Journal of Food Protection, Vol. 68, No. 6, 2005, Pages 1314–1317
Copyright ©, International Association for Food Protection

Authentication, Antitamper, and Track-and-Trace Technology Options To Protect Foods

RICHARD B. JOTCHAM*

Technology Services, Axess Technologies, Ltd., Andover, Hampshire SP11 7HB, UK

MS 04-711: Received 24 September 2004/Accepted 2 March 2005

ABSTRACT

Many security technologies (Anonymous, Effective supply chain protection, 2002) have been developed to protect a wide range of products, documents, and individuals. The food industry has very specialized needs, and food products may be affected by criminal activities such as tampering, relabeling, unauthorized diversion, and counterfeiting. It is important to understand the attributes associated with security technologies so that the benefits may be weighed against the restrictions that arise when selecting appropriate solutions to protect the food supply chain. Security technology may be split into a number of categories: authentication, coding, tamper evidence, and tracking. Within each category the technology may be subdivided into overt, covert, and forensic features. No single technology provides an infallible solution to all problems, so the most enduring and effective solutions almost always comprise a combination of technologies that provide deterrence, aid detection, and assist with subsequent prosecution of perpetrators.

Downloaded from http://meridian.allenpress.com/jfp/article-pdf/68/6/1314/1676750/0362-028x-68_6_1314.pdf by guest on 19 January 2021

For as long as there have been branded products that command premium prices, criminals have attempted to make cheap facsimiles of these products to deceive the consumer. With the advent of readily available design software packages and the easy access to print and packaging techniques, it has become apparent to criminals that the counterfeiting or relabeling of goods such as drugs *(2)* and food is easier and more lucrative than copying bank notes.

Persons with malicious intent can relatively easily penetrate the food supply chain and contaminate an ingredient or process, causing serious and widespread damage. Foodstuffs also can be stolen or illegally reclaimed, and labeling can be replaced before the product is reinserted into the legitimate supply chain. The proceeds from this type of activity can be used to fund other insidious activities, such as the purchase of weapons.

The security document industry has been applying technologies to combat illegal copying and tampering for over 200 years. Many of these techniques form the basis of features that can be used to authenticate and track products. The requirements for each industry and application differ, and all options should be analyzed before determining which security technology would be appropriate in a particular situation.

AUTHENTICATION, CODING, TAMPER EVIDENCE, AND TRACKING CATEGORIES

Security technologies can be categorized into four main sections: authentication, coding, tamper evidence, and tracking. There are many instances where these categories overlap, and it is often difficult to recognize which is the primary or most important category.

Authentication. Authentication may be separated into three specific categories. Overt security features are apparent and visible and do not require additional readers or instruments to detect them. The general public or untrained personnel can often verify them.

Covert features are concealed and may require a relatively simple reader or verifier (such as a UV lamp or magnifier) to locate and identify them. Covert tagging is particularly useful to customs inspectors and company investigators as long as these individuals are kept fully informed of what they should be looking for and are trained to use the readers and testing kits.

Forensic features are extremely covert and are often present only on a need-to-know basis. They may comprise the addition of unique taggant material or imperceptible changes to a substrate or print whose detection requires a very specialized reader. Alternatively, a testing process may involve the identification of a component or naturally occurring material within the product, thereby ensuring the presence and concentration of this material. The quantity of taggant may be so small that it cannot be detected using available analytical techniques, and detection may require a specific test method.

One of the main benefits of forensic tagging is that it can provide unequivocal evidence that a seized product is or is not genuine. This information can be very valuable in the prosecution of counterfeiting cases in which the counterfeit products and packaging are very similar to those of the genuine article.

Authentication features may be combined with a wide range of substrates, carriers, and application processes, which can include direct application into packaging, films, metals, or glass as an integral part of the material or may involve addition to a material such as foil, adhesive, or ink that is subsequently applied to the substrate.

* Author for correspondence. Tel: +44 (0) 1264 369005; Fax: +44 (0) 1264 366750; E-mail: rjotcham@axesstechnologies.com.

Examples of overt authentication features include the following.

