ANTI-COUNTERFEIT TECHNOLOGIES (A PHARMACEUTICAL INDUSTRY PERSPECTIVE)

Dr. Zufi Shad[1], Dr. Hadia Naz[2], Syeda Rida Abbas[3], Sara Ishaque Shaikh[4], Aleeza Rashid[5]

[1]Faculty of Pharmacy
Hamdard University
Zufi.shad@hamdard.edu.pk

[2]Faculty of Pharmacy
Hamdard University
Hadia.Naz@hamdard.edu.pk

[3]Faculty of Pharmacy
Hamdard University
ridaabbas25@yahoo.com

[4]Faculty of Pharmacy
Hamdard University
sishaque01@gmail.com

[5]Faculty of Pharmacy
Hamdard University
aleezarashid29864@gmail.com

Abstract:

This research, primarily based on a comprehensive review of existing literature, provides a thorough examination of Counterfeiting and Anti-counterfeit technologies from the perspective of the pharmaceutical industry. The study encompasses various critical aspects, including an introduction to the global standard definition of counterfeiting, a historical overview of pharmaceutical counterfeiting on a global scale, an exploration of contributing factors, an assessment of current and future risks, and the presentation of potential solutions and suggestions. The research dives deep into the realm of anti-counterfeit technologies, shedding light on their essential characteristics, functionalities, classifications, and the global adoption trends across several countries, including the United States, Canada, France, Nigeria, Malaysia, India, China, and Pakistan. A comprehensive analysis of these technologies, categorized based on overt features, covert features, forensic markers, serialization/track and trace mechanisms, chemical attributes, physical attributes, mechanical features, and other relevant factors, offers valuable insights into their multifaceted nature. Additionally, the study covers recent innovations in the field of anti-counterfeit technologies, showcasing the dynamic nature of this evolving landscape. In conclusion, the research synthesizes key recommendations from both manufacturers and consumers, highlighting effective strategies for implementing anti-counterfeit techniques and collectively working towards discouraging and ultimately eradicating the pervasive practice of counterfeiting within the pharmaceutical industry. By addressing these critical aspects, this research aims to contribute to the ongoing efforts to enhance the security and authenticity of pharmaceutical products, ultimately safeguarding public health and consumer trust.

INTRODUCTION

COUNTERFEITING

Definition by World Health Organization (WHO)

A counterfeit medicine is one which is deliberately and fraudulently **mislabeled** with respect to ***identity*** and/ or ***source***.

Counterfeiting of medicines can apply to both *branded* and *generic* products. Generally, counterfeit products may include products with *correct* or with *wrong* ingredients, *without* active ingredients, with *in correct* quantities of activities or with *fake* packaging.

We are not concerned here with *patent infringements* or *legal generic versions* of patented medicines: local laws dictate this, consistent within international rules.

PHARMACEUTICAL COUNTERFEITING

HISTORY OF COUNTERFEIT DRUGS

The ***International Institute of Research Against Counterfeit Medicines*** (**IRACM**), reported the history of counterfeiting as:

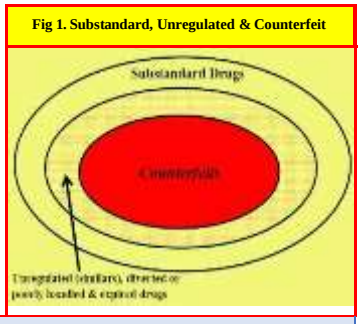


Fig 1. Substandard, Unregulated & Counterfeit

2nd century BC	First proven case of counterfeiting: a Gallic winemaker attempts to pass off his wine for outstanding vintage
40 AD	Dioscorides, a Greek physician and botanist, gives advice to distinguish between genuine and counterfeit medicines
15th century	The apothecary in Paris becomes a profession in itself.
17th century	Apothecaries are implicated in cases of adulterated medicines.
1985	The Nairobi conference in 1985 first brings the problem of counterfeit drugs to the international stage.
1985	An international meeting in Geneva leads to the first official definition of a counterfeit medicine.
2006	WHO organizes Rome Conference that leads to creation of the IMPACT group. Medicine counterfeiting is recognized as a serious and vile criminal offense.
2009	In Benin (October 2009), Jacques Chirac appeals to the international community to take action against counterfeit medicine trafficking. 50 heads of States sign.

May 2010	63rd WHO meeting establishes a working group focused on substandard/ spurious/ falsely-labelled/falsified/ counterfeit (SSFFC) medical products.
November 2010	92nd session of Council of Ministers of the African, Caribbean & Pacific group. Resolution adopted on fight against production & marketing of fake drugs.
November 2010	Interpol adopts resolution AG-2010-RES-06 for improved international cooperation & calls on Member States to prioritize fight against counterfeiting.
December 2010 to April 2011	20th session of U.N. Commission on Crime Prevention & Criminal Justice. UN adopts resolution 20/6 defining its role (UNODC), in fight against fraud drugs.
December 2010	Council of Europe adopts the Medicrime convention, the first international legal instrument to effectively fight against pharmaceutical crime.
June 8, 2011	Directive 2011/62/EU validated by the European Parliament. The Directive strengthens instruments to combat counterfeiting by securing pharmaceutical distribution channels, & foresees creation of a logo to identify legal pharmacy websites, a product traceability system and stricter repression for offenders.
2014	Pangea VII involved 111 countries, shuts down 10,600 websites, seizes 20,000 packages and results in 239 arrests.

PREVALENCE

- Medicine counterfeiting is much more of a threat to public health than to company revenues.
- Counterfeit and substandard medicines are common worldwide with more prevalence in developing countries.
- The actual prevalence could be difficult to estimate due to many factors, however, literature have reported that the prevalence of counterfeit medicines ranged from **10%** of the ***global market***, and from **25%** in ***developing countries*** and reaching up to **60%**.

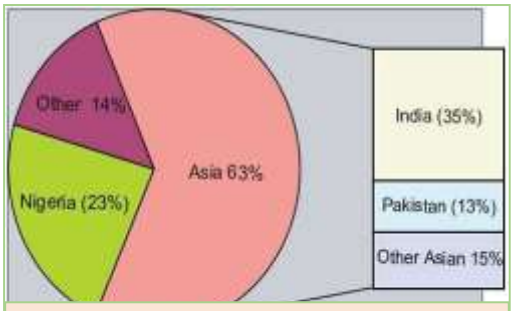


Fig 2. ORIGIN OF COUNTERFEIT DRUGS.
Source: Survey by the WHO. Counterfeit Drugs: Report on returned questionnaires from countries, 1997.

Fig 3. Worldwide incidents of counterfeit medicines, 2002–2009

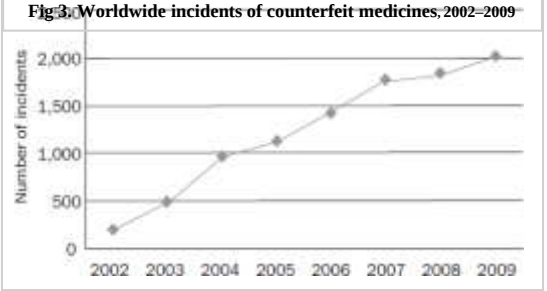


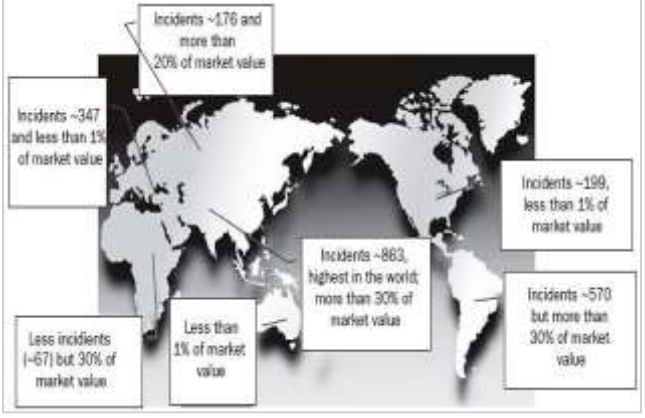
Table 1. INCIDENTS OF COUNTERFEITING, DIVERSION & THEFT (2003–2005)

Year	Counterfeit	Diversion	Theft	Total
2003	370	78	30	478
2004	444	144	55	643
2005* (9months)	243*	70*	35*	348*

Table 2. MAIN TYPES OF COUNTERFEITED DRUGS (January 1999–December 2002)

Category of drugs	%age of total counterfeits
Antibiotics	28
Hormones and steroids	18
Anti-asthma and anti-allergy	8
Anti-malarial	7
Analgesics and anti-pyretics	6
Others (14 therapeutic classes)	33

