Applications of MICA Freeform to Anticounterfeiting

Adam L. Cohen
Principal Consultant and CEO, Additive Insight LLC
Clinical Associate Professor, Southern Methodist University

The Problem

Product counterfeiting is a crime of vast proportions, directly causing loss of revenues to companies, damage to brands, and even loss of life. Moreover, it provides funding to organized criminal and terrorist groups[1]. According to the International Anti-Counterfeiting Coalition (IACC), there was an estimated $250 billion in cross-border trade in counterfeit and pirated physical goods in 2009. The IACC projects that in 2015, the global trade in such goods will be $1.77 trillion. The Alliance for Gray Market and Counterfeit Abatement estimates that nearly 10 percent of technological products sold in the global market today are counterfeit.

A broad variety of products are regularly counterfeited. Consumer products such as luggage, apparel, wallets, consumer electronics, computers, toys, sunglasses, watches and other jewelry, software, and cosmetics and fragrances are common items. While most such products create only financial damage, many fake products seriously threaten health and safety, such as counterfeit parts for automobiles and aircraft, counterfeit electronic components and electrical equipment, and counterfeit pharmaceuticals, medical devices, food, and beverages.

Current Solutions

Many technologies have been developed to reduce counterfeiting, enabling products to be authenticated by end-users and others in the supply chain. In some cases, these solutions—in conjunction with a database—also allow the movement of individual products to be traced all the way from manufacturer to final destination. Methods and devices for successful anticounterfeiting must meet certain requirements. They must be connected to the product in a way that precludes tampering (e.g., integrated into the product's material, bonded to a surface, or incorporated into product packaging). They must allow authentication of the product, preferably easily, quickly, and with very few false negatives or positives. They must be difficult—ideally impossible—for a counterfeiter to manufacture itself or copy. In some cases they should be covert (with the indication of authenticity hidden, requiring a destructive evaluation or specialized equipment). They must be robust, remain functional and attached to the product long enough to allow final authentication. If fastened to a product or its packaging, attachment should be easy, but intact removal (and re-attachment to a counterfeit product) impossible. Versatility is desirable: it should work when incorporated into a wide range of products, and compact to work with smaller products. If individual traceability of a product is needed, it should support a unique code which can read reliably and not be easily copied. In the case of devices applied directly to products, it should not detract from product appearance or functionality, or be easily removed by the end-user. Finally, to be readily adopted, anticounterfeiting solutions—including any required equipment—should be affordable.

Current anticounterfeiting devices may be categorized according to the technology employed. One major category comprises devices based on optics. For example, there are methods in use for printing checks and passports which render them more difficult to counterfeit. These include watermarks; special inks and dyes (e.g. pearlescent inks, color-changing inks, magnetic ink, thermochromatic ink, fluorescent dyes);

special papers (e.g., papers with security backgrounds, copy-evident patterns, and special threads or planchettes); high-resolution features (e.g., microtext, lathe work); and specialized printing processes (e.g., intaglio, alignment of features on both sides). Other optical techniques include holograms like those attached to credit cards, and optically variable devices such as inks which display moving or color-changing images; nanoscale holes which produce interference colors; lenticular elements; retroreflective elements which display an image with special lighting; patterns producing moiré effects; peel-off films; up-converting phosphors which glow under infrared light; diffractive optical elements; color-shifting inks, photonic inks, and use of X-Ray fluorescent materials in threads.

Electronic methods are also in use, the most common of which is radio-frequency identification (RFID). RFID tags have dropped in cost and can be incorporated into many products; moreover, they can provide traceability of products in addition to authentication. Another electronic method involves measuring the electromagnetic emissions of integrated circuits, yielding a "fingerprint" of the device[2]. ICs can be analyzed using techniques that rely on physical unclonable functions based on variations in manufacturing and unique to a particular device. Chemical methods of authentication include nano-particles, inks containing taggant compounds, and markers based on unique DNA sequences. Specialized and sometimes proprietary spectrophotometric or other equipment is normally required for readout. The final category encompasses anticounterfeiting solutions relying on microscale features. These include incorporating microtaggants with tiny barcodes, and measuring surface textures—e.g., on a molded part—to provide authentication.

