AC 2011-2192: ANTI-COUNTERFEITING TECHNOLOGY IN PRODUCT DESIGN AND MANUFACTURING: AN OPPORTUNITY FOR ENGINEERING TECHNOLOGY PROGRAMS

Daniel P Johnson, Rochester Institute of Technology

Daniel P. Johnson is an Associate Professor and Department Chair in the Manufacturing and Mechanical Engineering Technology/Packaging Science Department at Rochester Institute of Technology. He is the past Program Chair for Manufacturing Engineering Technology and teaches courses in manufacturing operations, automation, robotics, and computer aided manufacturing. Prior to joining the MMET/PS Faculty he was Director of RIT's Manufacturing Management and Leadership Program and Engineering Manager for the Center for Integrated Manufacturing Studies. His industrial experience includes work as an Advanced Manufacturing Engineer for Allied Signal. He has a Master of Engineering Degree in Manufacturing and a BS in Industrial and Manufacturing Engineering from RIT and an AS in Engineering Science from Hudson Valley Community College.

Rebecca Dobbs, Rochester Institute of Technology
Changfeng Ge, Rochester Institute of Technology (COE)

Dr Changfeng Ge is an associate professor at Rochester Institute of Technology. He holds Bachelor's and Master's degrees in Mechanical Engineering , and a Doctor of Engineering Degree in Packaging and Distribution from University Dortmund, Germany. He is Chairman of ASTM D10.13 packaging committee. He also holds the title of Editor-In-Chief, Journal of Applied Packaging Research, US. His research interest include: Packaging Performance Prediction using mathematic modeling ,barrier packaging material development and transport packaging design.

Anti-Counterfeiting Technology in Product Design and Manufacturing:

An Opportunity for Engineering Technology Programs

Introduction:

Counterfeit products have drawn considerable attention in recent years as a consumer problem and crime of growing concern. When considering the issue of counterfeit items, one might think only about pirated music CD's and 'fake' Rolex watches. However, a significant part of the counterfeit industry is producing items that consumers may find indistinguishable from 'the real thing'. A serious concern is items in the industrial supply chain that are not what they are promised to be. A common example being counterfeit cell phone batteries that may pose a performance and safety concern. Fraud in the area of counterfeit goods ranges from simple mislabeling of product, to enterprises completely dedicated to producing exact copies of name brand consumer products. Items counterfeited range from sneakers with an illegal designer logo, to counterfeit prescription medications and medical devices.

Counterfeiting has been estimated to be a $500B market, and one of the fastest growing industries in the world. [1] Ongoing globalization of manufacturing, distribution and markets is likely to expand the reach of the problem and add significantly to the challenge companies will face protecting their product and supply chain integrity. A wide range of individuals and enterprises make up the spectrum of exactly who engages in the activity of creating copies, knockoffs, fakes and frauds. As a research field however, the subject of anti-counterfeiting technology presents some challenge in that researchers working in the area may be reluctant to publish their findings in order to prevent the dissemination of the technologies to those working to defeat these new techniques.

A wide range of items can be considered counterfeit or bogus in that the item violates trademark or copyright laws and/or misstates its origin, performance, material composition or other characteristic. Table 1 presents examples in general categories.

Table 1: Counterfeit Item Examples

Fashionable Item Knockoff	Enterprises dedicated to duplication produce low cost copies of designer goods, and distribute through semi legitimate channels	Purses Sneakers Clothing Electronics Perfume
Digital Duplication	Distribution of unauthorized copies of digital material, often with no attempt to disguise the item as legitimate	Software Music CD's Movie DVD's