Fig 4. Global Market value of counterfeiting incidents, 2009



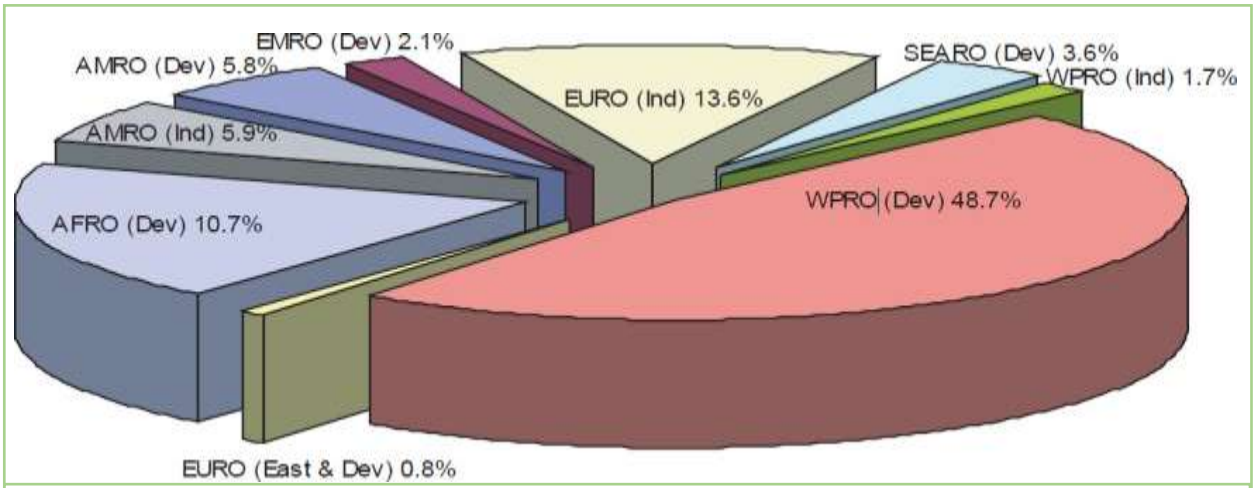


Fig 5. GEOGRAPHICAL ORIGINS OF CASES (1982 – 1999). ***Total number of cases: 771.***
AFRO: Regional office for Africa; **AMRO**: Regional office for the Americas; **Dev**: Developing; **EMRO**: Regional office for the Eastern Mediterranean; **EURO**: Regional office for Europe; **Ind**: Industrialized; **SEARO**: Regional office for South-East Asia; **WPRO**: Regional office for the Western Pacific.
Source: Summary of Counterfeit Drug Database as of April 1999, unpublished paper of WHO Division of Drug Management and Policies.

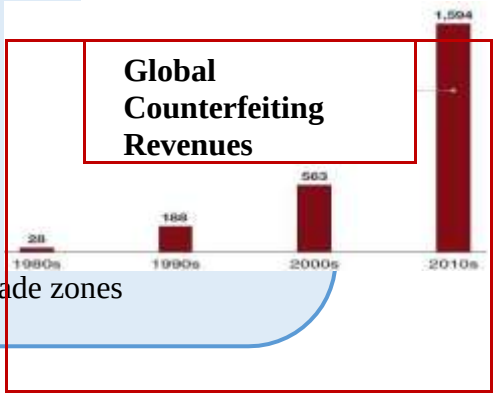
Table 3. EXAMPLES OF COUNTERFEITED DRUGS

Country and year	*Counterfeiting problem*
Nigeria, 1990	Cough mixture was diluted with a poisonous solvent leading to the deaths of 100 children.
Mexico, 1991	Anti-burn ointment contained sawdust.
Turkey, 1993	A pharmacist is arrested after the active ingredient in 'drugs' exported to Africa was found to be baking powder.
Niger, 1995	A meningitis drug contained only water.
Haiti, 1996	59 children die after taking a counterfeit syrup for fever.
Kenya, 1998	Anti-malarial drugs were found to be ineffective.
India, 1998	Diethylene glycol poisoning killed at least 30 children.
Brazil, 1998	Ineffective contraceptive pills resulted in unwanted pregnancies.
Malawi, 1999	Africa Health journal reports an influx of counterfeit drugs into country.
Italy, 2000	240 000 packs of medicines and 2 t of raw materials seized.
China 2001	The Shenzhen Evening News reports that more than 100 000 people died of fake drugs in 2001.
USA, 2001	Counterfeit Serostim, Neupogen and Nutropin AQ discovered.
India, 2001	Police found 660 kg of fake drugs, 1000 kg of raw materials and boxes bearing the logo of a reputable firm. All of these were discovered in one factory.
Nigeria, 2002	The head of the country's drug control agency reported that 60% of the drugs are counterfeit, substandard or expired.
USA, 2002	The FDA reported 3 lots of counterfeit Combivir.
China, 2002	Counterfeit drugs valued at USD 57 million were identified.
USA, 2003	Recall of 200 000 bottles of the anti-cholesterol drug, Lipitor

FACTORS AFFECTING DRUG COUNTERFEITING

With increasing free trade agreements and deregulation worldwide, as well as the proliferation of the Internet, there are now very few areas unaffected by counterfeiting. The WHO has found ten major factors promulgating the existence of counterfeiting, including:

1. Lack of legislation
2. Weak or absent drug regulatory authority
3. Absence of a legal mandate for licensing of manufacture/ import of drugs
4. Lack of enforcement of existing regulations
5. Transactions involving many intermediaries
6. Demand exceeding supply
7. High prices
8. Sophistication of clandestine drug manufacture
9. Inefficient cooperation between stakeholders
10. Lack of regulation by exporters and within free trade zones



Current & Future Risks

The current & expected risks include:

- Treatment failure in malaria, TB and HIV/AIDS & spread of drug resistant pandemics.
- Growth of resistance to existing anti-infectives from use of sub-par treatments
- Use of illegal funds to finance further illegal manufacture of medicines and even terrorism
- Globalization of pharmaceutical production know-how drives counterfeiting
- Counterfeit drugs are increasingly showing up in OECD countries

POSSIBLE SOLUTIONS & SUGGESTIONS

Recommendations & specific measures listed by WHO report to combat counterfeiting & create a national strategy include:

Strengthening political will

Corruption and *vested interests* in top positions often disrupt effective enforcement of legislation.

Promulgating appropriate legislation

Legislation should be reviewed & amended. Making licensing mandatory, *quality control* and testing of *imported* drugs should also be undertaken.

National drug regulatory authority

A national drug regulatory authority with effective *independent powers* should be established.

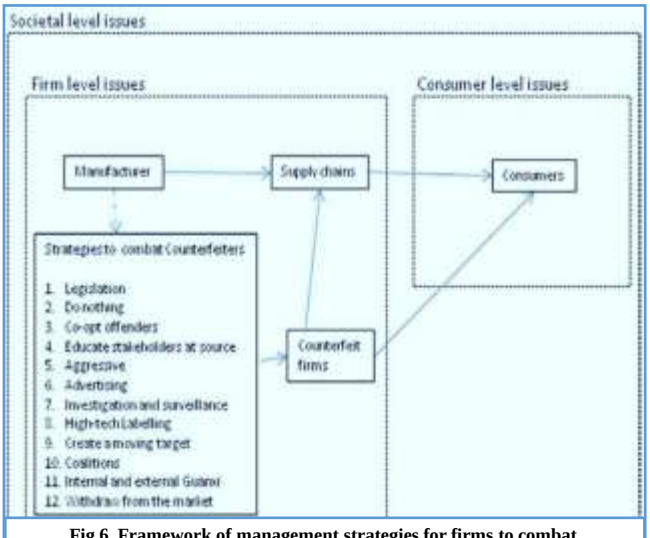


Fig 6. Framework of management strategies for firms to combat counterfeit firms

Fostering partnerships

Pharmaceutical companies should be more open about drugs being counterfeited, Consumers must also be educated about the scope and dangers of counterfeiting. Steps that should be taken at the international level include:

- ✓ Creation of an ***international database*** of all known sources of counterfeits.
- ✓ Pharmaceutical companies need to open the ***lines of communication*** and divulge all counterfeiting information to *agencies* such as INTERPOL, or to *national police force.*

Table 4. CONSIDERATIONS FOR DECIDING ON "FIGHT" OR "COOPERATE" STRATEGY

	Passive imitators and counterfeiters	**Potential collaborators with "copyand develop" capabilities**
Objective of counterfeiter	Quick profit from low qualityimitated goods	Interest in building own NPDcapabilities (by whatever means)
Nature of counterfeit products	Low quality	Aspiring to similar quality as original
Counterfeiter's strategy	Short-term gain, no repeatinteraction with customers	Building a brand identity. Gainingrepeat transactions with customers
Effects of counterfeiting on original manufacturer	Mainly damage to reputation	Loss of revenue in the short-term, potential competitor long-term
Attractiveness to consumers	Sometimes fooled, but often knowingly buying inferior product	As long as quality is satisfactory or equivalent to original, trademark infringement or nonpayment of royalties does not concern consumers
Strategic options for original manufacturer	If damage to reputation is serious, the defend and prevent strategy should be chosen	If threat of becoming a competitor is serious, then a collaborate and build strategy should be chosen

ANTICOUNTERFEIT TECHNOLOGIES

Characteristics of an Ideal Anti-counterfeit Technology

- An ideal anti-counterfeit technology should possess a *high level* of **security** (non-clonable), *higher* **product application** and **authentication speed**, *proven* **standards**, be *difficult to* **remove** and **reapply**, easy to **check**, have **automatic authentication**, be **useable** by consumers, and must be **legally compliant** by the *industries*. FDA recommends use of *multiple,periodically* changing, authentication measures on a product-specific basis.
- Majority of these technologies can be implemented on one or more of the ***packaging*** components, but some features can even be applied at the ***product***.

