

Overt Security Features Through Digital Printing

Mark-Hampden-Smith, Scott Haubrich, Ralph Kornbrekke, Jainisha Shah, Rimple Bhatia, Ned Hardman and Rich Einhorn Cabot Corporation- Albuquerque, New Mexico 87113 USA

ABSTRACT

Digital printing technology represents a counterfeiting threat and a counterfeiting deterrence opportunity. Digital reproduction methods have been used to produce holographic and printed features similar to those on banknotes. As digital technology continues to improve, the quality of those features will become nearly indistinguishable from intaglio printing, offset printing and holograms. Optically active devices and inks have been useful to slow counterfeiters, but security document and feature designers need more tools. The toolbox for digital technologies is very large and being exploited by the counterfeiters, but their toolbox has been limited to commercially available digital technologies. Security designers also need to take advantage of this toolbox with the additional lever of secure materials. By leveraging digital technologies with secure materials, variable information and integration with other security features, security document designers can create new, attractive features that are hard to replicate. The high level of difficulty to create security materials in the sub-micron to nanometer size range with multiple functionalities is one barrier. Creating inks that are formulated to fit the stringent requirements for custom digital printing methods creates another barrier to unauthorized reproduction. All of the other valuable aspects of digital technology are therefore accessible only to those with access to these secure materials. Leveraging these digital materials to make optical effects make them useful for the end-user authentication. Furthermore, use of digital technologies allows the incorporation of variable data that can be authenticated visually or using proprietary algorithms and detection / sorting equipment.

Keywords: overt, digital printing, metallic, reflectance

Current Overt Security Features

Overt security features are those features that can be authenticated by the public with little or no education. Overt features are used on everything from banknotes to personal IDs, to tax documents to brand hangtags. Overt features on banknotes include such obvious visual effects as the portrait images and the fonts used. These features though can be imitated by many printing techniques, and although useful for the public to identify a banknote and its denomination, they are not very useful to authenticate the banknote as genuine. Overt features, like all security features, are only valuable for authentication when they are unique to the security document manufacturing process. Valuable overt security features include the intaglio printing process, optically variable devices (OVDs) such as holograms, metallic patches, de-metallized threads, iridescent films, kinograms and similar devices, and optically variable inks (OVI). Figures 1 and 2 show examples of these types of features. More recently, several companies have commercialized additional printed, substrate-borne, and substrate-applied overt features. Why are there so many different overt features? Several government agents have remarked that, even with all these new and existing overt features there are few secure, unique, and obvious overt features that the public can find useful. This may or may not be true, but the fact is that the counterfeiters are getting better and better (often using digital origination and printing technologies), so security companies have to come up with more and more useful overt features to stay ahead of their 'competition'.

Figure 1
Printed Optically Variable Ink

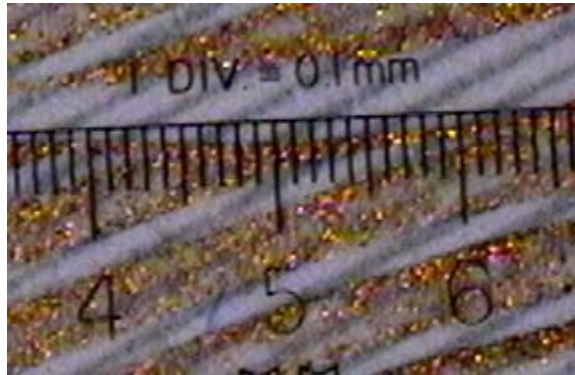
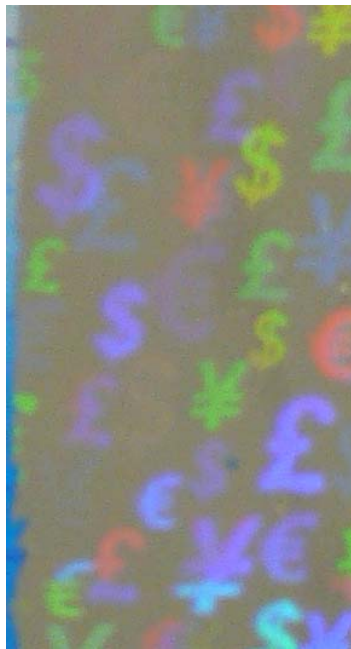