Licensed Production Fraud	Manufacturers licensed to produce name brand goods produce outside of the agreed quality and quantity in the production contract. A 'ghost shift' of extra production.	Electronics Clothing Sneakers Batteries Auto Parts
Fraudulent Items	Items produced to a standard just good enough to fool the initial buyer. May not function at all or contain necessary components.	Pharmaceuticals Cigarettes Electronics Auto Parts Liquor
Consumer Goods Copies	Low cost copies of common consumer items. Buyers and even retailers/wholesalers may not know the items are bogus	Cigarettes CD's DVD's Liquor Shampoo Razor Blades
Business to Business/Supply Chain Fraud	Raw material, components and supply items that are used, scrap, refilled, relabeled or have misstated properties	Metals Auto Parts Airplane Components Electronic Components
Specification Fraud	Non-name brand manufacturers falsify material content, UL certification, product performance information, etc.	Tools Electronics Food Items Personal products (toothpaste, soap, etc)
Imitators	Legitimate companies that produce copies that come very close to violating copyright or trademark protection	Fashion Clothing Electronics Tools Herbal Supplements

Challenges:

A number of factors have been identified as driving an increase in counterfeit goods. The first is demand created by an expanding global marketplace. Emerging markets are demanding fashion name brand products, popular music, electronics, personal products, soft drinks, liquor and cigarettes to name only a few. Many these markets are not fully served by internationally known brands, so a gap is created that can be filled by counterfeit items. The very existence of internationally known mega-brands such as Nike drives demand for copies. Remote markets once served by local producers and brands are demanding internationally known items. In some cases these same local producers may become counterfeiters. Another driver is the common corporate practice of licensing other companies to manufacture and distribute products and/or outsourcing manufacturing. These practices make it quite common to find factories around the world doing full service contract manufacturing, and manufacturing branded products under license agreements. This remote production may be lightly monitored by the brand owner. The

temptation is then to produce ‘extra’ items which don’t need to meet agreed upon quality levels and for which the licensing fees are not paid to the brand owner. A final reported driver is organized crime and terror organizations forced out of more dangerous activities like drug and human trafficking by increased enforcement, have found product counterfeiting to be an easy money making alternative. [1]

Dangers inherent to the existence of illegitimate products are many. For the manufacturer/brand owner of the legitimate product there is an obvious loss of revenue. Additionally their brand and product reputation can be significantly damaged when consumers, unaware that they are using a fraudulent item, are unhappy with its performance. These same consumers may also take legal product liability action against the producer for damage done by the product. The producer in this situation could be faced with proving that the items were not legitimate, and that they had taken reasonable steps to prevent such items from falling into the hands of consumers. Risks for consumers follow these same themes. Funds may be spent on illegitimate items, harm may come from using items manufactured without regard for the consumers safety, and in the case of a fraudulent business to business sale the purchasing company my become liable for the poor performance of an item they felt was legitimate.

Law enforcement, border security and customs officials are commonly engaged in prevention and detection of illegitimate product trade. Many companies employ their own specialists who attempt to detect and prevent trademark infringements, counterfeit goods production and their distribution and trade. Traditionally enforcement is focused on detecting items in the marketplace or as they travel through international customs procedures in the supply chain. In fiscal year 2010 US Customs and Border Protection is reported to have seized more than $260 million worth of counterfeit goods including snuggies, DVD’s, brake pads, computer parts and baby formula. Counterfeit footwear and electronics were the largest categories, accounting for 40% and 12% of seizures respectively. [2] A critical aspect of enforcement is producers providing law enforcement with a means to identify items as illegitimate. Enforcement officials clearly can’t be experts at spotting fakes as diverse as purses, electronic components, airplane parts, auto parts and sneakers, so a reliable method of verification is one key to the enforcement process.

Technologies:

Current anti-counterfeiting technologies can be classified into five major areas. These five are classified by the tracking method utilized: covert pattern tracking, overt pattern tracking, random tracking, cryptography and optical variable devices. Covert and overt pattern tracking are conventional technologies. Random pattern and cryptographic technologies are based on physical uncloneable function (PUF) technologies that are difficult to counterfeit. Table 2 illustrates a comparison of the five identified technologies in terms of their registration and verification process as well as the main features of each alternative.