Functions of Anti-counterfeit Techniques

- The purpose of an anti-counterfeit feature is primarily to
  - ✓ Enable **authentication**, either by industry investigators, or ideally, by the wider public.
  - ✓ Second function may be to **deter** anyone considering counterfeiting on the *difficulty* or *cost* involved set against likelihood of *detection*, and therefore *prosecution*.

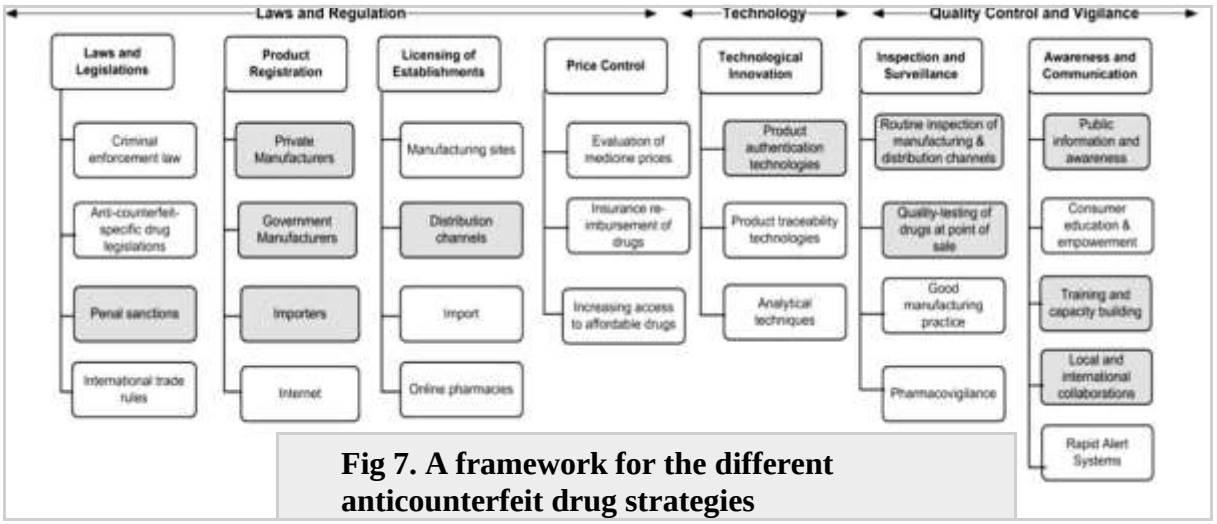


Fig 7. A framework for the different anticounterfeit drug strategies

Classification of Anti-counterfeit technologies

Anti-counterfeit technologies can be *broadly* classified as follows:

- **Overt**, or **Visible** features
- **Covert**, or **Hidden** markers
- **Forensic** techniques
- **Serialization**/**Track** and **Trace**

Table 5. COMPARISON OF AUTHENTICATION CHARACTERISTICS				
	Overt Features	***Covert Features***	***Forensic Markers***	***Serialization / Track & Trace***
Advantages	User verifiable, more secure, decorative appeal, low cost	Easily added or modified, need regulatory approval, applied in-house or via component suppliers, low cost	High-tech and secure against copying, provide positive authentication, may be disclosed for overt purposes	High tech and secure against copying, capable of remote authentication, accessible to authorities and investigators, eliminate dispensing errors, allows recall of defective product
Disadvantages	Require use reducation, easily mimicked, rely on covert features, may be re-used or refilled, provide false assurance	Need strict secrecy, risk of compromise, more secure options add supply complexity and cost	Licensed technologies, significant cost, difficult to implement and control across many markets, unlikely to be available to authorities or public	Significant cost, difficult toimplement, vulnerable to hackers, robustness RFID tags not proven, privacy issues, not accessible to public, damaged labels cannot be read

Global Implementation of Anti-counterfeit Technologies

- The implementation of anti-counterfeit technologies is an important strategy taken up by drug manufacturers and regulatory authorities in several countriesto protect the supply chain & address the problem of drug counterfeiting.
- Efficient and reliable processing of information as well as dissemination of alerts is warranted to the damage caused by the administration of any faulty medicines.
- Implementing **2D** and **data matrix barcoding** has come up as a unified global strategy. Countries have placed this ***global intervention program*** within their respective health

system at varying pace.

- *Phase wise realization* is seen, with first step being verifying the ***serialization*** and ***data banking*** at a local repository (fixed data), proceeding to the second level of enabling data access using a ***cloud-based repository*** accessible by multiple users to receive, share, and update information. Equipping pharmacies with the respective soft and hardware devices is also a major part of this process. The final stage of "Track and Trace" process enables a ***proactive bidirectional system*** of sending *alerts* and *product warnings* that could be linked to ***electronic prescribing portals*** to ensure maximum patient safety.

- However, **costs** and **lack of awareness** about the barcoding system had been the major impeding factors in its implementation process.

U.S.A.

- According to the **Healthcare Distribution Management Association** (***HDMA***) as of July, 2008, 29 states in the US had implemented pedigree requirements and six other states had pending legislation. Federal law requires all dealers except manufacturers and ADRs to pass pedigree requirements, but state requirements show several variations.
- A limited number of transactions are allowed without the pedigree requirement, as in Nevada: pedigrees must be passed when a drug leaves a normal distribution chain (as is the case in Arizona, Maryland, and North Dakota), and in Florida where all wholesale distributors including authorized distributor of records (ADR) must comply with the law.

Canada

- The **Automated Identification of Vaccine Projects** (***AIVP***) Advisory Task Group of Canada as documented in the Canadian Consensus Statement released in late 2009, stated the following recommendations for all vaccines in Canada: **2D bar codes** on ***primary*** package and **2D** or **linear barcodes** on ***secondary*** package, both include *GTIN* and *lot no*.

France

- According to a French Official Journal dated March 16, 2007, French Health Products Safety Agency notified distributors mandating by 31st of December in 2010: a 13-character (**Club Inter Pharmaceutique**) ***CIP*** 13 code with batch number and expiration date and **Simplex linear barcode** to be replaced by the **2D Data Matrix marking**.

Nigeria

- The Mobile Authentication Service is a **National Agency for the Food, Drug Administration, and Control** (***NAFDAC***) program in Nigeria supported by BIOFEM pharmaceuticals where **Sproxil** technology enables any consumer to check the authenticity of medication with a simple text message. *GSK* with *NAFDAC* collaboration uses this service for the authentication of the antibiotic ampiclox (tradename).

Malaysia

- The "**Meditag**" holographic authentication sticker was introduced in 2005 by the Malaysian Ministry of Health to confirm the authenticity of medicines registered.

India

- According to the public notice issued by the Directorate General of Foreign Trade dated January 10th, 2011, exported pharmaceutical products should have **track and trace capability** using ***barcode technology*** as per GS1 global standards.
- The stated requirements are: **2D barcode** at the ***primary*** level, **1D** or **2D** on the ***secondary*** level, and **1D** at the ***tertiary*** level packaging encoding the *GTIN code*, *batch number*, *expiration date*, and *serial number* of respective packaging.
- However, this system does not ensure absence of counterfeits as effectively as serialization. Barcodes increase the risk of being caught if counterfeits are present, whereas serialization uniquely identifies every entity and ensures the absence of counterfeits. Serialization using barcodes as data carriers is a more secure strategy and is even more economical compared to the RFID system.

