C17 Counterfeiting and Counterfeit Deterrence Applications for Imaging Technologies

Joel A. Zlotnick, MSFS, U.S. Department of State, 600 19th Street, NW, Ste 12.601, Washington, DC 20522*

After attending this presentation, attendees will better understand how imaging technologies are used by both counterfeiters and producers of security documents such as passports, visas, identity cards, and birth records, and how understanding the specific workflows used by counterfeiters can point the way to innovative counterfeit deterrence solutions based on the capabilities of imaging processes.

This presentation will impact the forensic science community by connecting the forensic science disciplines of questioned document examination and forensic imaging. As a result, attendees may find unexplored potential for greater cooperation in the areas of hardcopy counterfeit document deterrence and detection.

The forensic science disciplines of questioned documents and forensic imaging may be thought of as opposite ends of a spectrum in which hardcopy casework is in the realm of questioned documents and digital images are forensic imaging problems. Yet many common types of evidence in questioned document casework originate from a chain of analog or digital imaging processes, including (for illustration) the examples of trashmark comparisons for common source determination and examination of faxed or photocopied documents. Similarly, questioned document examiners routinely apply imaging techniques to resolve common casework problems. These include not just specialized techniques like electrostatic imaging for visualization of indented writing and alternate light source photography, but also more fundamental digital imaging techniques such as adjustment of contrast (and many similar enhancements) to scans or digital photographs of physical documents.

This presentation focuses on the relationship between the problems of counterfeiting and counterfeit document examination (usually regarded as questioned document issues) and the workflows used by counterfeiters to manufacture their products (which are unquestionably imaging processes). Counterfeiters possess two basic workflows through which they can manufacture fake documents: (1) a scan-and-print workflow where artwork is captured directly from a genuine document template and printed using process color devices; and, (2) a more involved artwork reorigination process in which the artwork is replicated, often using vector imaging tools, for printing using line art and spot color. The first option is popular with some counterfeiters because of its simplicity, but has limited ability to simulate the finer characteristics of genuine security documents. The second workflow has the potential to produce counterfeits that more closely approximate the artwork of a genuine document, but requires substantially greater skills and resources to accomplish.

This model is a significant oversimplification, since counterfeiters often blend these approaches. Further, it does not capture the complexities of simulating various classes of advanced document security features; however, it does provide a foundation for the idea that document artwork, by itself, plays an important role in counterfeit deterrence if it is used specifically to interrupt one of the two counterfeiting workflows described above. In fact, the important role of security document artwork in counterfeit deterrence is emphasized as sophisticated security feature technologies (such as optically variable devices and color shifting inks) become more widely adopted for non-security applications, which makes these technologies more accessible to potential counterfeiters and brings into question their value as standalone counterfeit deterrence solutions.

The basic techniques of counterfeit deterrence are, with certainty, rooted in imaging science. Certain security artwork strategies that are already in common use to combat one or both of the specific counterfeiting workflows described include the use of line art and spot color design, split fountain printing, microprinting, void pantographs, dedicated security halftones, and the use of inks encompassing expanded color gamuts (such as the use of Ultraviolet (UV) -responsive, metallic, or iridescent inks). These foundational security printing techniques are great examples of how inexpensive design strategies can make documents more resistant to counterfeiting; however, this presentation proposes that there is room for further work in this area and will describe some novel counterfeit deterrence concepts that specifically exploit differences between printing workflows used for production of genuine documents and counterfeit documents. The final purpose of this presentation is to initiate further conversation with the imaging science community regarding intractable forensic imaging problems, to determine if those problems can be purposefully extrapolated into the hardcopy printing world to deter counterfeiting.

Counterfeit, Imaging, Document