Figure 2
Security Holographic Foil



Overt Security Feature Needs

First and foremost an overt security feature must be obvious to the man-on-the-street, use secure manufacturing & transportation logistics and/or use secure materials. Intaglio printing is an illustrative example. Intaglio printing results in a raised image that can not only be easily recognized by touch, it is produced only when using intaglio printing presses that are expensive and have limited availability. Running an intaglio press is also not the easiest thing to do. So intaglio is obvious and is a secure manufacturing technique. Intaglio inks also have limited availability but the materials used to make the inks are generally available to others. In fact, you can find basic intaglio inks from several commercial sources. Intaglio depends mostly on the custom nature and limited availability of the printing tools. It does not depend on highly secure materials, although there are very few makers of high quality intaglio inks.

Beyond obvious, secure manufacturing and secure materials, what else does an overt secure feature require? Reviewing several overt security features, one finds several common aspects:

- Metallic visual effect
- Eye-catching but not so much that the feature looks like a toy

- Requires some interaction with the authenticator – like tilting or touching
- Easily integrated into current manufacturing processes (paper production, banknote production or other printing for ID, tax and brand applications)
- Durable (wide array of requirements)

When you add brand and tax applications into the discussion, you also have to add authentication by government or industry inspectors. For this group, they are also interested to easily authenticate the variable information- a serial number or batch code. This overt feature is most often printed by digital presses using non-secure black inks and non-secure presses. Other methods include a non-secure embossing technique or a non-secure laser etching technique. This important ‘variable’ overt feature is in fact not secure at all when applied by currently used processes.

Digital printing is used for covert security features but in this case, the security is based on secure materials – usually covert additives, and the secure locations the printing is done at. The presses used are available to just about anyone and the inks are designed to work in the standard presses. So can digital printing be made secure? And more interestingly, can variable overt secure features be made using digital techniques?

Can Digital Printed Features be Secure?

Like all security features, a digital printed feature to be truly secure should be:

1. Printed on unique equipment with limited availability
2. Printed with materials that are unique, have limited availability, controlled supply chain and even better are materials designed only to work with the unique equipment
3. Printed at secure locations by approved security suppliers
4. Integrated into other security features
5. Durable to its in-use environment

Like all overt security features, a digital printed overt security feature should be:

1. Obvious
2. Easily authenticated, preferably requiring interaction with the user
3. Easily integrated into current security manufacturing processes

A platform of overt digital printed features based on unique and difficult-to-replicate-materials, and custom built printing presses is being developed that shows the promise to fulfill the requirements mentioned above.

These features are based on unique metallic and inorganic fine particles that are made by unique production processes. There are many lab-scale techniques to make similar particles but these lab processes result in agglomerated particles that cannot be printed using high-resolution digital techniques. The particles made by these new-to-world processes have special nano-scale surface modification that result in non-agglomerated, non-agglomerating and non-settling particles useful in ultra-low viscosity digital inks. **The particles have inherent security.** The chemical nature and size of the particles can result in metallic effects, microprint effects, angle dependent effects and even optically variable color-change effects. And because the particles are inorganic-based, they are more durable than many security features. **The effects are obvious, easy to authenticate and durable.** Like intaglio inks, digital inks made with metallic and inorganic particles are not easy to formulate. The formulations depend on the nature of the particles, the printing method, the print speed and the substrate. The inks are only made for security applications. **The materials have security aspects.** To make the high resolution, high quality features in a robust printing process, custom tooling was developed that is only available to the security market. Digital printing techniques are routinely integrated into other security manufacturing processes. This custom digital tooling can also be integrated into typical security manufacturing processes. **The need for custom security printing tooling adds another layer of security to the features.**

Digital Printing Technology

There are many different technologies that can be employed for transferring a material to a substrate. In the context of this paper, the focus is coating or printing methods that transfer inks or pastes that contain materials that impart security to the substrate. Typically the material is the ink or paste, often in the form of a dispersed particle, has a unique composition and/or unique performance characteristics that combined with the printing/coating technique results in the secure feature.