Table 2: Summary of Technologies

Technology	Registration Process (Encode)	Verification Process (Decode)	Main Features
Covert Pattern Tracking	Tag	Reader	Low cost, easy and quick to counterfeit, difficult to identify the source of counterfeit
Overt Pattern Tracking	Sticker	Eye, Decoder	
Random Pattern Tracking	Tag, Camera	Scanner, Camera	Reliable, difficult to counterfeit
Cryptography	Label	Eye	Multiple verifications in supply chain, difficult to counterfeit
Optical Variable Devices	Embossed Microstructure	Eye	Difficult to counterfeit, high cost

Anti-counterfeiting methods typically involve binding the product with an identifier of either an overt or covert nature. Examples of an overt identifier include physical identifiers such as watermarks and holographic labels. The process of confirming the authenticity of a typical physical overt identifier is shown in Table 3.

Table 3: Application of Overt Identifiers

Product Manufacturer	Product Distributor	Retailer	Consumer
Applies identifier to product or package and educates distributor, retailer and consumer about identifiers	Visual verification of overt identifier	Visual verification of overt identifier	Visual verification of overt identifier

A holographic image is used as a security device by incorporating it into a permanently affixed sticker or tag on the product or its packaging. The holographic tag generally will contain an image or brand logo altered using different effects. Types of effects applicable to holograms are: kinetic effects, which cause the image to appear to move or change color, depth effects, which cause the image to appear two or three dimensional, and multi-channel effects, which can increase the complexity of the holographic image. Holographic labels can contain a single effect or a combination of several effects.

A simple holographic label is verifiable by the naked eye. This type of verification is generally done at each stage of the products supply chain, all the way to the consumer. Simple

holographic security can be vulnerable to counterfeiting because the consumer and retailer are very unlikely to verify the hologram. Research estimates only about 1% of consumers, and 10% of retailers verify a hologram. [5] This issue can be mitigated if members of the supply chain, including the consumer, are educated about how the hologram is supposed to look and the common forms forgeries take on. A slightly more advanced hologram will use a simple decoder, often inexpensive, that when used, will alter the appearance of the hologram. This type of security is typically only applicable to the supplier level of verification.

When first implemented, holographic tags were very difficult to reproduce and required significant investment on the counterfeiter's part. Now however, holographic counterfeiting is much cheaper for counterfeiters to accomplish, and consumers pay little attention to holograms because they have become quite common. Holographs in their current form offer minimal protection of brand integrity, and can often give a false sense of security to the brand owner.

Physical identifiers are a very basic form of anti-counterfeiting protection, and are subsequently quite vulnerable to being cloned. When a physical identifier is cloned, it can be applied to counterfeit products and the counterfeits can become difficult to distinguish from the legitimate product. This has led to the introduction of covert digital identifiers. The predominant form of covert identifier is Radio Frequency Identification (RFID). The process of verification for RFID, and similar covert digital identifiers is shown in Table 4.

Table 4: Application of RFID for Covert Identification

Network	Manufacturer	Distributor	Retailer
All Verifications Go Through Network Setup	Applies Covert Identifier to Product or Package	Checks Covert Identifier with Network to Confirm Item Identity	Decodes Covert Identifier for High Value Goods
Contains all Encode and Decode Data	Registers Encoded Data from Covert Identifier Into Network		Decoding Typically Not Done for Inexpensive Goods

Radio frequency identification (RFID) is a term that encompasses a broad category of technology that uses radio waves to identify an object. The most commonly used type of RFID in anti-counterfeiting operates simply by encoded a serial number onto a microchip, attaching the microchip to a radio antenna, and then inserting the microchip and antenna, referred to as a tag, into a product or its packaging. There are two main types of RFID tags, passive and active. Passive tags don't have an independent power source; instead, passive tags get the necessary power to operate from electromagnetic waves transmitted by the tag reader. The electromagnetic waves induce a current in the antenna within the tag, providing it with short burst of power to

send a signal back to the RFID reader along the electromagnetic wave. The range a passive tag works within is only about 20 feet. Passive tags are also only capable of very limited computational tasks, which prevent them from containing cryptography and other complex security protocols. Active tags have an internal power source, which provides the power for the antenna and the microchip within the tag. This allows active tags to use cryptography and encryption and decryption algorithms. Passive tags are much cheaper and generally cost around $0.10, active tags can range from $3.00 to $10.00. [8] The infrastructure required for RFID is minimal. RFID tags need to be introduced into the product or package, and registered into a computer database. In the supply chain packages need to be checked using an RFID reader, however packages don't need to be opened and no visual contact is necessary to verify the items authenticity.

