/> (accessed on 14 August 2024).
108. Dusser, B.; Sagan, Z.; Bruneel, D.; Jourlin, M.; Audouard, E. Laser deep marking of metals and polymers: Potential interest for information coding. *J. Phys. Conf. Ser.* **2007**, *77*, 012002. [\[CrossRef\]](#)
109. Available online: <https://www.sure-paper.com/news/how-to-choose-self-adhesive-label-materials/> (accessed on 15 August 2024).
110. Available online: <https://gasperini.it/en/finishing-technologies/microtextured-hot-foil-dies/> (accessed on 15 August 2024).
111. Kim, H.; Kwon, G.; Park, C.; You, J.; Park, W. Anti-Counterfeiting Tags Using Flexible Substrate with Gradient Micropatterning of Silver Nanowires. *Micromachines* **2022**, *13*, 168. [\[CrossRef\]](#) [\[PubMed\]](#)
112. Terranova, S.; Costa, F.; Manara, G.; Genovesi, S. Three-dimensional chipless RFID tags: Fabrication through additive manufacturing. *Sensors* **2020**, *20*, 4740. [\[CrossRef\]](#)
113. Xiao, G.; Lu, M.; Qin, L.; Lai, X. New field of cryptography: DNA cryptography. *Chin. Sci. Bull.* **2006**, *51*, 1413–1420. [\[CrossRef\]](#)
114. Gehani, A.; LaBean, T.; Reif, J. DNA-based cryptography. In *Aspects of Molecular Computing: Essays Dedicated to Tom Head, on the Occasion of His 70th Birthday*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 167–188.
115. Clelland, C.T.; Risca, V.; Bancroft, C. Hiding messages in DNA microdots. *Nature* **1999**, *399*, 533–534. [\[CrossRef\]](#)
116. Wolfrum, C.; Josten, A. Oligonucleotides as coding molecules in an anti-counterfeiting system. *Nucleosides Nucleotides Nucleic Acids* **2005**, *24*, 1069–1074. [\[CrossRef\]](#)
117. Erlich, Y.; Zielinski, D. DNA Fountain enables a robust and efficient storage architecture. *Science* **2017**, *355*, 950–954. [\[CrossRef\]](#)
118. Gupta, K.; Singh, S. DNA based cryptographic techniques: A review. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2013**, *3*, 607–610.
119. Hashiyada, M. Development of biometric DNA ink for authentication security. *Tohoku J. Exp. Med.* **2004**, *204*, 109–117. [\[CrossRef\]](#)

120. Mead, B.K.; Hayward, J.; Liang, B.; Wan, M.; Benson, T.; Karp, J. The role of DNA-stained currency in gang robberies within the United Kingdom. *J. Forensic Sci.* **2014**, *59*, 264–267. [\[CrossRef\]](#)
121. Sharief, S.A.; Chahal, P.; Alocilja, E. Application of DNA sequences in anti-counterfeiting: Current progress and challenges. *Int. J. Pharm.* **2021**, *602*, 120580. [\[CrossRef\]](#)
122. Bloch, M.S.; Paunescu, D.; Stoessel, P.R.; Mora, C.A.; Stark, W.J.; Grass, R.N. Labeling milk along its production chain with DNA encapsulated in silica. *J. Agric. Food Chem.* **2014**, *62*, 10615–10620. [\[CrossRef\]](#)
123. Jung, L.; Hogan, M.E.; Sun, Y.; Liang, B.M.; Hayward, J.A. Rapid authentication of pharmaceuticals via DNA tagging and field detection. *PLoS ONE* **2019**, *14*, e0218314. [\[CrossRef\]](#)
124. Naef, T.; Besnard, A.L.; Lehnen, L.; Petit, E.J.; Van Schaik, J.; Puechmaille, S.J. How to quantify factors degrading DNA in the environment and predict degradation for effective sampling design. *Environ. DNA* **2023**, *5*, 403–416. [\[CrossRef\]](#)
125. Puddu, M.; Paunescu, D.; Stark, W.J.; Grass, R.N. Magnetically recoverable, thermostable, hydrophobic DNA/silica encapsulates and their application as invisible oil tags. *ACS Nano* **2014**, *8*, 2677–2685. [\[CrossRef\]](#) [\[PubMed\]](#)
126. Chien, J.; Tsai, C.; Cheng, Y.; Yang, C.R.; Wang, P.; Chang, T.L.; Lee, D.; Chang, C.; Chou, W.; Chiang, C.; et al. A RFID tag based remote DNA sensing system. In Proceedings of the 2006 1st IEEE International Conference on Nano/Micro Engineered and Molecular Systems, Zhuhai, China, 18–21 January 2006; pp. 278–282.