When most people think about digital printing, they think about the printers we have at home. (Figure 3) These printers require certain types of inks- usually water-based and result in certain printed features. By eye, they might look good, but under closer inspection, one can see that the droplet placement and the visual image are not clean (Figure 4 and 5). The inks have been formulated for home-quality applications- not security applications.

Figure 3
Typical Home Digital Printer and Ink Cartridge

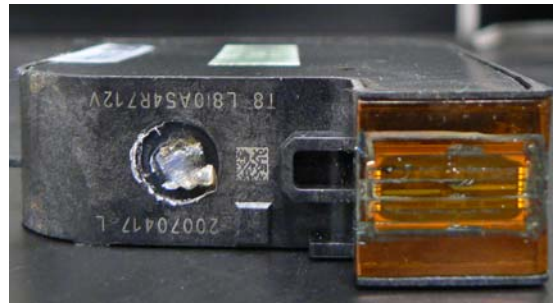


Figure 4
High Magnification Image of 'Snow' Printed by a Bubble Ink Jet Printer

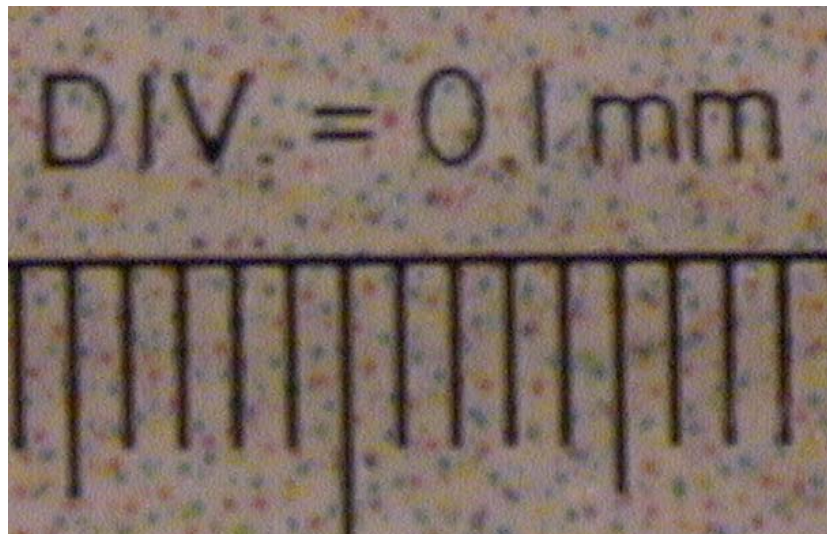


Figure 5
Image of High DPI Characters Printed on a Home Thermal Printer



Continuous inkjet (CIJ) is a common printing method used in brand and security manufacturing. CIJ is used to apply variable information at high speeds and has been used widely to apply covert security features. Leading companies have commercialized high speed, high dots-per-inch (DPI) features. Because of the way droplets are applied in CIJ, high quality micro-images are difficult to produce, and just like home printing, the inks have not been developed to give ultra-high quality images.

Figure 6
High DPI CIJ Images Printed on Postal Cards



The security industry has typically employed printing/coating methods to deliver secure particles that are analogue – that is, a pattern is transferred to the substrate that is identical on each security feature. These coating methods include intaglio, gravure and flexographic printing. These techniques provide high quality images and characters required by security applications. These printing methods add an additional barrier to the counterfeiter due to the high infrastructure cost of the equipment as well as the technical skill required to operate the equipment to deliver a specific structure to a substrate.