(i) Optically variable coatings or inks can change color when the viewing angle is changed, e.g., a metallic coating that is magenta when viewed perpendicularly but looks green when viewed from an angle.

(ii) Holographic foils with complex image changes that become apparent when the viewing angle alters may be attached directly to packaging or applied to labels and tamper-evident seals.

(iii) Tear tapes are embedded into overwrap to facilitate removal of the overwrap. These tapes can contain printed, colored, or optically variable effects.

(iv) Thermochromic inks and coatings that decolorize on warming may be printed over images or script that appear when the ink is warmed by rubbing with a finger.

(v) Perforations are used to ease the tearing of paper or packaging. The perforation shape and size can be unique.

(vi) Embossing may be applied to packaging or paper to provide a tactile feature that may also include numbers, letters, or indicia.

(vii) Watermarks are used extensively in document security to provide anticounterfeit protection for certificates and labels.

Covert authentication features are particularly useful to company inspectors and enforcement agencies. They represent the second line of defense against counterfeiters and are often ignored by the criminals, who may not realize they are present or may find them too difficult to reproduce. Examples of covert authentication features include the following.

(i) Microscopic particles of specific colors or colored layers can be viewed using a magnifier or pocket microscope and are dispersed throughout the product or packaging. An edible version has been developed for food applications. The coding on the particle may differ among batches of product or packaging.

(ii) Tiny planchettes or narrow threads can contain microtext that is only visible using a magnifier or pocket microscope and may be employed as a tear tape.

(iii) Labels can be printed with color combinations or line structures that will not resolve on a normal scanner or color copier. Either the range of colors cannot be reproduced accurately by copying or the line structure causes a hidden image to appear in the copy.

(iv) Holograms can contain microtext that is only readable under magnification. The hologram may display an effective three-dimensional image when viewed normally, but magnification reveals that the macroimage is composed of letters, numbers, or indicia.

(v) Inclusions or print can contain materials with characteristic spectroscopic properties, such as inks that emit light in the visible region when illuminated by UV light. Products that are excited by infrared light and emit in the visible spectrum are known as upconvertors.

Forensic authentication may involve the chemical identification of a particular component within the product, such as an active ingredient, a specific sugar structure, or a particular binder or excipient. Alternatively, a taggant may be added during the manufacturing of the product or packaging. Examples of forensic authentication features include the following.

(i) Paper and packaging can contain very small amounts (parts per million) of a taggant that is undetectable by conventional analysis but may be extracted and identified using a dedicated test procedure. The taggant may be any chemical that is harmless but never naturally associated with the product it is protecting.

(ii) The isotopic composition of naturally occurring materials can be identified, providing information about the authenticity and source of the material. For example, a foodstuff grown in one part of the world may have a different isotopic composition that the same foodstuff grown elsewhere, thereby giving a clue as to the origin of the product.

(iii) Infrared analysis has been used to authenticate pharmaceuticals. Results for a test sample are compared with a library of spectra held in a database.

(iv) Elemental analysis can be conducted using X-ray fluorescence, which can be detected quickly and accurately using hand-held equipment. Therefore, X-ray fluorescence can be used as a rapid verification tool for complex products and packaging that may be seeded with unique elementals.

(v) DNA fragments can be added to products and packaging. For example, half of a strand of DNA is embedded in an ink or substrate, and the other half is contained within an authentication solution. When the two components are brought together, an authenticator is used to verify that the strands match.

Coding. Coding is defined as the ability to apply numbers, letters, or indicia in a structured format that can be deciphered to produce variable information. Bar codes on products have been used successfully to identify and track products. A number of agreed standards have been developed that allow universal use of bar codes across the manufacturing and retail spectrum. However, these codes have three major limitations.

(i) Numeric or linear bar codes hold a relatively small amount of data. This limitation has been partially addressed by the introduction of two-dimensional bar codes. However, these codes require readers different from those used for linear barcodes, and the cost of converting from linear to two-dimensional codes can be somewhat prohibitive.

(ii) The information is fixed, and no further data can be added.

(iii) The coding systems normally are black ink structures. Thus, they are easily reproduced by counterfeiters or alternatively located and removed by diverters.