127. Liu, Y.; Xu, C.; Pan, Z.; Wang, G.; Liu, L. Anti-Counterfeiting Composition for Anti-Counterfeiting Chemical Fiber and Preparation Method and Use Thereof. U.S. Patent App. 17/311,427, 24 March 2022.
128. Simões, R.; Rodrigues, J.; Neto, V.; Monteiro, T.; Gonçalves, G. Carbon Dots: A Bright Future as Anticounterfeiting Encoding Agents. *Small* **2024**, *20*, 2311526. [\[CrossRef\]](#)
129. Skwierczyńska, M.; Woźny, P.; Runowski, M.; Perzanowski, M.; Kulpiński, P.; Lis, S. Bifunctional magnetic-upconverting luminescent cellulose fibers for anticounterfeiting purposes. *J. Alloys Compd.* **2020**, *829*, 154456. [\[CrossRef\]](#)
130. Li, R.; Zhang, Y.; Tan, J.; Wan, J.; Guo, J.; Wang, C. Dual-mode encoded magnetic composite microsphere based on fluorescence reporters and Raman probes as covert tag for anticounterfeiting applications. *ACS Appl. Mater. Interfaces* **2016**, *8*, 9384–9394. [\[CrossRef\]](#)
131. Bhakare, M.A.; Likhite, V.V.; Bhosale, K.L.; Lokhande, K.D.; Bondarde, M.P.; Dhumal, P.S.; Degani, M.; Some, S. Synthesis of a Dual-Functional Fluorescent Zinc-Based Metal Organic Framework for Antibacterial and Anti-Counterfeit Ink Applications. *J. Indian Chem. Soc.* **2025**, *102*, 101898. [\[CrossRef\]](#)
132. Xie, M.; Lin, G.; Ge, D.; Yang, L.; Zhang, L.; Yin, J.; Jiang, X. Pattern memory surface (PMS) with dynamic wrinkles for unclonable anticounterfeiting. *ACS Mater. Lett.* **2019**, *1*, 77–82. [\[CrossRef\]](#)
133. Ma, T.; Li, T.; Zhou, L.; Ma, X.; Yin, J.; Jiang, X. Dynamic wrinkling pattern exhibiting tunable fluorescence for anticounterfeiting applications. *Nat. Commun.* **2020**, *11*, 1811. [\[CrossRef\]](#)
134. Feng, D.; Guo, Q.; Huang, Z.; Zhou, B.; Gong, L.; Lu, S.; Yang, Y.; Yu, D.; Zheng, Z.; Chen, X. Viscoelasticity-Controlled Relaxation in Wrinkling Surface for Multistage Time-Resolved Optical Information Encryption. *Adv. Mater.* **2024**, *36*, 2314201. [\[CrossRef\]](#)
135. Chen, M.; Chen, F. Anti-Counterfeit Printing Material with a Hot Stamping Texture, Special Hot Stamping Foil and Manufacturing Method for the Same. U.S. Patent App. 13/880,979, 19 September 2013.