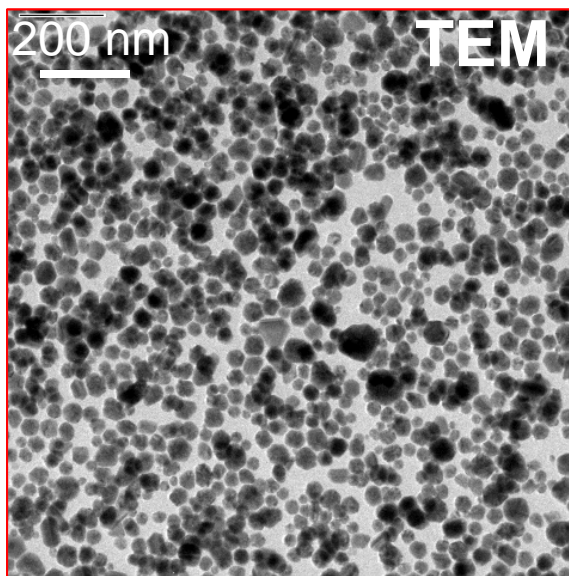
Digital printing methods, which are those that can transfer digitized information such as a digital image or pattern to a substrate have not been used extensively in the security industry outside serialization. It is the drop-on-demand methods that are the focus of this paper.

Security and Digital Printing

Given that desktop ink-jet printers are ubiquitous, it is reasonable to ask how ink-jet printing can be used as a printing method in the security industry. There are a number of aspects to the solution. The **first** aspect is in the technical complexity of the ink-jet ink formulations. – the fluids used in the ink-jet printing process. It should be appreciated that the ink-jet inks are extremely technically sophisticated materials that have to exhibit a number of combined critical criteria. The ink formulations (containing the functional security materials) are designed to operate in ink-jet print heads that require specific viscosity and surface tension tolerances to enable the controlled firing of multiple jets at high frequencies (often over 10,000/second) to reliably deliver small (e.g. 30 pL) droplets to a substrate that can be moving under the head at speeds greater than 1 meter per second and the ink is required to chemically interact with (wet) the substrate in a way that many thousands of droplets give rise to formation of a high resolution feature.

The **second** aspect is in the demands on the particle characteristics of particulate security materials that can be used in ink-jet formulations. Each droplet must pass through an ink-jet print head nozzle orifice that can range in diameter from a few microns to a few tens of microns. As a general rule, the particles contained in an ink-jet ink should have an average diameter around 10 times smaller than the diameter of the orifice through which it passes. In the context of security materials, this already sets a requirement for the materials to be at least smaller than ~200nm with absolutely no particles present in the fluid that have a dimension that approaches the diameter of the ink-jet nozzle. Figure 7 shows a transmission electron micrograph of ink jettable metallic particles. For particulate-based security materials, there are relatively few materials that have particle sizes in this range.

Figure 7
Metallic Fine Particles Used in Overt Security Features



The **third** aspect of the solution is the formulation of security particles of the second aspect above into inks that meet the requirements for the first aspect. This is particularly challenging where the security particles are inorganic particles and typically have a relatively high density. As a result the surfaces of these particles are often required to be modified using either steric or electronic modification strategies to achieve the necessary viscosity and surface tension as well as the reliability and shelf life (dispersion) characteristics.

This leads to the **fourth** aspect of the solution which is that unique processes for creating small (<200nm) particles of compositions suitable for security applications can provide an additional barrier to the counterfeiter, especially where there are either no, or extremely limited alternative productions methods for these materials. This size range is generally outside the range that can be achieved by typical particle size reduction techniques such as grinding or milling. In the case of certain specific materials, particle size

reduction leads to detrimental effects, for example reduction in luminescence intensity in phosphors and particle agglomeration in metals.

In the **fifth** aspect, the industrial ink-jet printing tools that can enable commercial security printing are generally highly limited in availability and provide feature characteristics on a scale that are hard or impossible to duplicate with more readily available SOHO printers. Figure 8 shows 2 lab scale versions of the custom tooling that can be used.