The development of low-cost laser systems that can operate at production line speeds and write variable data has resulted in the permanent encoding of containers and packaging with lot numbers and sell-by dates. These laser systems may now be installed alongside ink jet printers and

Downloaded from http://meridian.allenpress.com/jfp/article-pdf/68/6/1314/1676750/0362-028x-68_6_1314.pdf by guest on 19 January 2021

provide a way of foiling criminals who remove and replace ink-jet printed information or labels.

Variable data may be accounted for by providing each product with a unique bar code that is contained within a database. This bar code acts as a license plate and permits read-write-erase capability for the information stored on the database.

Identity or recognition information may be embedded directly into a design during the printing process. For example, when an image is scanned or viewed using a digital camera, the image is resolved into its components. A number of digital watermarking companies have devised a technique whereby these components are changed in a controlled manner. The applied alteration has a negligible effect on the final image but allows subsequent scanning (using the correct software) to identify the change and associate this change with a particular product or batch. Because the verification process is digital, it can be combined with additional actions such as the automatic activation of a specific website or the opening of a computer file or spreadsheet. Because digital watermarking is embedded directly into the design on the packaging, it requires no materials or space on the packaging, making it particularly attractive for high-volume low-cost applications.

Tamper evidence. Food products make use of a variety of tamper evidence technologies to resist the fraudulent alteration of product codes and sell-by dates and the malicious addition of noxious products for political reasons. Here, I address only systems of tamper evidence that complement the methods for authentication and tracking. Examples of tamper evident security include the following.

(i) Caps and closures for bottles or other containers can contain tear strips that must be broken the first time the product is opened, e.g., shrink sleeves over bottle tops.

(ii) Seals can be fit to the inside of the closure of a bottle or other container that will be broken the first time the product is used. These seals can contain a full range of overt, covert, and forensic security features.

(iii) Labels can be applied over a bottle closure (e.g., Banderol) or the closure of a carton so that they must be broken when the package is opened.

(iv) Film labels can be made so that they distort if an attempt is made to fraudulently remove them. The distortion results in display of a message (such as ‘‘VOID’’) that cannot be removed by replacing the label.

(v) Tear tapes used to open outer packaging can contain authentication features and will be distorted or irreparably damaged when the packaging is removed.

Tracking. Tracking is defined as the addition of a feature to the product or packaging that provides information about the origin of the product, its manufacture, or its authorized destination. It is difficult to differentiate between the security value of a device that allows authentication of a food product or packaging and that of a device that provides information about its source or destination. Control of the supply chain is of paramount importance to deter unauthorized reintroduction of food products and a rapid and efficient response to recalls.

Combinations of authentication and tracking features. Tracking is most commonly done through variable data such as ink-jet codes or bar codes applied directly to the packaging. To identify the removal of data and reprinting of codes, the inks may contain security taggants such as spectroscopic features or chemical characteristics that can be verified using specialized equipment or techniques.

Batch tracking may be carried out using one or more of the authentication features described above. If covert tracking is required, then a combination of variable data printing and a covert security feature such as UV ink may be employed.

Batch tracking will allow information about manufacturing sites, countries of destination, or manufacturing times to be easily recorded. When individualized data are required, item numbering or coding will be necessary.

Serial numbers are useful because they allow users without specific readers to identify individual items; however, for data management it is necessary to utilize a machine-readable feature that can process data at speed.

The linear bar code is the most universal machine-readable data carrier. If the amount of data stored is relatively large, then a linear bar code will not be sufficient. A two-dimensional bar code can contain approximately five times the amount of information in the same amount of space.

All numeric codes and bar codes are read individually and require that the reader be in the same line of sight as the code. Thus, multiple packs of products cannot be read without unwrapping, and large or unwieldy items can be difficult to process. The need to read and verify information remotely (non–line of sight) and simultaneously collect data has spurred the development of electronic tagging.

Electronic tracking. Radio frequency identification (RFID) was initially introduced as an asset recognition system and has been developed into smart labels on which data can be electronically written to and read from using a remote transponder. These smart labels contain an integrated circuit (chip) and may be either passive (no power source) or active and include an integral battery. Reading protocols allow very rapid sequential reading of tags, in effect providing simultaneous reading of multiple tags.