Assessment of Current Solutions

Many optical anticounterfeiting solutions are easy to authenticate with the naked eye or a low-power magnifier. They can also be inexpensive and can be applied to a variety of surfaces. However, too often they are also within the capabilities of counterfeiters. Many holograms fall into this category as they are readily copied or re-mastered. So do watermarks, various inks, and some optically variable devices. Moreover, optical approaches are sometimes too large to be attached to a product or would mar its appearance, are not covert or sufficiently robust, or don't support item-level serialization for traceability.

The dominant electronic anticounterfeiting solution is RFID. RFID is non-contact and doesn't require line-of-site reading, allows item-level tracking, and can be built into certain products for covert use. But RFID tags can be costly, may be too large, may be unsuitable for metal substrates, may be susceptible to copying or eavesdropping[3], and usually cannot tolerate high temperatures or radiation. Chemical anticounterfeiting solutions offer covert, reliable authentication and tracking, and the ability to work with liquids and very small products. They are also tough for counterfeiters to duplicate. However, they normally need costly equipment and trained personnel for assessment, lending themselves more to forensic than casual use. Item-level serialization is not normally an option, and reliable, robust integration with the product may be challenging. Microtaggants offer covert authentication using inexpensive equipment (e.g., a microscope) yet are small enough to be added to many products and are not easily reproduced. However, suitable means of attachment to, or incorporation into, a product is not always available. Surface texture-related approaches involve no additional per-product costs and are robust and covert, but are limited to products manufactured using specific processes such as injection molding. In summary, given the number of products now counterfeited and the fact that no existing solution is a

panacea, there is a need for additional approaches that complement current ones and offer new possibilities.

MICA Freeform

MICA Freeform is a unique mass production additive manufacturing (AM, a.k.a 3-D printing) technology for microscale metal parts. As with other AM processes, parts are produced one layer at a time from 3-D CAD designs, and complex geometries can be produced, including undercut and internal features. MICA Freeform also borrows from semiconductor manufacturing, benefiting from high resolution and repeatability, and wafer scale production in a cleanroom. The process for making a part with MICA Freeform involves three key steps per layer. First, a structural metal is electrodeposited onto a substrate in selected regions corresponding to a cross section of the part. Then, a sacrificial metal is electrodeposited over the structural metal. Finally, both metals are planarized to yield a layer that is flat, planar, and of precise thickness. After all layers are formed, a chemical bath is used to dissolve ("release") the sacrificial metal, yielding a batch of parts that are ready-to-use without further processing.

As a manufacturing technology, MICA Freeform has some intrinsic benefits overall such as:

- Very small features (e.g., 20 µm within a layer, 5 µm vertically) and tight tolerances (e.g., +/- 2 µm)
- Very smooth surfaces (e.g., < 0.8 µinch R_a)
- Well-defined, sharp edges; nearly-vertical sidewalls

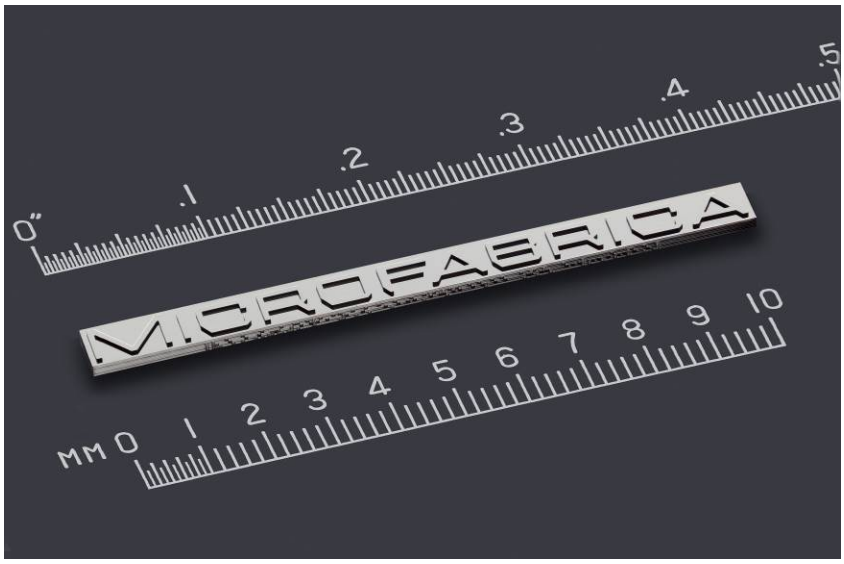

Fig. 1. Complex, microscale metal logo made with MICA Freeform.