Figure 8
Custom Industrial Reel-to-Reel and X-Y Table Lab Scale Security Printing Tools



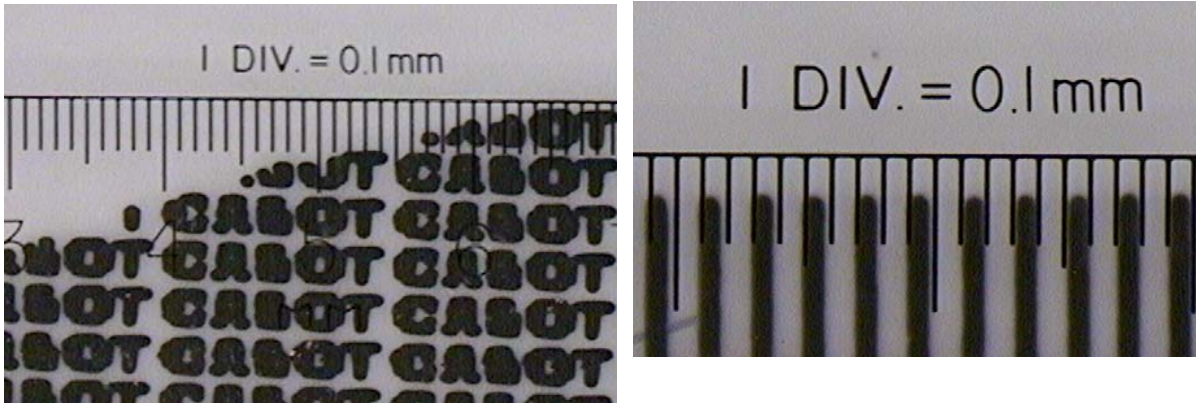
New Overt Digital Features

In this paper, we describe several aspects of digital printing of new overt features with characteristics that to our knowledge have not been demonstrated previously. The basic novel aspect is the ability to create ink-jet formulations of particles that when printed lead to metallic features. The metallic particle formulations are comprised of metallic fine particles that have average diameter of approximately 50nm and have been formulated into stable (many months shelf life) ink-jettable inks that have loadings that can be in excess of 50 wt.% if required.

Serialization

The ability to create a digitally-printable metallic ink enables the ability to impart variable information to a security feature, particularly serialization. The serialization can comprise numbers, letters, characters and the like. In addition other forms of individualization are possible which include printing of images. The unique attributes are the ability to provide serialized information directly as a metallic feature. An example of such metallic serialization and the line definition possible are shown in Figure 8.

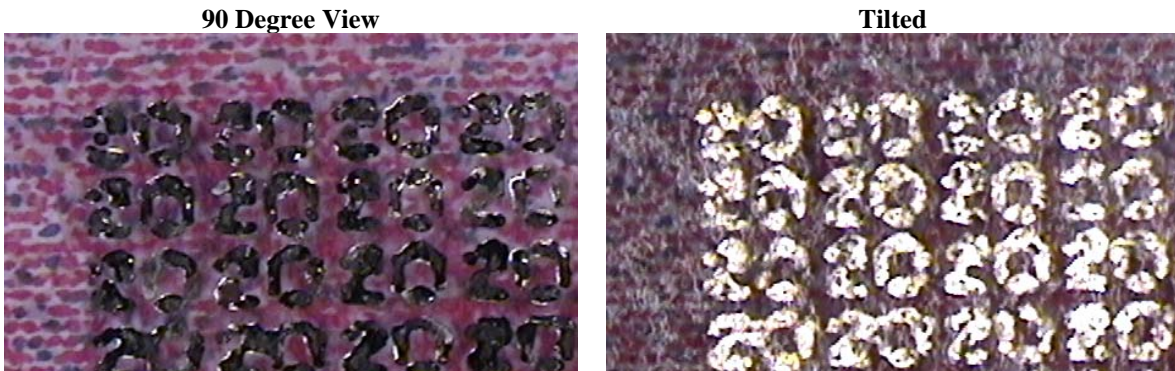
Figure 8
High Resolution 500DPI Features Using a Metallic Digital Ink



MicroPrint

Digital printing also enables to printing of very small features with primary feature size than can be on the order of the droplet size of the ink-jetted ink (~10 microns at a minimum). This enables the embedding of metallic microprint into security documents that can provide a level of overt (due to the metallic nature) and semi-covert (due to the size of the metallic microprint) characteristics.