136. Wang, S.; Toreini, E.; Hao, F. Anti-counterfeiting for polymer banknotes based on polymer substrate fingerprinting. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2823–2835. [\[CrossRef\]](#)
137. de Almeida, M.R.; Correa, D.N.; Rocha, W.F.; Scafi, F.J.; Poppi, R.J. Discrimination between authentic and counterfeit banknotes using Raman spectroscopy and PLS-DA with uncertainty estimation. *Microchem. J.* **2013**, *109*, 170–177. [\[CrossRef\]](#)
138. Fraser, S.J.; Oughton, J.; Batten, W.A.; Clark, A.S.; Schmierer, D.M.; Gordon, K.C.; Strachan, C.J. Simultaneous qualitative and quantitative analysis of counterfeit and unregistered medicines using Raman spectroscopy. *J. Raman Spectrosc.* **2013**, *44*, 1172–1180. [\[CrossRef\]](#)
139. Gu, Y.; He, C.; Zhang, Y.; Lin, L.; Thackray, B.D.; Ye, J. Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels. *Nat. Commun.* **2020**, *11*, 516. [\[CrossRef\]](#) [\[PubMed\]](#)
140. Yu, D.; Zhu, W.; Shen, A. Raman encoding for security labels: A review. *Nanoscale Adv.* **2023**, *5*, 6365–6381. [\[CrossRef\]](#) [\[PubMed\]](#)
141. Pham, H.H.; Gourevich, I.; Oh, J.K.; Jonkman, J.E.; Kumacheva, E. A multidye nanostructured material for optical data storage and security data encryption. *Adv. Mater.* **2004**, *16*, 516–520. [\[CrossRef\]](#)
142. Liu, S.; Liu, X.; Yuan, J.; Bao, J. Multidimensional information encryption and storage: When the input is light. *Research* **2021**. [\[CrossRef\]](#)
143. Solin, S.; Ramdas, A. Raman spectrum of diamond. *Phys. Rev. B* **1970**, *1*, 1687. [\[CrossRef\]](#)
144. Bormett, R.W.; Asher, S.A.; Witowski, R.E.; Partlow, W.D.; Lizewski, R.; Pettit, F. Ultraviolet Raman spectroscopy characterizes chemical vapor deposition diamond film growth and oxidation. *J. Appl. Phys.* **1995**, *77*, 5916–5923. [\[CrossRef\]](#)
145. Holtz, J.S.; Bormett, R.W.; Chi, Z.; Cho, N.; Chen, X.; Pajcini, V.; Asher, S.A.; Spinelli, L.; Owen, P.; Arrigoni, M. Applications of a new 206.5-nm continuous-wave laser source: UV Raman determination of protein secondary structure and CVD diamond material properties. *Appl. Spectrosc.* **1996**, *50*, 1459–1468. [\[CrossRef\]](#)

146. Ferrari, A.C.; Robertson, J. Raman spectroscopy of amorphous, nanostructured, diamond-like carbon, and nanodiamond. *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **2004**, *362*, 2477–2512. [CrossRef] [PubMed]
147. Haubner, R.; Rudigier, M. Raman characterisation of diamond coatings using different laser wavelengths. *Phys. Procedia* **2013**, *46*, 71–78. [CrossRef]
148. Berenguel Centeno, A. Analysis of Background Textures in Banknotes and Identity Documents for Counterfeit Detection. Ph.D. Thesis, Universitat Autònoma de Barcelona, Departament de Ciències de la Computació, Bellaterra, Spain, 2019; ISBN 9788449091575.
149. Kumar, A.K.; Gupta, N.V.; Lalasa, P.; Sandhil, S. A review on packaging materials with anti-counterfeit, tamper-evident features for pharmaceuticals. *Int. J. Drug Dev. Res* **2013**, *5*, 26–34.
150. Harris, N.A. *Paper and Watermarks as Bibliographical Evidence*; Institut d'histoire du livre: Lyon, France, 2017; ISBN 9782956042716.
151. Available online: <https://portalsinternational.com/excellence/watermark-origination/> (accessed on 17 September 2024).
152. Zhang, P.; Zhang, W.; Yu, N. Copy detection pattern-based authentication for printed documents with multi-dimensional features. In Proceedings of the 2019 7th International Conference on Information, Communication and Networks (ICICN), Macau, China, 24–26 April 2019; pp. 150–157.
153. Khermaza, E.; Tkachenko, I.; Picard, J. Can copy detection patterns be copied? Evaluating the performance of attacks and highlighting the role of the detector. In Proceedings of the 2021 IEEE International Workshop on Information Forensics and Security (WIFS), Montpellier, France, 7–10 December 2021; pp. 1–6.
154. Tkachenko, I.; Puech, W.; Destruel, C.; Strauss, O.; Gaudin, J.M.; Guichard, C. Two-level QR code for private message sharing and document authentication. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 571–583. [CrossRef]
155. Tkachenko, I.; Puech, W.; Strauss, O.; Destruel, C.; Gaudin, J.M. Printed document authentication using two level or code. In Proceedings of the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, 20–25 March 2016; pp. 2149–2153.
156. Xie, N.; Zhang, Q.; Chen, Y.; Hu, J.; Luo, G.; Chen, C. Low-cost anti-copying 2D barcode by exploiting channel noise characteristics. *IEEE Trans. Multimed.* **2020**, *23*, 3752–3767. [CrossRef]
157. Yan, Y.; Zou, Z.; Xie, H.; Gao, Y.; Zheng, L. An IoT-based anti-counterfeiting system using visual features on QR code. *IEEE Internet Things J.* **2020**, *8*, 6789–6799. [CrossRef]
158. Benton, S.A. Rainbow holograms. *Opt. Photonics News* **1991**, *2*, 50. [CrossRef]
159. Gale, M.T. Replication technology for holograms and diffractive optical elements. *J. Imaging Sci. Technol.* **1997**, *41*, 211–220. [CrossRef]
160. Reichelt, S.; Sahm, H.; Leister, N.; Schwerdtner, A. Capabilities of diffractive optical elements for real-time holographic displays. In *Practical Holography XXII: Materials and Applications*; SPIE: Cergy-Pontoise, France, 2008; Volume 6912, pp. 185–195.