China

- India and China are the two main global suppliers of raw materials and finished pharmaceuticals, and their compliance with the implementation of GS1 standards using barcoding holds crucial importance in the success of an end-to-end "Track and Trace" process. The **Indian Drug Authentication and Verification Application** (***DAVA***) introduced in 2012 was an award-winning project (GS1 India, 2017). Contrary to that, China has not yet adopted the global concept of serialization and a separate China National Drug Code with serial numbers is issued through its own **Product Identification, Authentication and Tracking System** (***PIATS***)

Pakistan

- Pakistan has postponed the implementation process to several deadlines. The 2011 "Fake Drug Crisis" acted as a driving force to reform the regulatory structures of the country and for establishing the autonomous "Drug Regulatory Authority of Pakistan". Despite Pakistan possessing a huge pharmaceutical industry, it is yet to achieve the first milestone of elevating a **Global Trade Identification Number** (***GTIN***) and serialization to the level of primary packaging by all manufacturers.

Table 6. Mass serialization and track-and-trace around the world

Country	Deadline for implementation	Type of protection
Argentina	Inplace	Track-and-trace
Brazil	Inplace	Track-and-trace
China	December 2015	Serialization
E.U. & Switzerland	Enforcement begins in 2019	Serialization
India	Inplace	Serialization
Russia	2019	Track-and-trace
Saudi Arabia	Expected in 2017	Serialization
South Korea	Inplace	Serialization
Turkey	Inplace	Track-and-trace
U.S.	Serialization by 2019, full Track-and-trace by 2025	Track-and-trace

OVERVIEW OF ANTICOUNTERFEIT TECHNOLOGIES
W.R.T. THEIR CLASSIFICATION

OVERT (VISIBLE) FEATURES

End users are supposed to be able to check the **legitimacy** of a pack using overt features. Such characteristics are typically very ***noticeable*** and ***expensive*** or ***difficult to duplicate***. Overt features may result in *major cost increases*, *supply availability restrictions*, and *end user education requirements*.

To prevent unauthorized diversion, they also demand the ***highest level of security*** during supply, handling, and disposal procedures. In order to prevent real used components from being recycled with phoney contents and creating a false sense of authenticity, they should be applied in such a way that they cannot be **reused** or **removed** without ***defacing*** or ***harming*** the pack. For increased security, an overt *device* may be included within a ***Tamper Evident feature***.

1. HOLOGRAMS

- The "**dove**" hologram, which has long been used to protect credit cards, is perhaps the characteristic that people are most familiar with.
- A hologram typically includes an image that gives the impression of being ***three-dimensionally*** constructed, or that has a distinct ***depth*** to it.
- When incorporated into a tamper-evident feature or made a vital component of the primary pack, holograms and other **optically variable devices** (***OVD***) can be made more effective (e.g., blister foil).

- They can be woven into the *tear bands* of the ***overwrap films*** or inserted as *threads* into the ***paper substrates***.
- However, certain hologram labels have been skillfully and readily imitated, and they frequently rely on secret, covert components for authentication.

TYPES

- ***TRADITIONAL HOLOGRAMS*** can be printed directly on a product or its packaging or incorporated into sticky labels.

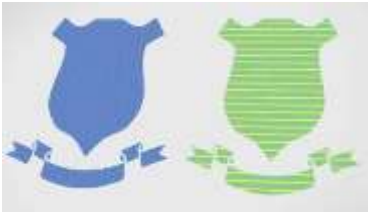
  Examples include ***multi-layer*** 2D to 3D holograms, 3D holograms, dot-matrix, hot stamping foil (HSF), and holograms produced using the demetallization process.

- ***COMPLEX HOLOGRAMS*** resemble standard holograms visually, but they also include a range of secret information in the form of "cryptograms." The level of security that is provided by this mix of visible and invisible security elements is increased.

- ***NANOOPTIC HOLOGRAM*** include security characteristics at the **nanoscale**. It combines two levels of verification on the bottle label, "**phygital**" (physical + digital).

2. OPTICALLY VARIABLE DEVICES (OVD)

- OVDs also comprise a variety of **substitute technologies**, many of which resemble *holograms* but frequently lack any *3D elements*.
- They typically involve **picture flips** or **transitions**, which frequently include ***color changes*** or ***monochromatic contrasts***.
- Similar to holograms, they typically consist of an image-carrying transparent film and a reflective backing layer, which is typically a very thin layer of aluminum.
- For specialized security purposes, other metals, like copper, may be utilized to impart a distinctive tint.
- Partial de-metallization, involves chemically removing a portion of the reflective layer to give the picture a detailed contour as seen on many banknotes, may add further security.
- A clear film with more of a ghost reflected image is produced when the reflective layer is so thin it is transparent, depending on the viewing angle and lighting.
- Because partial removal of metallic layer is a more complicated procedure, it raises both the cost and the level of protection.

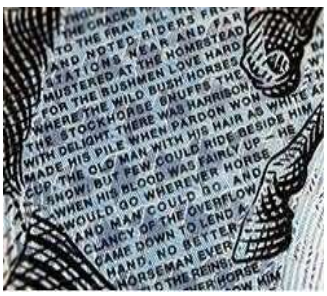


3. COLOUR SHIFTING SECURITY INKS AND FILMS

- These can function as an obvious graphic element or by being included into a security seal, showing positive color variations depending on the viewing angle.
- Color shifting pigments are finely powdered metallic laminates that require a thick opaque layer to be laid down in order to generate the optical effect; as a result, gravure and screen printing rather than lithography are better suited to use color shifting pigments.
- The distinctiveness and dynamics of the color shift (from blue to gold, for example), along with the difficulty and expense of manufacturing, give these objects their security value.
- They are only accessible through a few specialized ink makers and a small number of pigment suppliers.
- Embedded taggants and forensic (microscopic) analysis may be required for successful authentication.
- Security applications have made use of color-shifting films, which are constructed by layering thin films to create a material with distinct diffractive characteristics and striking color shifts.
- They can be used as tamper-evident labels or security seals.

4. SECURITY GRAPHICS

- Similar to ***banknote printing***, **fine line color printing** uses both <u>overt</u> and <u>covert</u> design features including *guilloches*, *line modulation*, and *line emboss*.
- They can be produced using standard offset **lithography** or, for improved security, **intaglio** printing.
- They can be used as backdrop in a specific zone, such as an overprint region, or as whole pack graphics.
- The design is made more difficult to scan and duplicate by the subtle use of pastel "spot" colors, and security is further



increased by the use of a variety of hidden design components, such as micro-text and latent pictures.

5. SEQUENTIAL PRODUCT NUMBERING

- Counterfeit goods may be easier to spot in the supply chain if each pack or label in a batch is given a unique sequential number.
- Because duplicates or incorrect numbers will be rejected, it offers a semi-overt method of authentication by reference to a secure database if printed in plain sight.
- Sequential numbering has several drawbacks, but its main drawbacks are that end users need a way to access the database and that the sequence is predictable and simple to copy.
- Serialization using a pseudo-random, non-repeating sequence is the safer method.

6. ON-PRODUCT MARKING

- Conventional oral dosage forms can now be marked with unique graphics or codes thanks to on-product marking technologies.
- These obvious technologies can be challenging to imitate and provide security down to the pill level.
- Even when things are taken out of their original packaging, this extra security measure is still effective.

COVERT (HIDDEN) FEATURES

A covert feature's function is to help the brand owner spot counterfeit goods. The ordinary populace won't be aware of it or have the tools to confirm it. Without specialized knowledge, a hidden feature shouldn't be simple to find or reproduce, and its specifics must be kept under "need to know" restrictions. Most covert features will lose some, if not all, of their security value if they are exposed or hacked.

1. INVISIBLE PRINTING

On nearly any substrate, invisible markings that only become apparent under specific lighting circumstances, including UV or IR irradiation, can be printed using specialized inks. They can be designed to exhibit various colors when illuminated at various wavelengths.

2. EMBEDDED IMAGE

A hidden image that can only be seen with a particular filter and cannot be replicated by standard scanning techniques can be incorporated into the pack graphics. The results can be fairly spectacular while remaining discreet.

3. DIGITAL WATERMARKS

Graphics elements can digitally encode invisible data that can be read by a reader and confirmed with specialized software. The data can be recorded using a webcam, phone, or other scanning apparatus, but the digital information cannot be seen by the human eye. Attempts to duplicate the data will be discovered since the embedded data will degrade.

4. HIDDEN MARKS AND PRINTING

It is possible to apply special marks and print in a way that deters attention and makes it difficult to replicate. Since their effectiveness depends on a blend of secrecy and nuance, we won't go into additional detail here.

5. ANTI-COPY OR ANTI-SCAN DESIGN

Background patterns with fine lines first look as uniform tones, but when scanned or duplicated, they reveal an unnoticed latent image. They can be used as a background tint on product packaging and are frequently used on secure documents to avoid photocopying.