The future of anti-counterfeiting may include several different approaches including: random pattern tags, cryptography based authentication product labels, and optical variable devices. This is just a small sampling of an increasing field of research involved with anti-counterfeiting.

Random pattern tracking creates a random scatter pattern on either the product or its packaging. The product is then given a unique digital identifier which is encoded into the random pattern. The random pattern can be applied using a phosphorous ink, which when exposed to ultraviolet light will show the pattern. Phosphorous ink is an attractive choice because the product will not appear any different to the consumer. However using normal ink, a micro dot image could also be applied to the product. The visible pattern can be blended into existing features of the product, or can be applied externally to the packaging in the form of a permanently affixed label. Such patterns must be registered into a secure computer system at the manufacturing stage and then encoded with the digital identifier using computer algorithms. This registration can be done on the manufacturing floor by taking a digital photograph of the pattern with something as simple as a cell phone camera, recording the serial number and product info, and sending the information to a secure computer server within the manufacturing plant. To implement registration for large scale production, a camera could be mounted at the end of the manufacturing or packaging stage of production to record and transmit the information. As the item is then shipped and purchased, it can be verified by each stage of the process. Even the final consumer could take a photograph of the product or its packaging label (depending on where the random pattern is printed) and use a web-based service to verify the authenticity of the product. Random patterns cannot be used in cases where the packaging may be reused, as the random pattern is not removable from the package.

Cryptography based authentication incorporates a cryptographic number sequence within the product label. Authenticated Product Labels (APLs) are applied at the manufacturing stage inside the package, on the outside of each individual package, and on the wholesale group of packages. The inner APL contains a random prime number, an expiration date, and the manufacturing date. The outer APL contains a factor of the inner label numerical sequence. APL data must be stored by the manufacturer in a central database to use when counterfeiting

occurs. APLs need to be verified at each stage in the supply line. Verification can be done offline without calls to a central repository. Implementation of the system requires not only those involved in the shipping and selling of the product to confirm the APL, the consumer may also need to confirm the APL. The consumer confirms the APL by checking that the labels are properly signed, that the expiration and manufacturing dates are reasonable, and that the outer label is a numerical factor of the inner label's prime number. To implement this system, the manufacturer needs to create the complex cryptography algorithms to apply to their product labels. APLs are simple to implement on the manufacturing side, because only a small change to the label is required.

Optical variable devices (OVD) create a microstructure within a product, similar to an embossed surface. With the use of electron beam lithography, the microstructure applied to the product can be an easily recognizable image, a fast switching graphic effect, optical variable grayscale, or line art portraits. OVDs main use in counterfeiting is creating microstructures 1-30 microns in size that diffuse light and create an image. This type of OVD is incredibly difficult to counterfeit due to the complexity of the process and the investment in the equipment. OVD requires the implementation of the laser micrograph device at the manufacturer level of the supply chain. It is best suited for use with high end products, and is typically used in the printing of money. OVD does not require any verification by those along the supply chain, except the consumer. The consumer needs only to look for the microstructure on the product and confirm this item is authentic.

Table 5: Summary of Applications

Products/Categories	Covert	Overt	Random Pattern Tracking	Cryptography	Optical Variable Devices
Consumer Products					
Watches	X	X	X		
Electronics Product/Appliance	X	X	X	X	
Clothing	X	X	X		
Perfume	X	X	X	X	
Batteries	X	X	X		
Pharmaceuticals	X	X	X	X	
Food Items		X			
DVDs	X	X			
Industrial Products					
Auto Parts	X				X
Electronic Component	X	X	X	X	X
Tools	X	X	X	X	X
Aerospace Components	X			X	X

Opportunities:

Table 6 has listed possible approaches to blend anti-counterfeiting technologies into common courses in engineering technology and packaging science. The applied form of engineering done in engineering technology programs allows for several opportunities to expand coverage of these techniques. Generally courses in design, product development, materials, and manufacturing processes have opportunities for links. Courses in supply chain, packaging and logistics also have many opportunities to expand coverage and help students gain an overview of how companies can protect their products and supply chain.

