Personalizing Digital Printing Using Digital Watermarking

J. Scott Carr
Digimarc Corporation
Tualatin, Oregon, USA

Abstract

Counterfeiting and piracy of branded products, packaging, and documents is one of the fastest growing industries in the world. In the past, brand counterfeiting and product diversion were the activities of individuals with small-scale, local operations. Today, a sophisticated global network targets specific documents, brands and products, contributing to billions in yearly business loss.

Consumers make purchase decisions based on the package of brand products. The availability of low-cost personal computers, color inkjet printers and scanners are making it easier and cheaper for professional counterfeiters – or even amateurs – to create "look alike" packaging to promote counterfeit products. This results in an erosion in brand confidence and profits going into the counterfeiters' pocket instead of the brand owner.

Gray market products, diverted from their intended destination, further rob brand owners and undermine market pricing.

Digital print-on-demand provides a platform to create personalized packaging and labels. When used in security applications, the digital printing environment allows for the insertion of covert, machine-readable data using digital watermarks.

Whether you issue secure documents or manufacture and distribute brand-name products, this presentation will show you how to turn the digital revolution to your advantage and defend against digital counterfeiting and forgery.

Introduction

Digital watermarking is a new and diverse communications infrastructure that can be used within brand packaging, as well as other printed and digital content, for security, marketing and e-commerce applications.

The Digital Counterfeiting Threat

New counterfeiters and pirates are being aided by powerful, new digital imaging products that are supplanting traditional means of counterfeiting, such as lithography.

Low-cost personal computers, scanners, and color inkjet printers are more readily available to home consumers and are shipped today with more powerful features and functionality. With these products, everyone and anyone can counterfeit. All documents and packages are at risk.

Digital Watermarking as a Security Feature

Digital watermarking gives printed content a unique identity that adds marketing value or enhances document security.

In security applications, digital watermarking is a feature that can be applied to protect brand packaging, value documents, and cards from counterfeiting.

This identity – digital codes that are embedded into a document during the printing process – can be the same for all printed materials or can be unique to each individual printed piece. In fact, the ability to easily apply personalized digital watermarks to different print documents is especially well suited to the short-print-run nature of the digital printing environment.

Carrying covert data specific to the package or distribution, the machine-readable digital watermark allows inspectors and businesses to identify the authenticity of a package or to determine that a product came through a legitimate distribution channel. Digital watermarks do not require a packaging design change or additional materials, and are durable to the lifetime wear and tear of the package.

Digital Watermarking for Enhanced Marketing and E-Commerce

Digital watermarking can also be applied to packaging, documents, and cards in a new way to increase the marketing value of these printed materials. For example, digital watermarking can be used to enhance the marketing or promotion of packaging or other print materials, or to provide purchase opportunities.

In e-commerce applications, digital watermarking allows content and brand owners to effectively manage digital assets and rights, deter counterfeiting and piracy, and improve Internet access and navigation.

Defending Against Counterfeiting with Machine-Readable Features

To defend against new threats to document or brand packaging, security design typically has employed a wide arsenal of defense features and deterrents:

- Ink and paper
- Special printing
- Optical security features
- Security threads and other physical devices
- Special chemicals / adhesives
- Machine-readable features

Machine-readable features include barcodes; magnetic strips and ink; OCR; RFID; embedded chip devices; and now, digital watermarking.

Applications for digital watermarking to protect brands and product packaging from digital counterfeiting or diversion are diverse, from intelligent packaging to authentication and track and trace capabilities.

Conclusion

As a security feature, digital watermarks are compatible with other security designs and features and can be added to secure documents and packaging at a very low production cost and without the need for new materials or designs.

With digital watermarking technology, now every package, value document, or card can carry machine-readable data to defend against digital counterfeiting and product diversion.

Biography

As general manager and vice president of Digimarc's Secure Documents business, J. Scott Carr oversees strategy, operations, and performance of digital watermarking solutions to enhance the security of printed value documents, product packaging, and cards.

In this role, Carr authored a paper on “Digital Watermarks as a Security Feature in Identity Documents,” and has presented papers at several leading security and digital imaging conferences, including:

- Tag, Ticket, and Label Digital Printing Conference
- SPIE – The International Society for Optical Engineering
- PISEC – Product and Image Security
- Intergraf – International Confederation for Printing and Allied Industries

Carr is also the co-inventor of 26 pending patents in the U.S. and three pending foreign patents in the use of digital watermarking technology as a security feature.

Carr has more than 18 years experience in technology management, strategic marketing, and software development, with a focus on electronic commerce and interactive media. He joined Digimarc in 1996, and works from the company's headquarters in Tualatin, Oregon, a suburb of Portland.

Prior to joining Digimarc, he was vice president of marketing for nCUBE, a firm that specializes in servers for broadcast-quality video delivery. Carr also held several software and marketing positions at Sequent Computer Systems, where his work included strategic marketing and business development for video-on-demand and complex, highly available database systems.

Carr has previously held software development positions at manufacturing and factory automation companies. He holds a Bachelor of Science degree in Computer Science from Oregon State University.