6. LASER CODING

It takes specialized, expensive equipment to apply batch variable information by laser coding, and the results are recognizable artefacts that may be challenging to recreate. Carton and label surfaces, as well as plastic and metal parts, can all use laser codes.

7. SUBSTRATES

There are numerous different techniques to incorporate covert markers into a substrate, such as chemical reagents in carton board or paper, visible or UV fluorescing fibers, or both. Watermarks can be weaved into leaflet paper or incorporated in metallic threads, possibly with an obvious OVD feature. These call for a specialized supply source and high production volumes, which, if feasible, produce a very efficient choice.

FORENSIC MARKERS

1. CHEMICAL TAGGANTS & TRACERS

- Chemical traces that are ordinarily undetectable by standard examination but can only be discovered by highly specific reagent systems. These particles are invisible to the naked eye and can be affixed to any kind of surface.
- However, specialized technology can be used to identify the particles' distinct characteristics, such as a color reaction to light.

2. BIOLOGICAL TAGGANTS

A biological identifier can be applied to packing components or integrated at extremely low quantities (parts per million or less) in product formulations or coatings. In order to validate them at such low concentrations, extremely specialized "lock and key" reagent kits are required.

3. DNA TAGGANTS

Numerous printing techniques can be used to apply highly precise DNA "lock and key" reagent systems to packaging. They need a "mirror image" recombinant strand to complete the pairing, and a special equipment can identify this response. The marker and reagent pair is concealed in a matrix of random DNA strands to further increase security, but the test is designed to only function with one recombinant pair.

4. ISOTOPE RATIOS

By using laser fluorescence or magnetic resonance techniques, naturally occurring isotopes can be used to precisely identify the source of a molecule. These can serve as a "fingerprint" of one or more of the product's components, or an additional marker with a distinct signature can be added. Highly specialized laboratory equipment is needed for detection.

5. MICRO-TAGGANTS

Micro-taggants are tiny particles with coded information that can be used to specifically identify each variant when examined under a microscope. This could be in the form of shards of multicolored, multilayered laminates with a distinctive color scheme or alphanumeric data printed on tiny flakes or threads. These can either be directly put to packing components as spots or threads or inserted within adhesives.

SERIALISATION/TRACK AND TRACE TECHNOLOGIES

Although the concepts have been well-established for many years in other contexts, there are currently a number of Track and Trace applications being developed for the pharmaceutical industry. This entail giving each stock unit a distinct identity during manufacturing, which stays with it along the supply chain until consumption. Although in theory it may just take theform of a unique pack coding that provides access to the same information kept on a secure database, in practice this identity will typically include details of the product name and strength,as well as the lot number and expiry date.

These perform several different **tasks**, including

(a) **tracking** an item along the supply chain to every location with a data collecting facility.

(b) Giving a **history** of any item's traceability (electronic pedigree), subject to a cap on the number of control points.

(c) Make it possible for the data to be **authenticated** at any time, implicitly including the pack or unit to which it is applied.

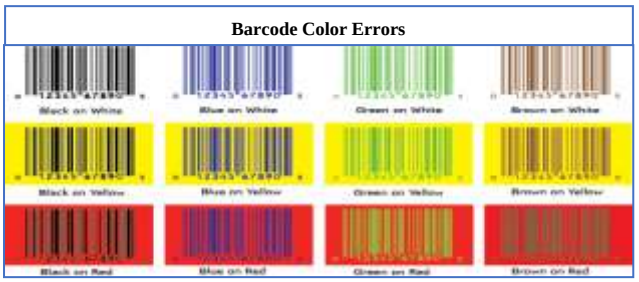
The most obvious advantages are in **supply logistics**, where increased *inventory* and *demand transparency* can result in increased ***productivity*** and lower ***costs***.

Serialization The security of the Track and Trace label is substantially improved with the addition of unique and seemingly random serialization, or non-sequential numbering, ideally at the individual item level. The Track and Trace label may not be resistant to copying or falsification on its own. The level of security would be very poor if the serialization were sequential because the sequence is predictable, however "random" serialization utilizing a highly secure algorithm or form of encryption gets around this. Individual packs may still be duplicated, but the database will spot duplicates or invalid serials, along with those that have been cancelled or expired, appear in the wrong market, or have erroneous product details. Individual packs may also still be copied. Customers may authenticate packs when secure serialization is applied visibly to them by connecting to the database through the phone or the internet. To guarantee that the data is easily available while remaining secure against

compromise, one issue that needs to be tackled is ownership, management, and access to the database. To enable automatic data collecting, there are two primary ways to incorporate unique pack data:

A. MACHINE-READABLE CODES OR BARCODES:

- Identification codes called "machine-readable codes," or "barcodes," are those that are intended to be readable by technology like optical scanning equipment.
- A barcode is made up of ***parallel black lines***, ***white spaces***, ***dots***, or ***squares*** of variable widths, or a combination of the two.
- Unique identifiers or product-related information, such as the owner, origin, expiration date, and date and location of manufacture, are written into the codes. A reader, which can currently be a laser beam or a smartphone camera, analyses and extracts the data from the codes by decoding the binary data in the barcode.
- These are high-density linear or two-dimensional bar codes that incorporate product identity right down to the level of the unit pack.
- They are scanned and used as a point of reference for the main database.
- The 2D data matrix code is one widely used implementation, while other options include PDF417 codes.
- The normal size of a 2D code is 1 cm square or less, but it can hold up to 1 Kb of data with sufficient "redundancy" or error correction.
- Linear bar codes can also be used if space is not an issue.
- The codes can be printed online using inkjet or digital printing techniques, enabling direct computer control and data transfer to the main database.
- The need for line-of-site scanning across the supply chain is eliminated by the development of hierarchical systems in which the label on a shipping case is intimately linked to the identities of all of its contents.
- This capability can also be extended up the chain to pallet labels.
- Technologies referred to as "**nano-printing**" enable microscopic application on individual tablets.



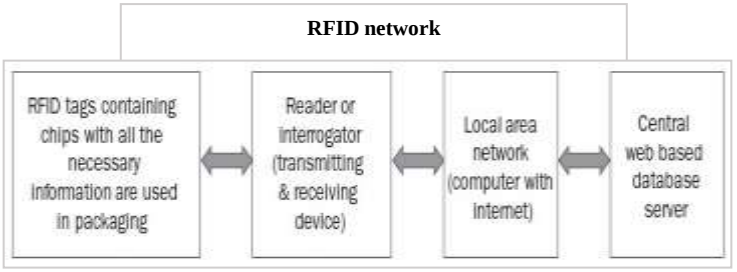
TYPES

- **ONE**-*DIMENSIONAL* BARCODES
- **TWO**-*DIMENSIONAL* BARCODES

B. Radio Frequency Identity (RFID) Tagging

- An antenna with a microchip in the middle makes up an RFID tag.
- This has batch and item-specific data that can be accessed remotely and without a direct line of sight (unlike bar codes).
- The range and sensitivity depend on the radio frequency being utilized, but no single standard is appropriate for all purposes.

- While some systems can record multiple records for a variety of items, there are certain challenges with tag orientation and radio signal absorption by liquids and foils. However,
- RFID has the ability to be fully automated in warehouses and even extend to pharmacies without requiring manual intervention, which is a definite advantage.
- Data standards and equipment specifications are being created. The price of tags, as well as the lack of application and verification equipment if it is to be applied at the pharmacy level, continue to be major obstacles to individual pack application.
- Another problem is the tags' robustness throughout application and handling all the way to the end of their useful lives, as studies to date have shown a high failure rate.
- Nevertheless, there is hope that a printed edition will be created. Prior to widespread application, privacy concerns and susceptibility to intentional adulteration must alsobe addressed.



TYPES

- ***PASSIVE RFID TAGS*** are most frequently found as smart labels. They can be attached to a range of products for a number of reasons, including trademark protection and anti-counterfeiting, and are typically composed of adhesive paper or plastic. They carry important data that is used to track goods as they go from the warehouse to the point of sale, enable customers to leave a store without having to stand in line to pay for a purchase, and let sales staff check inventory without separating themselves from the customer.
- ***ACTIVE RFID TAGS*** utilized for remote inventory and to make sure that items stay where they belong, offering anti-theft security as well.
- ***BATTERY-ASSISTED PASSIVE (BAP) RFID TAGS*** These RFID tags have a tiny battery that only supplies power to the microchip. This enables them to execute and retain data from environmental sensors, as well as benefit from larger, potentially rewritable storage (among other possible types of sensors). BAP tags are frequently used in the "cold chain" to ensure that the temperature of products (food, medications, or other healthcare products) remains at a consistent low level from the manufacturer to the end user because of these properties.
- ***PHYSICAL UNCLONABLE FUNCTION (PUF)*** An RFID tag's chip uses PUF technology. Since it involves recognizing and authenticating a certain sort of RFID tag (passive, active, or semi-passive), it can be used in the same circumstances and for the same purposes.