Potential Benefits of MICA Freeform in Anticounterfeiting

MICA Freeform makes possible complex, miniature 3-D metal microscale parts such as the miniature logo shown in Fig. 1, as well as far more intricate devices incorporating multiple, independent moving parts which are built in a single process, without needing assembly. The process is unique and extremely difficult to replicate both in terms of its overall capabilities—intricate microscale metal parts typically

made from dozens of layers—and in its specific performance. In enabling unique devices for product authentication or tracking/tracing, MICA Freeform offers several potential benefits:

- Devices can in many cases be quickly authenticated by with low-cost equipment such as a loupe or microscope. Minimal training is required, and authentication by consumers is feasible.
- Devices can easily be integrated with a wide range of products (e.g., by insert molding, adhesives, brazing, etc.). Once affixed, devices can be designed (e.g., with elements which break, or which deform and become misaligned) so that they cannot be removed intact and transferred to another product.
- Devices can be very small, allowing them to be incorporated into smaller products unobtrusively. For example, an anticounterfeiting device can easily be embedded in the temples of luxury sunglasses, or a piece of jewelry.
- Additional levels of security can be incorporated using micro barcode features or serial numbers.
- Devices are made from metal. Depending on the design, they can therefore be very robust, especially before release. Devices can also withstand high temperatures or intense radiation if required.
- When compared with security printing, holograms, and so on, MICA Freeform devices are harder to duplicate, often smaller, and potentially more covert.
- Devices can have an aesthetic, high-tech appearance that adds value to the product, or emphasizes product branding. For example, the complex 3-D logo shown in Fig. 2 (left and center) both provides a hard-to-duplicate metal mesh that authenticates the product, and a jewel-like logo.
- Devices can serve not just anticounterfeiting roles, but also add functionality to products, as illustrated by the unique, dynamic watch minute hand shown in Fig. 2 (right). Such a hand, which changes in length as it rotates, may be appealing for watches with non-circular dials.
- Devices can include moving elements, allowing them to behave in pre-programmed ways when stimulated. For example, rotating or shaking a device or pressing on flexible elements can produce motions observable on the surface. Since devices can incorporate magnetic materials, manipulations using external fields are possible.

As a means of making anticounterfeiting devices, MICA Freeform also has its share of challenges. The process is limited to part heights of ~1 mm, and cost increases with device footprint and layer count.

Fig. 2. Rendering of an anticounterfeiting device in the shape of a Parmigiani-Fleurier logo (left); composite photo of the device bonded beneath the watch crystal (middle); rendering of a variable-length watch hand (right).

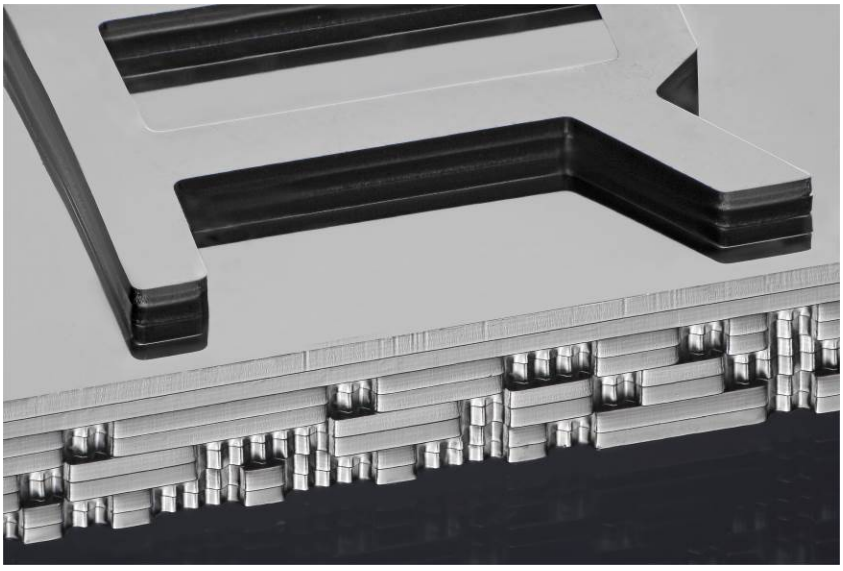

Fig. 3. Barcodes on the vertical sides of the device shown in Fig. 1.