The high cost of RFID tags has resulted in the development of a number of lower cost chipless electronic tags that provide short-range remote sensing capability and batch or low-level unique coding. Examples of chipless tags include magnetic and electromagnetic materials in the form of fibers, threads, or patches that may be embedded directly into packaging or closures during manufacture. Most of these tags are designed to be read at short distances (less than 1 mm), although some will still be readable up to 1 m away.

The Auto ID Center at the Massachusetts Institute of Technology (now known as EPC Global) has proposed a specification for a unique electronic coding system called ePC (electronic product code). This system is based on an electronic tag with a minimum data capacity of 80 bits that

Downloaded from http://meridian.allenpress.com/jfp/article-pdf/68/6/1314/1676750/0362-028x-68_6_1314.pdf by guest on 19 January 2021

can be read remotely and contains a code that is allocated when the associated product is manufactured. This code stays with the product throughout its life cycle.

EPC Global has not specified a particular supplier of tags, stating that the system is open to any company whose tag meets their technical specification. The introduction of RFID tags for cases and pallets has been championed by Wal-Mart (Bentonville, Ark.) and the U.S. Department of Defense. They are demanding that their top 100 suppliers fix ePC-type electronic tags to all cases and pallets during 2005.

SECURITY FEATURE SYNERGIES

Food products are often low-margin high-volume products with fixed or relatively short shelf lives. Because of these attributes, manufacturers must be creative in how security technologies are included into products and packaging.

Example 1: reconciliation of packaging. In October 2003, the German government introduced a standardized deposit system for recycling beverage containers that involved the printing of a security code or mark onto 16 billion glass bottles, cans, and PET (polyethylene therephthalate) containers. The code or mark will be read and cancelled by hand-held readers or by redemption machines outside stores. The color of the ink used to print the code is irreversibly changed once the container redemption has been paid, preventing multiple submissions.

The security ink used in this application is not available to the general public and therefore provides a means by which the packaging can be authenticated without the application of additional security features.

Example 2: retail theft prevention. Retail shops currently employ electronic article surveillance (EAS) systems to prevent theft of portable high-cost goods such as cosmetics and electrical and entertainment products. Use of these tags has not been embraced by the food industry because of the substantial additional packaging costs. However, the food industry needs to operate a very efficient supply chain management system and must maintain effective recall procedures.

The recent developments in low-cost electronic tagging systems could be justified in terms of their supply chain efficiency benefits. Many of these tags also can be used as EAS detectors, thereby providing additional security without added costs.

Example 3: multifeature systems. When considering a tamper-resistant label or closure, it is sensible to include authentication protection for the label. Entry into the package results in breakage or distortion of the feature. A person attempting to tamper with the product would be compelled to remove all of the label and replace it with a copy. Authentication protection would allow detection of and thus deter this activity. Although the label is attached to the secondary packaging, it acts as an authentication feature for the whole product.

SUMMARY

Food product counterfeiting and tampering are becoming increasingly attractive to either terrorists wishing to create mayhem or criminals compromising valuable brands names to fraudulently obtain money. There are many different security technologies available to the food industry to prevent terrorist and criminal activities. Many of these technologies were originally developed for the security document industry to protect sophisticated products such as bank notes or passports. Although the criminals targeting these products may now have moved their attention to branded products such as foods, the packaging, processing, and cost restraints associated with food products mean that some technologies will be inappropriate or unsuitable. Brand owners wishing to protect their products must first analyze their specific needs and constraints before trying to adopt a security solution that may not be relevant.

REFERENCES

1. Anonymous. 2002. Effective supply chain protection. IDTechEx, Ltd., and Axess Technologies, Ltd., Andover, UK.
2. Le Parc, M. 2003. Protecting medicines and pharmaceuticals. A manual of anticounterfeiting solutions. Reconnaissance International, Shepperton, UK.

Downloaded from http://meridian.allenpress.com/jfp/article-pdf/68/6/1314/1676750/0362-028x-68_6_1314.pdf by guest on 19 January 2021