C. Unique Surface Marking or Topography

- A pseudo-random picture, such as a pattern of lines or dots in one region of the carton, can be applied in a number of ways to each item in a batch before the signature is scanned into the batch database using secure algorithms for subsequent authentication.
- As an alternative, the pack surface offers a distinct fingerprint that can be read by a special laser instrument, allowing each pack to be registered into the database during batch manufacturing and making it hard to duplicate or forge.

- Although it is not yet fully developed, unique pack serialization has the potential to provide reliable solutions to fraud and pharmaceutical counterfeiting.
- Although barcode systems make use of tried-and-true existing technology, they lack the advantages of automation and remote scanning offered by RFID.
- RFID tags could be corrupted or altered on purpose and invisibly.

OTHER TECNIQUES

1. INK

- If a special product identification number is incorporated in the marking, ink-based technologies, which are generally used for product verification, may also be utilized for identification and tracking.
- The majority of these technologies are accessible and somewhat cheap to use.
- They are frequently used to authenticate paper products, such as paper documents and valuables, and are quite successful in doing so.
- For the goal of preventing counterfeiting, a variety of inks can be used to mark products.
- They can be identified based on:
  - ✓ reaction to chemicals
  - ✓ reading procedure
  - ✓ reading tool
  - ✓ specific characteristics

- Both visible and invisible anti-counterfeit inks are possible. Uses for invisible ink include:
- Avoiding doing so will help to:
  - ✓ prevent simple identification by possible counterfeiters;
  - ✓ avoid interfering with the product's following processing; and
  - ✓ avoid changing the product's look.

TYPES

- Photosensitive ink that is visible to the unaided eye but changes color or vanishes when exposed to ultraviolet light is known as ***UV-SENSITVE INK (UV LIGHT)***. fluorescent pigments, which appear in two different shades under UV light. Only specialized tools, like a "Wood's light," can detect the ink.
- ***IR-SENSITIVE INKS*** must be identified with a particular infrared scanner because they are absolutely invisible to the human eye. Barcode concealment or anti-replication is one of the more popular uses of IR-sensitive inks. They typically outperform UV-sensitive inks, which can lose their effectiveness with time, in terms of strength and durability.
- ***MAGNETIC INKS*** contain metallic pigments that react strongly to magnets. The most used method for serializing and numbering on banknotes and checks is magnetic ink. They can also be used to encode documents with magnetic bar codes, allowing information to be read and the authenticity of the documents to be verified.
- ***OPTICAL VARIABLE INKS (OVI) AND IRIDESCENT INKS*** These inks are produced using pigments that, when viewed from different angles, appear to be two different colors. Common color combinations include red-green, gold-silver, and green-

blue. OVI is regarded as the best type of ink to avoid document fraud since it is so difficult to duplicate; copiers and scanners cannot copy the color change effect.

- ***THERMOCHROMIC INKS*** change color when subjected to temperature changes, even those as slight and brief as those brought on by finger rubbing. The color change may be irreversible or reversible, meaning that the ink will revert to its original color if the temperature returns to its original level. When heated, some inks become transparent, displaying the color of the background beneath.

- ***REACTIVE INKS*** which react when exposed to aqueous solutions, solvents, and other chemicals The reaction may manifest in a variety of ways, including erasing, discoloration, color transformation, running, staining, and smudging, all of which clearly indicate that an attempt was made to alter the object.

  - ***Types Of Reactive Ink***
  - ✓ Erasable inks use water-soluble dyes and resins; hence they can only be used in dry offset printing or typography. Some nations print the backgrounds of their checks using erasable ink.
  - ✓ Solvent-sensitive inks are those that respond to chemicals or solvents like alcohol, acetone, or bleach, which are frequently employed in forgery efforts. These inks will run, alter color, or leave a stain when exposed to solvents or chemicals, making the fake obvious.
  - ✓ Fugitive inks: These inks respond to water or an aqueous solution in a manner similar to solvent-sensitive inks. The fake will be obvious since the ink will bleed and smear the printed area.
- ***PENETRATING INKS*** Also known as "bleeding inks," these inks penetrate a document's paper substrate completely. Any attempt to mechanically remove the contents of the document will expose the ink and leave behind obvious damage.

2. ENCRYPTED IMAGES

- This technology functions by adding encrypted data to the background of images or documents.
- The encoded information is printed in an encoded format and cannot be seen with the unaided eye.
- It can only be seen while using a special decoding lens (special viewer) or laboratory apparatus (usually a scanner or video camera connected to a computer equipped with specific image processing software).

3. WATERMARKS

- Design or pattern imprinted on paper during manufacture is known as a watermark.
- They are created by exerting pressure in the form of a pattern or text to the substrate.
- Only the places where pressure was applied experience the paper's compression and thinning as a result.

- The thinner areas of the paper allows more light to pass through, making the watermarked picture visible without the need for additional materials.

4. MICROTEXTS

- This technology entails creating a text or a whole document at a microscopic scale, with the final text only being readable by highly developed machinery.
- Microtexts are printed using specific inks and procedures from specialized machine- or laser-engraved matrices.
- Due to the need for exceptional precision in recreating the minute features, they demand sophisticated graphic technology.
- Given the tiny scale of the produced text, a print quality superior to ordinary offset printing plates is typically required.

5. UNIQUE IDENTIFIER MARKS

- In essence, this technique operates by adding obvious or covert identifiers to goods or paperwork.
- The identifiers appear to be accidental ink smudges or spots when they are visible.
- Typically, they are created by arbitrary, essentially non-replicable chemical and physical processes. In rare circumstances, it might also be possible to print the encoded signature on the product as a 2D barcode.
- This would assist in both the identification and tracking of the marked goods. OR
- Documents and packaging can be directly affected by this technology. The pre-recorded identities and/or encoded signatures can also be printed on labels as an alternative.

6. COPY DETECTION PATTERNS

- Small, random or pseudo-random digital pictures to be printed on packaging, goods, or papers to identify counterfeits are known as copy detection patterns, also known as secure graphics.
- The technology is founded on the idea that some of the information present in the original image is lost every time a digital image is printed or scanned, regardless of the scan's quality or the photocopying method employed.
- When information is printed or copied, copy detection patterns (CDPs) are created to minimize this information loss.
- The counterfeit picture produced will have less information than the original image since a counterfeit copy detection pattern will have been duplicated or scanned at least twice more than the original.
- Therefore, authentication is carried out using an algorithm that contrasts the original with the quantity of information in the scanned copy detection pattern.

CHEMICAL AND PHYSICAL TECHNOLOGIES FORANTI-COUNTERFEITING

These systems' primary objective is authentication without concurrent unique product identification. To read and validate the markers they produce, specialized devices or laboratory

testing are required. As a result, it is highly challenging for outside parties to develop identical marks. The creation and application of chemical & physical markers often comes at a modest cost.

However, when necessary, specialized automatic reading machines might be pricey. It is important to remember that fast on-site verification is frequently impractical. Instead, testing must be performed in labs, which takes additional time. Four different categories of chemical and physical technology exist:

1. GLUE CODING

- In the process of "glue coding," bubbles emerge in a polymer randomly, spontaneously, and uniquely.
- Each specific combination is as unique as a snowflake since the precise location, size, and form of the polymer bubbles vary every time.
- Each set of bubbles is documented in a database for reference that is solely available to the product owner.
- Because they are virtually impossible to duplicate, these unique three-dimensional patterns are excellent for preventing and spotting fake goods.

2. SURFACE FINGERPRINT & LASER SURFACE ANALYSIS

- A unique identifier is created using surface fingerprint technologies and laser surface analysis based on the results of a physical random process that is, by its very nature, unrepeatable and uncopiable.
- Techniques that pinpoint the structural variations unique to each surface are used to analyze the composition of the materials' surfaces.
- These variations are used to generate identifiers that enable the product to be uniquely identified.
- For instance, special identification codes can be generated at random by analyzing the structural changes that are produced on silicon films (also known as "wrinkles").
- Similar to a person's fingerprint, these codes are univocal, making it technically impossible to duplicate them.

MECHANICAL TECHNOLOGIES FOR ANTI-COUNTERFEITING

Effective anti-counterfeiting and anti-tampering barriers are made possible by mechanical technologies, which interact with the physical characteristics of materials. They carry out basic authentication tasks when used alone. They can also be used for tracking and identification when combined with other technologies.