Anticounterfeiting Devices produced by MICA Freeform

The presence of a MICA Freeform-produced anticounterfeiting device on a product or package can itself serve to authenticate it. However, by leveraging MICA Freeform's unique capabilities, additional levels of security and/or traceability can be produced. Some examples of these are:

Novel barcodes. Devices can encode information such as unique and encrypted serial numbers that are designed in, allowing product tracking and tracing. Codes can be located on horizontal surfaces or, as in Fig. 3, vertical surfaces. 1-D and 2-D codes can be included, but by exploiting the 3-D capabilities of MICA Freeform, 3-D barcodes can also be made. For example, the 2 x 2 mm 3-D barcode shown in Fig. 4 comprises a 4 by 4 array of columns whose individual heights can vary in 30-µm increments from 0 to 150 µm. The number of possible codes that can be represented is 6^{16} (i.e., 2,821,109,907,456, or over 2.8 trillion). Since it is possible to incorporate many more than 16 columns (i.e., 225 columns in a low-cost 1x1 mm code built using three layers would yield ~3 x 10^{135} combinations, more than provided by the 448 bits of a typical RFID tag), the availability of unique codes is virtually endless. Barcodes need not have the simple shape shown, but can be integrated into product logos, etc.

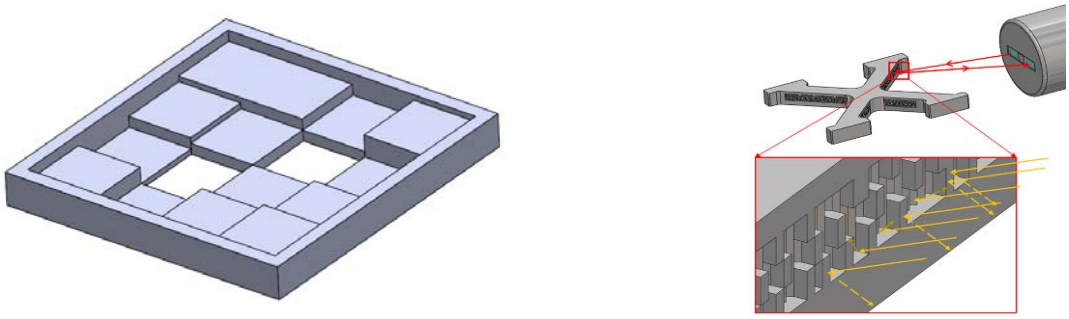

Fig. 4. CAD model of a representative 3-D barcode enabled by MICA Freeform (left);

reading a micro 2-D barcode on the side of a device (right).

1-D and 2-D barcodes can be read using standard techniques that are scaled down, such as cameras (Fig. 4 (right)). 3-D barcodes can be read using photometric stereo methods, miniature 3-D scanners, Gelsight contact imaging[4], etc. By incorporating undercuts, removable caps, etc., replication of 3-D barcodes can be thwarted. MICA Freeform barcodes are very small and inconspicuous, can be read using low-cost equipment, can easily be used on metallic products, and can survive very high temperatures and radiation. However, they require close proximity for reading and cannot normally be embedded within a product. While they can't be updated with new data, many codes are available so more barcodes can be added to record the product's progress as it moves through the supply chain. Barcodes produced using MICA Freeform can be an excellent solution for consumer products such as sunglasses, jewelry (including watches), and mobile electronics; medical devices; and automotive and aerospace parts for harsh environments.

Other optical devices. Optical anticounterfeiting devices relying on geometric optics can be made with MICA Freeform..

Backlit devices. Precision 3-D structures can be backlit so that the edges of words, logos, and other shapes are precisely illuminated. Fig. 5 depicts a 3D Systems logo in which the top part of the logo is suspended by built-in, hidden supports above a solid surface having apertures matching the letters. The amount of overlap between the letters and the surface can be controlled to a few microns. When illuminated from the rear (e.g., using a smartphone), light enters the apertures, reflects from the rear of the letters, and further reflects off the front of the surface, producing a distinct, well-defined outline or halo effect. This is seen in Fig. 5 (bottom), which shows the 3D Systems logo with a glow around the characters "3D".