161. Lee, S.Y.; Kim, Y.H.; Cho, S.M.; Kim, G.H.; Kim, T.Y.; Ryu, H.; Kim, H.N.; Kang, H.B.; Hwang, C.Y.; Hwang, C.S. Holographic image generation with a thin-film resonance caused by chalcogenide phase-change material. *Sci. Rep.* **2017**, *7*, 41152. [CrossRef]
162. Yakovlev, A.V.; Milichko, V.A.; Vinogradov, V.V.; Vinogradov, A.V. Sol–Gel assisted inkjet hologram patterning. *Adv. Funct. Mater.* **2015**, *25*, 7375–7380. [CrossRef]
163. Gale, M. Zero-order grating microstructures. *Opt. Doc. Secur.* **1994**, 267–288.
164. Petruškevičius, R.; Baltrusaitis, J.; Kezys, D.; Mikolajūnas, M.; Grigaliūnas, V.; Viržonis, D. E-beam lithography of computer generated holograms using a fully vectorial 3D beam propagation method. *Microelectron. Eng.* **2010**, *87*, 2332–2337. [CrossRef]
165. Moser, J. Document protection by optically variable graphics (Kinegram). In *Optical Document Security—Whitepaper*; van Renesse, R.L., Ed.; 1998; pp. 169–185.
166. Staub, R.; Tompkin, W.R.; Moser, J.F. Combination gratings. In *Diffractive and Holographic Optics Technology III*; SPIE: Cergy-Pontoise, France, 1996; Volume 2689, pp. 292–299.
167. Tompkin, W.R.; Staub, R. Low-density diffractive optical memories for document security. *Opt. Eng.* **1996**, *35*, 2513–2518. [CrossRef]
168. Markov, V.; Millerd, J.; Trolinger, J.; Norrie, M.; Downie, J.; Timucin, D. Multilayer volume holographic optical memory. *Opt. Lett.* **1999**, *24*, 265–267. [CrossRef] [PubMed]
169. Shamir, J.; Wagner, K. Generalized Bragg selectivity in volume holography. *Appl. Opt.* **2002**, *41*, 6773–6785. [CrossRef]
170. Widmer, R.W. Method for Producing Aluminum Holographic Masters. U.S. Patent 3,875,026, 1 April 1975.
171. Available online: <https://internationalbarcodes.com/> (accessed on 5 October 2024).
172. Available online: <https://www.labels-sp.com/upc-barcode-need-know/> (accessed on 5 October 2024).
173. Erhan, S.; Bagby, M. Lithographic and letterpress ink vehicles from vegetable oils. *J. Am. Oil Chem. Soc.* **1991**, *68*, 635–638. [CrossRef]
174. Erhan, S.Z.; Bagby, M.O. Vegetable-oil-based printing ink formulation and degradation. *Ind. Crops Prod.* **1995**, *3*, 237–246. [CrossRef]

175. Chen, Q.; Li, X.; Chen, G. Vegetable oils based UV-luminescent ink for screen printed anti-counterfeiting marking. *Prog. Org. Coatings* **2021**, *151*, 106009. [CrossRef]
176. Andres, J.; Hersch, R.D.; Moser, J.E.; Chauvin, A.S. A new anti-counterfeiting feature relying on invisible luminescent full color images printed with lanthanide-based inks. *Adv. Funct. Mater.* **2014**, *24*, 5029–5036. [CrossRef]
177. He, Z.; Wang, W.; Fan, J.; Bao, B.; Qin, X.; Yu, D. Photochromic microcapsules anchored on cotton fabric by layer-by-layer self-assembly method with erasable property. *React. Funct. Polym.* **2020**, *157*, 104762. [CrossRef]
178. Seipel, S.; Yu, J.; Viková, M.; Vik, M.; Koldinská, M.; Havelka, A.; Nierstras, V.A. Color performance, durability and handle of inkjet-printed and UV-cured photochromic textiles for multi-colored applications. *Fibers Polym.* **2019**, *20*, 1424–1435. [CrossRef]
179. Available online: <https://metamaterial.com/banknote/products/lumachrome-anti-counterfeit-solution/> (accessed on 8 October 2024).