1. LABELS

- Any tangible component that is applied to a product or its packaging and contains identification information and product details is referred to as an identification label.

- Paper and plastic film, which frequently have information printed on front and an adhesive coating on the reverse, are most frequently used materials for labels (adhesive labels).

- The type of adhesive, the support utilized (such as silicon paper), the printing process, the degree of resistance to atmospheric agents, and the type of use are all variables.
- Identification labels can be applied to any kind of container or packaging, including cardboard boxes, glass bottles, jars, or plastic bags, as well as directly to the product itself (for example, in the case of clothing or footwear).
- When weighing different implementation strategies, it's important to take into account whether it might be more cost-effective to incorporate specific solutions into the artwork that will be printed directly onto the cardboard, plastics, or shrink sleeves, thereby avoiding the need to alter the standard production procedure.
- Labels can be used in conjunction with a number of other technologies to increase security. They become "smart labels" when they are paired with near-field communication (NFC) or radio-frequency identification (RFID) tags.

TYPES

- ***FABRIC LABELS*** These labels typically take the shape of a tiny scrap of cloth that bears the brand name, contact information, and a few product-specific characteristics like the item's origin, size, composition, washing instructions, etc. They work well for product identification, especially when paired with a barcode or hologram. They can also be paired with an RFID tag to create "smart labels". Fabric labels come in two different forms: woven and printed. The logo or text is either woven into the fabric itself or printed on top of it.
- ***LABELS WITH MICRO-ENGRAVED CLICHÉ*** Micro-engraved clichés are hot-printed onto labels for use on labels. A cliché is a metal matrix with engravings that replicate various designs, pictures, etc. The surface of micro-engraved clichés has an incredibly delicate texture and can be personalized with random or recurring designs. This tiny texture, when hot-printed onto the label, produces optical refractive effects that, like a hologram, alter form and color when viewed from different angles.
- ***ULTRA-RESISTANT LABELS*** A wide variety of special plastic materials, including vinyl, nylon, polyester, and polyethylene, can be used to create ultra-resistant labels. These materials are resistant to solvents, detergents, oil, grime, UV rays, and seawater and can tolerate temperatures as high as +250°C and as low as -40°C. Labels composed of polyester and polyethylene can adhere to curved surfaces since these materials are stretchy as well. Aluminum and other non-plastic materials are also acceptable choices.
- ***ULTRA-DESTRUCTIBLE LABELS*** Extremely fragile materials (typically paper or PVC) are used to create ultra-destructible labels, which are then glued on. The label will shatter into small fragments if someone tries to remove it, making it impossible to do so completely. This combination makes it impossible for the label to be removed. They are therefore a highly potent anti-tampering method. These labels are also ideal for the food industry, where they are placed on jars and other products to assure freshness.

- ***VOID LABELS*** These labels function by transferring a portion of their color to the product in the shape of the term "void," a custom text (such as "opened,"), or a logo. Because of this, removing the label leaves a visible trace of an attempted manipulation. The same alert message will still appear in negative when the label is reapplied if the message or logo is removed from the product. They offer a practical means of maintaining the integrity of the product across the whole supply chain, from production to retail sales.

2. LASER ENGRAVING

With the use of this technique, any support or surface can be cut with closely spaced grooves of different depths. On top of the engraving, images, logos, text, or identifying codes can be placed; when viewed from different angles, they will change color. The fact that the marking is permanently attached to the goods and hence extremely difficult to tamper with is a significant benefit of this technology. There are three primary methods of laser engraving:

- ***ANNEALING*** sometimes known as laser surface stamping, is a process that discolors ferrous metals like titanium by heating the metal's surface and generating oxidation underneath.
- ***REAL LASER ENGRAVING*** is a process that involves removing material from a product's surface in the shape of the marking (this is especially used for metals, plastics and ceramics)
- ***DEEP LASER MARKING*** is a highly specialized method in which markings are applied to a product's surface at a certain depth (which is usually made of metal).

3. ANTI-ALTERATION DEVICES

- The alcoholic beverage sector uses this technology extensively to stop the counterfeiting of wines and spirits.
- Anti-alteration tools, such as anti-refill caps, prevent this by installing one-way valves in the necks of bottles, rendering it impossible to re-pour liquid.
- To further deter tampering and alteration, anti-alteration devices can be used in conjunction with shrink sleeve labels applied to bottle and jar caps and lids.

4. SEALS

- Any mechanism that hermetically shuts a package to safeguard the contents from alteration is called a seal. Seals can be as straightforward and affordable as a screwcap on a bottle, and they can be constructed of plastic or metal.
- They are typically simple to install and remove, but the degree of protection they provide much depends on the knowledge and skills of the person conducting the inspection.
- A seal's general characteristics include:
  - ✓ identity (each seal has a distinctive identifier);
  - ✓ non-duplicability (seals are very difficult to duplicate); and
  - ✓ reliability (seals offer a high level of security).

- Mechanical seals come in many forms, but they all have the following features in common:
  1. Visual inspection is used to determine their integrity.
  2. They reassure a consumer about product's security through visual proof of tampering
  3. They don't keep track of the date or location of any tampering.

4. Unlike electronic seals, they cannot verify their own integrity.

5. SECURITY THREADS

- Security threads are weaved into or otherwise attached to items to enable authentication and prevent tampering.
- They are made of a variety of materials (metal, cloth, polymers).
- Due to the variety of thread materials, this technique can be used into a wide range of items. For enhanced protection against counterfeiting, additional security measures, such as specific coatings or microprinting, may be put to the thread.
- The various security thread varieties can be categorized by both material and purpose:
  - ✓ ***METAL THREADS***, such as those found in banknotes, are directly incorporated into the product to prevent copying.
  - ✓ Other threads for attaching and/or sealing (polypropylene, fabric, etc.); these are used, for instance, to attach tags to clothing or products and as micro-seals for warranties.
  - ✓ ***POLYMERIC THREADS***, which come in a range of thicknesses and can be:
    - metal-coated (totally or partially) painted with specific light-sensitive pigments
    - microprinted with numbers and text that can only be read by magnetic readers to include concealed information.

6. SECURITY FILM

- This technology's primary objective is to protect data printed on documents and packaging.
- It accomplishes this by applying a plastic layer with pressure or heat to the pages or other surfaces that require protection with security measures such as printed, tactile, or colored.
- The three most typical methods for incorporating security into the movie are as follows.
  - ***OVERPRINTING*** To prevent damage and manipulation, security features are often printed on the back (inner side) of the security film or in the space between the adhesive layer and the film (they are usually printed by screen printing, rotogravure or flexographic printing).
  - ***EMBOSSING*** Tactile elements like fine lines, intricate patterns made of thin lines, or microscopic prints are embossed onto the security film.
  - ***EMBEDDING BY BINDING*** this method typically safeguards printed personal identification information and images in passports. The film is inserted into the passport book through the binding to prevent tampering; as a result, a strip of the film creates a thin margin on the page next to it on the document's reverse. Iridescent film, which has a dazzling, pearlescent quality and changes color when viewed from different angles, and back-reflecting film, which is made visible by a particular viewing device that employs coaxial light, are two further, less prevalent methods.

7. DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEMS

- DRM technologies regulate who has access to and utilizes digital content. There is a DRM system at work when streaming services restrict the number of devices per account or when game developers demand customers enter a product key before playing.

- DRM systems are made to prevent the widespread, unauthorized copying anddissemination of online-based digital content protected by copyright. To assist copyright and associated rights holders in securing their digital material and managing access to it, they employ two key procedures:
  - ***USE OF METADATA*** the digital files contain information (such as the buyer's name or account information) that can only be read by certain software.
  - ***ENCRYPTION*** Depending on the authentication processes, the encryption key may be made available offline or online and transforms the digital content into a code that can only be read by hardware or software that has it.
- Digital files are made very difficult to duplicate (outside of the managed environment) by encoding and encrypting them. DRM systems also make sure that their use is constrained (to certain times or purposes) and governed by the terms of the access license given to end users.

8. SHARED LEDGER TECHNOLOGY FOR ANTI-COUNTERFEITING (BLOCKCHAIN & ENCRYPTED QR CODES)

- Using shared ledger technology, which is a type of digital data storage, transactions may be sent, received, tracked, and completed more quickly and securely.
- The most well-known shared ledger technology is blockchain.
- There is no requirement for reliable intermediates because it uses a decentralized design.
- Transaction's origin as well as associated data must be verified by all blockchain users.
- The transaction data is encrypted and saved in a new block after being verified. The next block in the chain, which is the link, likewise contains a copy of the encrypted data.
- Participants can verify the whole history of a transaction since data contributed to a block can never be removed.
- Blockchain was developed as a solution to protecting digital money from replication risk.
- Despite the fact that blockchain technology is still relatively young, certain anti-counterfeiting solutions have already been implemented.
- Such systems enable businesses to monitor their own supply chains and develop their own product IDs, among other things.