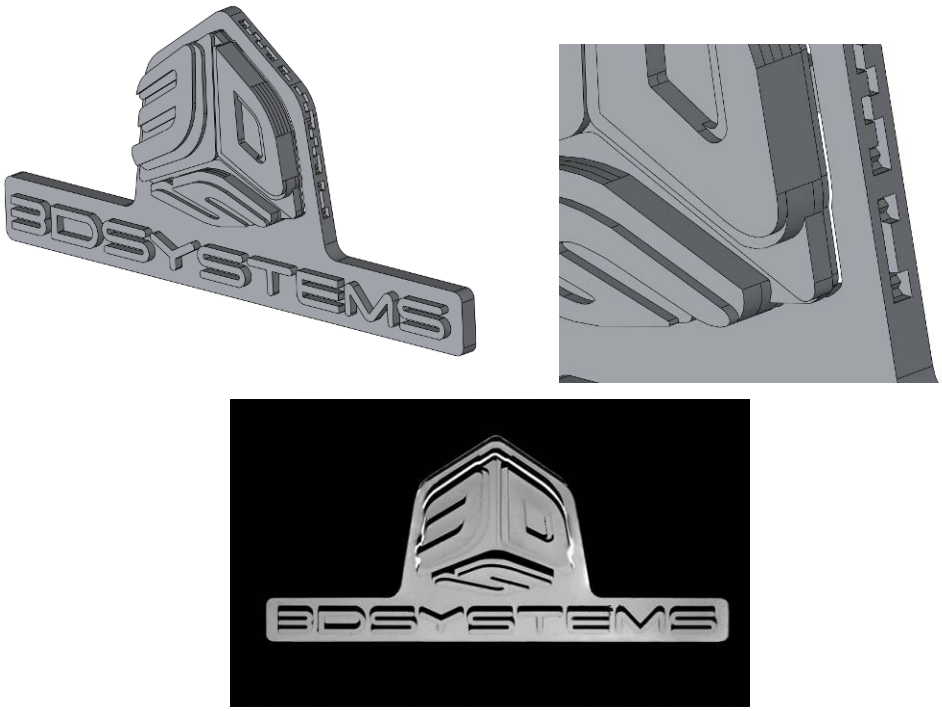

Fig. 5. CAD model of backlit 3D Systems logo structure (top left); close-up view of gap between logo edge and back surface (top right); photograph of the logo with backlighting.

Angle-sensitive devices. Microscale structures which can only be viewed correctly from specific angles can be made. Fig. 6 (left and center) depicts such a structure representing the letter "I". Crossed-grating, eggcrate-like structures with elements converging to a single focus can be fabricated. A small light source located nearby will be visible only if placed at the predetermined focus.

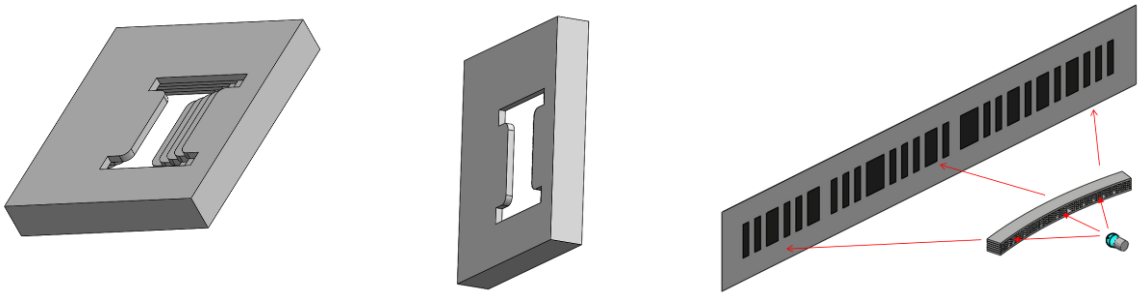

Fig. 6. CAD model of angle-sensitive 3-D device viewed at an arbitrary angle (left); viewed correctly, showing a clean letter "I" (center); concept for projection of a microscale barcode pattern onto a large surface (right).

Projection devices. Structures such as that shown in Fig. 6 (right) can be built with MICA Freeform. When illuminated as shown, a pattern, such as the 1-D barcode shown, is projected onto a viewing surface in an enlarged form. Alternatively, an array of initially co-planar mirrors can be fabricated with each held in place by a deformable support. The array can then be "programmed" so certain mirrors are tilted to project a unique image when illuminated. *Light guide devices*. Devices which transmit light by internal reflection can be built, allowing light to be introduced at one point and observed elsewhere. For example, the X-shaped structure of Fig. 7 (left), has internally-reflective channels which propagate light shone in the central hole to the corners shown in Fig. 7 (right).