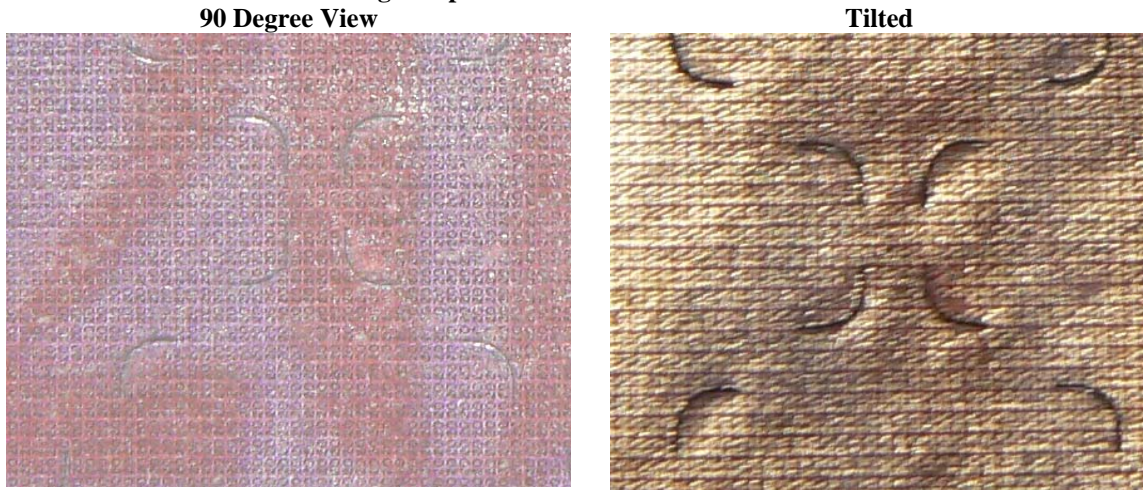
Figure 9
<200 Micron Height Serialization Using a Metallic Digital Ink Printed Over Thermal Ink Jet Images



Angle Dependent Effects

Ink-jetted metallic features can also be created in a way that gives rise to angle-dependent effects. For example, a metallic pattern, image or text can be printed over the surface of an underlying image in a way that only partially covers the underlying image. As a result, the underlying image is visible through the digital metallic over-coating when view perpendicular to the orientation of the substrate. However, because the over-coating is comprised of a metallic ink, when the security feature is tilted to an angle where the highly reflective nature of the over-coat reflects the background light directly at the viewer, the underlying image is apparently extinguished. This gives rise to an apparent angle-dependency of the visibility of the underlying image. An example of this effect printed on tamper evident labels is shown in Figure 10.

Figure 10
Angle Dependent Metallic Variable Effect



Integrating the digital metallic printing into an OVD creates another example of this angle dependent effect. (Figure 11) Straight-on viewing of this integrated feature shows the variable information in the OVD but not obviously in the rest of the document. Tilted, the printed variable information is extinguished by the OVD, but at the same time the metallic variable information in the rest of the document becomes obvious.

Figure 11
Angle Dependent Metallic Variable Effect Integrated into an OVD



Conclusions

Digital metallic overt security features have been created and result in a new class of security features. These new materials can be used to impart serialization, microprint, and even angle dependent effects. These features meet all of the needs for an overt security feature.

1. Printed on unique equipment with limited availability ➤ Custom digital tooling is required
2. Printed with materials that are unique, have limited availability, controlled supply chain and even better are materials designed only to work with the unique equipment ➤ Particles are unique and are made by a process with very limited availability.
3. Printed at secure locations by approved security suppliers ➤ Tooling and materials are only available in the security market
4. Integrated into other security features ➤ Features can be integrated into OVDs
5. Durable to its in-use environment ➤ Features are made with inorganic particles
6. Obvious ➤ Metallic, reflective and angle-dependent effects are obvious even in medium light
7. Easily authenticated, preferably requiring interaction with the user ➤ Angle dependent effects are most pronounced when tilted
8. Easily integrated into current security manufacturing processes ➤ Digital tooling can be integrated into other processes

This new class of overt security features shows great promise to provide new, interesting and useful security devices and allow designers to better incorporate variable information.