How It Works

Here is an illustration of how blockchain might be used in real-world applications to safeguard a pharmaceutical supply chain.

- The manufacturer, the packager, the wholesaler, the distributor, the doctor, etc. are all links in the chain. Participants can be objects, people, or other entities. Each participant is given a key identifying their particular network activity. The original identities of the participants are concealed, and they are only identified by these keys, such as "manufacturer," "packager," etc.
- The "assets" in the supply chain are medications. A special key is assigned to each medication (or hash). A QR Code serving as the medication's identification is added to it.

- The transaction records must be stored on a specific blockchain network. A few examples of networks on the market are BigchainDB, Ethereum, Hyperledger, and Bitcoin Blockchain (the original network).
- The blockchain stores all necessary transactions. Once data has been added to the blockchain for a specific transaction, it cannot be modified.
- Participants utilize a smartphone app to conduct blockchain transactions.
- A mobile app makes it simple to transfer ownership of the medication to another person. Possible outcomes include:

RECENT NEW INNOVATIVE TECHNOLOGIES

CRYPTOGLYPH®

Your current print vendors can add a digital invisible marking called Cryptoglyph® to printed products without altering the design in any way and without using any specialized inks or other consumables. With a Cryptoglyph®, product protection is achieved by printing tiny holes or tiny dots in the varnish or solid color layer. With the aid of a special smartphone app, the detection is carried out.

CYPHEME'S NOISE PRINT

This strategy is accomplished by adding a chemical to the printing process that, by itself, generates random patterns. Similar to a fingerprint, the resulting pattern by AI is unique and cannot be duplicated. At this way, it is impossible to create an identical replica of any label, even with the same tools or in the same factory.

Aims And Objectives:

Certainly! Anti-counterfeiting efforts aim to protect consumers by ensuring they receive safe and genuine products, safeguard the reputation of businesses and brands, and minimize the economic and health risks posed by counterfeit goods. These efforts involve enforcing intellectual property rights, enhancing supply chain security, fostering global cooperation, raising public awareness, and leveraging advanced technologies to detect and deter counterfeiting. Legal remedies, industry collaboration, and customs control measures are essential components in the fight against counterfeiting, working together to create a safer and more reliable marketplace for everyone.

Methods:

We constructed a conceptual framework for diverse anti-counterfeiting strategies, drawing upon a comprehensive examination of existing literature. This framework provided us with direction in refining our review inquiry and in formulating the criteria for inclusion.

CONCLUSION

Overt user-verifiable solutions were generally reliable, reasonably priced, and easily understood by end users, they would be the best choice. Although some licensed technologies make this claim, requiring their use would be ineffective. Their wider use would serve as a bigger incentive for counterfeiters to spend in manufacturing the technology, as has happened with holograms, even if they would not be appropriate for all uses or affordable by all manufacturers for all products.

KEYWORDS:

Covert, Sterilization, Counterfeit, Cryptoglyph, Annealing

RECOMMENDATIONS

OVERT FEATURES

- Only the manufacturers' discretion should be used when using overt features. Where they are utilized, manufacturers should inform the public (including wholesalers, distributors, and healthcare professionals) about how to authenticate them.
- It serves little use to require the adoption of an overt solution because counterfeiters will be forced to try to undermine or get around it.

COVERT FEATURES

- Since widespread use of covert markers raises everyone's danger of compromise, it's use should be discouraged as they cannot be depended upon to completely stop counterfeiting.
- Manufacturers ought to think about informing reliable supply chain partners about some concealed indications.
- **Manufacturers have a lot to gain from covert solutions, while authorities and the general public gain little because of the possibility of compromise if they are widely used or understood. Although they can be quite easy to handle and very cost-effective.**

FORENSIC MARKERS

- Use should be promoted in high-risk sectors, however, producers must be free to choose which system to use, and effort to impose a particular solution must be opposed.
- **Even such forensic markers have some benefits over more straightforward covert features, they are typically more expensive, both in terms of equipment costs and licensing or royalties. They may bridge the gap between less secure covert features and unreliable overt features due to their security being sufficiently strong to allow for overt marketing of their presence.**

SERIALISATION/ TRACK & TRACE TECHNOLOGY

- The foundations for the harmonization of a global system include the establishment of specifications for the database architecture and data structure. It is necessary to agree on the fundamentals of ownership, management, and access, and to make the access methods as flexible as possible.
- **Serialization/Track and Trace systems differ in that they guard the supply chain against espionage and abuse rather than necessarily being safe against copying.**
- Manufacturers should be free to choose the hardware platform, however barcode-based system should be built for efficiency and speed, allowing a smooth evolution to RFID if, when, and where practical. While 2D barcodes are more cost-effective at the individual pack level, RFID tagging may be more efficient at the pallet and case levels.
- A working committee with representation from branded and generics makers, wholesalers, distributors, pharmacists, and healthcare professionals should be formed to develop the requirements.
- How access might be granted to authorities like customs, police, and public health investigators, as well as eventually to the client, should be taken into account.

REFERENCES

BOOK

- Aulton, M. E., & Taylor, K. (2018). ***Aulton's pharmaceutics: the design and manufacture of medicines***. (5th Ed.). Elsevier Health Sciences., *Part 5*: Dosage form Design & Manufacture, Chapter: **30** Tablets & Compaction (Pg. 518-561)
- Roy, J. (2011). **An introduction to pharmaceutical sciences: Production, chemistry, techniquesand technology**. Elsevier. Chapter: **12** Counterfeit Drugs & Drug Abuse (Pg. 327-348)

RESEARCH ARTICLES

- Deisingh, A. K. (2005). Pharmaceutical counterfeiting. *Analyst*, *130*(3), 271-279.
- Bale, H. (2005). Pharmaceutical counterfeiting: Issues, trends, measurement. WIPO/OECD Workshop.
- El-Jardali, F., Akl, E. A., Fadlallah, R., Oliver, S., Saleh, N., El-Bawab, L., ... & Hamra, R. (2015).Interventions to combat or prevent drug counterfeiting: a systematic review. *BMJ open*, *5*(3), e006290.
- Wertheimer, A. I., & Santella, T. M. (2005). Counterfeit drugs: defining the problem and finding solutions. *Expert opinion on drug safety*, *4*(4), 619-622.
- Blackstone, E. A., Fuhr Jr, J. P., & Pociask, S. (2014). The health and economic effects of counterfeit drugs. *American health & drug benefits*, *7*(4), 216.
- Hoecht, A., & Trott, P. (2014). How should firms deal with counterfeiting? A review of the success conditions of anti-counterfeiting strategies. *International Journal of Emerging Markets*.
- Bansal, D., Malla, S., Gudala, K., & Tiwari, P. (2013). Anti-counterfeit technologies: a pharmaceutical industry perspective. *Scientia pharmaceutica*, *81*(1), 1-14.
- Rasheed, H., Höllein, L., & Holzgrabe, U. (2018). Future information technology tools for fighting substandard and falsified medicines in low-and middle-income countries. *Frontiers in pharmacology*, *9*, 995.
- Kabiru, J. W. (2013). The effects of counterfeits on pharmaceutical distribution and retailing in Mombasa county, Kenya (Doctoral dissertation, University of Nairobi).
- Pitts, P. (2020). The spreading cancer of counterfeit drugs. *Journal of Commercial Biotechnology*, *25*(3), 20-14.

WEBSITES

- https://www.fip.org/impactglobalforum/pdf/backgroundinfo/IMPACT%20-%20AC%20Technologies%20v2.pdf
- https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfe iting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf
- http://www.nifds.go.kr/apec/SupplyChain/APEC_SupplyChainToolkit_170317.pdf
- https://www.gsma.com/iot/wp-content/uploads/2012/03/sproxilfinal.pdf
- https://alpvision.com/pharmaceutical-counterfeiting/

- https://www.fiercepharma.com/special-report/top-counterfeit-drugs-report
- https://www.cypheme.com/post/why-cyphemes-noise-print-is-better-than-qr-code-rfid-and-other- anti-counterfeit-solutions
- https://khangthanh.com/en/Other-news/Barcodes-On-Packaging-Identify-Authentic-And-Fake- Products-1409.html
- https://holoprint.ae/blog/Holoprint-helped-a-pharma-company-to-knock-off-product-duplication/
- https://www.healthcarepackaging.com/news/traceability-serialization/blog/15629409/using- holography-to-fight-pharmaceutical-and-healthcare-brand-piracy