Table 6: Possible Anti-Counterfeiting Technology in Current Courses

Course	Covert pattern tracking	Overt pattern tracking	Random pattern tracking	Cryptography	Optical variable devices (OVD)
Supply Chain Management	X	X	X	X	
Product Development & Integration	X	X	X	X	X
Materials Technology					X
Manufacturing Processes	X	X	X		X
Manufacturing Systems Design	X	X	X	X	X
Electronics Manufacturing	X	X	X	X	X
Packaging for End User	X	X	X	X	
Packaging for Distribution	X	X	X	X	
Flexible Containers	X	X	X	X	
Ridged Containers	X	X	X	X	

Conclusion:

This paper presents an introduction to countermeasures as well as the challenge currently presented by counterfeit goods. Factors growing the problem, risks to manufacturers and consumers, as well as legal enforcement related to counterfeiting are discussed.

Overviews of some anti-counterfeiting technologies are provided in the paper. Traditional technologies involve covert and overt verification processes using RFID tags, holographic and water mark images. These technologies require relatively low cost technology to produce the physical identifiers. These low entry barrier features however make it easy to counterfeit the identifiers, and in many cases, the product as a whole. In contrast, technologies such as cryptography based identification and random pattern image tracking require sophisticated technologies to produce the physical identifiers. These create a high entry barrier for counterfeiters and minimize the potential for problems, but in some cases can add significantly to production cost.

Anti-counterfeiting techniques and technology is an emerging area of research and teaching that presents an opportunity for engineering technology departments searching for new, challenging and relevant subject matter for applied research and teaching. Connections can also be made to management, distribution and logistics coursework and to specialty courses in packaging science and printing. The scale of the problem presented by counterfeit goods also indicates it will likely be a growing area of concern for companies hiring graduates from these programs. Anti-counterfeiting topics have been part of courses in the Packaging Science programs at the authors' university for quite some time; however these subjects have only recently been addressed in courses such as product development and production and operations management.

Several future applied research opportunities are apparent in this subject area. Integration of techniques into current product design efforts could yield benefits if a 'design for authentication' analysis was to become as commonplace as a 'design for manufacturing/assembly' assessment. Existing materials testing, metrology and lot sentencing techniques could be optimized to detect common frauds. And in the field of logistics and distribution supplier development/supply chain engineering techniques could be assessed in terms of their ability to mitigate the potential for counterfeit goods entering the supply chain. Cross disciplinary research efforts also seem to be possible as the subject covers many specialty areas. Counterfeit goods manufacturers are unlikely to go away anytime soon, so the subject of anti-counterfeiting technology will likely continue to be a subject of significant interest in the foreseeable future.

Bibliography:

1. “Knockoff: the Deadly trade in counterfeit goods,” Tim Phillips, Kogan Page, 2005

2. “Inside the Knockoff-Tennis Shoe Factory,” Nicholas Schmidle, New York Times, April 19, 2010

3. "Anti-counterfeiting with a Random Pattern," Chong, Cheun Ngen, Dan Jiang, Jiagang Zhang, and Long Guo. Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference, 2008

4. "Design and Implementation of PUF-Based 'Unclonable' RFID ICs for Anti-Counterfeiting and Security Applications." Devadas, S, E Suh, S Paral, R Sowell, T Ziola, and V Khandelwal. RFID, 2008 IEEE International Conference, 2008

5. "Optical Security and Counterfeit Deterrence Techniques V,” James, R., M. Long, and D. Newcomb. *Proc. of SPIE-IS&T Electronic Imaging* 5310, 2004

6. "Micro-Technology for Anti- Counterfeiting." Lee, R. A. Microelectronic Engineering 53, 2000

7. "Improving Supply Chain Robustness and Preventing Counterfeiting through Authenticated Product Labels." Pathak, Vivek. Technologies for Homeland Security (HST), 2010 IEEE International Conference, 2010

8. "Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting." Staake, Thorsten, Frédéric Thiesse, and Elgar Fleisch. ACM Symposium on Applied Computing, 2005