J13 Security Feature Implementation: The Other Side of Document Security

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 gain an understanding of why counterfeit deterrence is not just a function of security feature selection. In fact, the resistance of a security document to physical fraud also depends on how security feature technologies are integrated into the overall document design.

This presentation will impact the forensic science community by contrasting implementations of specific security feature technologies in documents such as passports, visas, identity cards, birth records, and currency. Attendees will develop a greater understanding of how to assess the value of security feature technologies based on how they are used and will be able to more critically evaluate feature authenticity using design considerations.

How should counterfeit deterrence be assessed? Some issuing authorities view document security as just a checklist, where a document must contain a minimum quantity of security features to meet a specified security threshold, but little attention is given to how the technologies interact with one another to make the document more robust than the sum of its parts. The effectiveness of a security feature depends on many factors: (1) the availability of the technology in commercial markets; (2) ease of feature recognition and inspection by both trained and untrained viewers; and, (3) how the feature is integrated into the document.

Recent decades have seen an explosion in the quantity and quality of security feature technologies available for prevention of physical attacks on security documents. Novel technologies that are new to market, or which possess limited commercial applications, are often attractive as new security features because they are relatively inaccessible to counterfeiters. As security feature technologies mature, many find applications in the commercial world, making them more available to criminals and potentially reducing their intrinsic value as security technologies. This view of security features as possessing a life span has merit and should not be ignored, particularly in light of many documented instances of complex security feature technologies (or high-quality simulations of them) being detected on counterfeit documents or sold into commercial markets over the internet. Specific examples will be provided.

If the above viewpoint holds that it is the rarity and proprietary nature of a security feature technology that provides its value for counterfeit deterrence, consider an opposing viewpoint: it is also the specific implementation of a technology, and not just the technology itself, that deters counterfeiting. For example, offset printing is widely used in the commercial world, yet it also finds broad applicability in production of passports, visas, birth records, identity cards, and other documents. Similarly, Ultraviolet (UV) -reactive and other specialty inks have been available in commercial markets for years, yet inclusion of UV-responsive artwork is nearly ubiquitous in security printing and UV inks are not considered high-security materials.

What these two examples have in common is that it is not the technology itself that provides security, but rather how it is employed differently in security environments than in commercial environments. In the offset printing example, commercial offset typically uses dot halftones and process color, so security document artwork is created almost exclusively using line art and spot color for no other reason than to make it different from commercial offset printing. Regarding UV inks, it is not the presence or absence of a UV response that makes a document genuine or counterfeit. Instead, genuine document issuers rely on intricate design work and the use of specialized printing techniques to create complex UV designs that counterfeiters may not possess the skill to replicate convincingly. The common thread between these two examples is that it is design, not just fundamental characteristics of the technology, that makes it appropriate for use in security printing.

The message from these and many other examples is that viewing a security feature technology as either secure or not secure ignores implementation considerations. This presentation argues that assessing a broader range of security technologies in terms of how they are implemented clarifies how these technologies can best be used in security environments and even prompts new security applications for certain document components that are often regarded as low-security commercial materials.

Security Feature, Counterfeit, Design

*Presenting Author