180. Available online: <https://www.iso.org/standard/55881.html> (accessed on 8 October 2024).
181. Liu, H.; Yan, L.; Huang, J.; An, Z.; Sheng, W.; Zhou, B. Ultrasensitive thermochromic upconversion in core-shell-shell nanoparticles for nanothermometry and anticounterfeiting. *J. Phys. Chem. Lett.* **2022**, *13*, 2306–2312. [CrossRef] [PubMed]
182. Lin, J.; Wang, P.; Wang, H.; Shi, Y.; Zhu, K.; Yan, F.; Li, G.; Ye, H.; Zhai, J.; Wu, X. Significantly photo-thermochromic KNN-based “smart window” for sustainable optical data storage and anti-counterfeiting. *Adv. Opt. Mater.* **2021**, *9*, 2100580. [CrossRef]
183. Li, H.; Zhu, M.; Tian, F.; Hua, W.; Guo, J.; Wang, C. Polychrome photonic crystal stickers with thermochromic switchable colors for anti-counterfeiting and information encryption. *Chem. Eng. J.* **2021**, *426*, 130683. [CrossRef]
184. Ma, Y.; Dong, Y.; Liu, S.; She, P.; Lu, J.; Liu, S.; Huang, W.; Zhao, Q. Chameleon-like thermochromic luminescent materials with controllable response behaviors for multilevel security printing. *Adv. Opt. Mater.* **2020**, *8*, 1901687. [CrossRef]
185. Guirado-Moreno, J.C.; Guembe-García, M.; García, J.M.; Aguado, R.; Valente, A.J.; Vallejos, S. Chromogenic Anticounterfeit and Security Papers: An Easy and Effective Approach. *ACS Appl. Mater. Interfaces* **2021**, *13*, 60454–60461. [CrossRef]
186. Qiao, J.; Fu, R.; Zhang, Y.; Zhao, X.; Feng, Y. Erasable invisible ink based on a TPE-based AIE pigment. *Authorea Prepr.* **2023**. [CrossRef]
187. Muthamma, K.; Nair, K.; Sunil, D.; Kulkarni, S.D.; Anand, P.; Ali, T.; Kekuda, D. Water-based combifuge ink with unique tamper-evident features for anti-counterfeiting applications. *J. Mol. Liq.* **2022**, *361*, 119695. [CrossRef]
188. Degott, P. Optically Variable Inks (OVI): Versatility in formulation and usage. In *Optical Security and Counterfeit Deterrence Techniques III*; SPIE: Cergy-Pontoise, France, 2000; Volume 3973, pp. 317–321.
189. Phillips, R.W. Optically variable films, pigments, and inks. In *Optical Thin Films III: New Developments*; SPIE: Cergy-Pontoise, France, 1990; Volume 1323, pp. 98–109.
190. Xiaohe, C.; Liuping, F.; Peng, C.; Jianhua, H.; Jianle, Z. Research on anti-counterfeiting technology of print image based on the metamer properties. In Proceedings of the 2017 2nd International Conference on Communication and Information Systems, Wuhan, China, 7–9 November 2017; pp. 284–289.
191. Available online: <https://www.fortunebusinessinsights.com/anti-counterfeiting-packaging-market-102692/> (accessed on 10 September 2025).
192. Li, J.; Crown, A.; Ney, P.; Yekhanin, S.; Partap, A.; Shirole, A.; Jiang, H.; Russ, S.; Gordon, M.; Aroh, A.; et al. Hybridization-encoded DNA tags with paper-based readout for anti-forgery raw material tracking. *Nat. Commun.* **2025**, *16*, 5832. [CrossRef]
193. Available online: <https://nfc-forum.org/news/2024-08-combatting-counterfeiting-how-nfc-technology-is-providing-protection-to-key-industries/> (accessed on 8 September 2025).
194. Lu, W.; Jiang, Y.; Chen, Z.; Ji, X. Blockchain adoption in a supply chain system to combat counterfeiting. *Comput. Ind. Eng.* **2022**, *171*, 108408. [CrossRef]
195. Available online: <https://www.nist.gov/publications/counterfeit-ic-detection-using-rf-excited-signals-and-ai-assisted-classification/> (accessed on 10 September 2025).
196. Available online: <https://logisticsviewpoints.com/2025/07/15/blockchain-for-transparent-and-secure-supply-chains-2025-update/> (accessed on 10 September 2025).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.