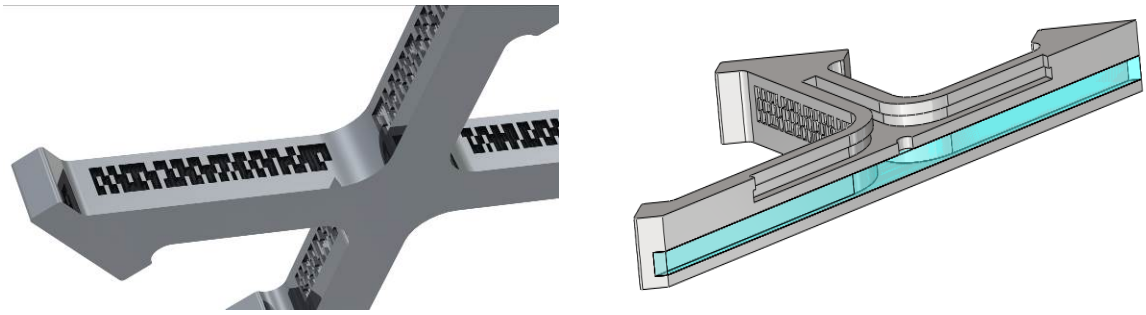

Fig. 7. CAD image of anticounterfeiting device (left); Sectional view of device showing Internal light guide (right)

Micromechanical devices. MICA Freeform's ability to build create internal features can be leveraged to provide unique authentication capabilities. *Micro-locks*. A covert device can be made using a ball which rolls through a block with internal passages and a set of windows allowing it to be observed. If the device is genuine, the ball appears in particular windows in a particular sequence. Another device uses external stimulation (e.g., gravity, acceleration, rotation, magnetic fields). The proper type and sequence of manipulations (e.g., tilting, spinning, shaking, striking)—known to authorized personnel—"unlocks" the device, triggering a visible flag. *Fluidic devices*. Devices are possible having internal channels through which liquid can wick or flow under pressure. For example, a colored liquid introduced into a port can wick until visible in one or more windows (e.g., forming a logo or the word "authentic"). Alternatively,

liquid can cause displacement (e.g., through surface tension) of a moveable flag. *Break-apart devices*. Covert and tamper-evident authentication devices can be built, similar to "scratch-off" paint and labels. Or, boxes with barcodes can be built with lids which must be removed to access the interior. Structures can be built which fall apart in a way impossible to reconstruct if tampered with. For example, small loose blocks can be trapped inside a structure in specific, coded locations. Orientating the device at a particular angle or using a magnet can move these elements to reveal their locations. But if the device is pried open, the elements fall out and the code cannot be determined.

Conclusions

The proliferation of fake products is a massive problem that is best mitigated both by increased adoption of current anticounterfeiting solutions and the development of new technologies that allow manufacturers, their authorized supply chains, and end-users to stay one step ahead of increasingly-capable criminals. MICA Freeform, Microfabrica's microscale metal AM technology, is capable of mass producing novel anticounterfeiting devices previously impossible to make. These devices are compact, robust, and easily and cheaply authenticated. They can be integrated with a wide variety of products, and can be either overt or covert. As an added benefit to certain products, they can enhance product aesthetics and functionality.

References

1. "The Negative Consequences of International Intellectual Property Theft: Economic Harm, Threats to the Public Health and Safety, and Links to Organized Crime and Terrorist Organizations", International AntiCounterfeiting Coalition, January 2005. http://cdm16064.contentdm.oclc.org/cdm/ref/collection/p266901coll4/id/3379

2. Huang et al., "The detection of counterfeit integrated circuit by the use of electromagnetic fingerprint". EMC Europe 2014, Sep 2014, Gothenburg, Sweden. pp. 1-5.

3. "Attachment E: RFID Security and Privacy White Paper", Smart Border Alliance RFID Feasibility Study Final Report. https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf

4. Johnson et al., "Microgeometry Capture using an Elastomeric Sensor". http://www.mit.edu/~kimo/publications/microgeometry/microgeometry.pdf