WHITE PAPER

OPTIMIZING DIGITAL WATERMARKING IN PRINT WORKFLOWS

1st Edition, August 2022

GLOBAL GRAPHICS® software

Contents

Introduction

Back in the 1970s and '80s barcodes on products in the supermarket were a wonderful innovation, enabling much faster and more accurate checkouts. As with pretty much everything else, they've moved on a lot over the intervening four decades. While UPC and EAN barcodes are still a common sight on packaging, you'll have also seen QR Codes for marketing outreach to users and consumers. And although you may not have recognized them, you'll also have seen Data Matrix and Aztec codes (amongst others) for logistics tracking on everything from secondary packaging to transportation tickets.

FIG 1 - Example 1D and 2D barcodes in common use

All of these are pretty good for staking a claim as to what an item is and how it should be priced or handled.

Countering counterfeits

Some of the more complex two-dimensional codes such as Aztec, Data Matrix and QR can also carry encrypted data. That can be connected, via a reader, to a database, often in the cloud, supporting authentication of that claim: is this object really what it claims to be?

That authentication is very important, and growing more so, especially as more goods are purchased or delivered from online systems and there is more need for transparency and authentication throughout supply chains. With that volume of ingredients, components, materials and products flying around the world, some of them with very high value in relation to their size or intrinsic cost, more and more products are counterfeit.

"The value of counterfeit and pirated goods will exceed $1.9 trillion globally by 2022, according to the International Chamber of Commerce."

But the cost of counterfeit goods runs well beyond the simple monetary value of those goods themselves. Poorly made products can be dangerous, and will often disappoint their consumers, damaging the reputation of a brand. Pharmaceutical companies and premium brands shipping goods such as tobacco, spirits and beauty products now routinely implement systems to track and trace packaging, and to authenticate that those products really are what the packaging claims them to be. In some cases, this is required by local or regional regulations. The same systems can provide extended information on ingredients lists, expiry dates and the like, and can be leveraged if product recalls are required.

Barcoding products to support these processes is therefore very valuable, which immediately makes the barcodes themselves the target of counterfeiting. That's why the barcode is usually only one part of an overall system that includes global databases and data validation. But if every instance of a barcoded object carries the same barcode it would be very easy to simply copy that barcode and inject counterfeit products carrying that same code.

The obvious next step is to ensure that every barcode is unique, carrying encrypted data with internal validation of consistency that can be traced back to a specific item printed, manufactured or packaged at a specific site at a specific time. If a barcode is copied and used on counterfeit goods, the authentication system can quickly identity a problem when multiple items are scanned in different locations and found to have the same code, or when internal checksums don't match.

Through the rest of this document, we'll describe jobs and items where the same digital watermark is used on every item as being 'static' jobs, and those where each item carries a unique digital watermark as 'variable'. Of course, there are intermediate models, where each unique digital watermark is used on some subset of the job, such as where a batch number or production date is included in the data in the watermark. These should be considered as static or variable depending on how large that subset is.

The terminology in this document speaks mainly to products and packaging, but there is significant value in using barcodes and digital watermarks for transparency in manufacturing workflows and supply chains, track & trace, authentication, and for many other use cases. The terminology here should not be taken as limiting!

Digital watermarking

Best practice in product security, covering track and trace, authentication and other anti-counterfeit goals, is to combine several measures, usually a combination of overt (visible to the average user) and covert (less obvious) techniques. A standard barcode is toward the overt end of this scale but can be made much stronger if data is provided in a covert way. One way of doing this is to use a digital watermark.

"Global Graphics Software has partnered with Digimarc, a leader in digital watermarking, to bring you this white paper, exploring aspects of some innovative joint discussions and developments"

Digital watermarks are an emerging technology, part of the latest step on the evolution of product identification. They provide a covert replacement or complementary addition to pre-existing barcodes for retail, logistics, track & trace, authentication, etc. In effect, they cover a large proportion of an item with an equivalent to a barcode, but do so in a way that is not immediately obvious to a human viewer, and is harder to reproduce on counterfeit goods.

With appropriate messaging they can also be used as an alternative to QR codes, providing data, web links or hooks for augmented reality (AR) experiences to consumers using appropriate apps on their smart phones, whether on packaging or point-of-sale graphics or any other use case.

Digital watermarks go beyond just being a more secure variant of other kinds of barcodes. They can outperform Data Matrix in supply chain logistics, scanning more reliably. In both supply chain and retail, they can reduce frustration and make scanning faster because an item may not need to be rotated to ensure that a reader can see the code to scan it. By carrying more data than a UPC or EAN retail code they can add track and trace and authentication capabilities, and make it easier for consumers to check important concerns such as expiry dates and allergens in the ingredients.

Moreover, their covert nature means that the aesthetics of the brand design are preserved, even when the encoded data is copied all over the item.

Approaches to digital watermarking

A digital watermark may be added in one of two ways.

If a product design includes images, whether photographic or generated digitally, data can be hidden within that image data using steganography.

" Steganography is the practice of concealing a message within another message or a physical object " Wikipedia

In order to hide the data, the color values of individual pixels in the image are altered in a way that is intended to not be obvious to the human eye. The alterations may need to be applied slightly differently depending on the image content and the print technology to be used. This means it's often valuable to be able to proof a design with the images in place, and to do that either on the printing device that will be used for production, or on one that has been carefully tuned to reproduce color, tones and levels of detail to match that production device.

Alternatively both the printer/converter and their customer can inspect the artwork and verify the Digimarc code using PACKZ or CLOUDFLOW Proofscope, professional prepress tools from HYBRID Software. As well as checking for the correctness of the code, this also allows verification that the code placement conforms to the customer's requirements, and supports a formal approval process.

Reviews of the proofed output may lead to a decision to re-embed the data into the image with slightly different parameters. Systems to automate that adjustment are improving, but the advisability of proofing means that steganography is best used at a point in the workflow where an appropriate review and reconfiguration may be made without disrupting throughput.

Steganography is a very effective technique if the same image will be used on every instance of an item because it can be difficult for a forger to reproduce. But if your goal is to encode unique data in each instance, you'd have to generate an altered image for each one. When you're producing watermarks for a large number of instances that would mean generating a huge number of copies of what started off as a single image. In most workflows and for most products that's not a commercially viable approach.

You can read more about creating efficient PDF files for variable data printing in Global Graphics' guide "Full Speed Ahead: How to make variable data PDF files that won't slow your digital press", available at https://www.globalgraphics.com/full-speed-ahead.

The second method for adding a digital watermark is to overlay an "artwork masking layer" that encodes the desired data. This is a pattern of graphics across large areas of the design, making sure that those graphics are sufficiently fine that they are not immediately apparent to a viewer. In practice this usually means something that looks like a sprinkling of very fine dots under a magnifying glass or loupe.

FIG 2 - A digital watermark as an artwork masking layer over a plain yellow area of a job.

These overlays are also very difficult for a forger to reproduce. They have the advantage over hiding data in images that they can also be used in efficient workflows to carry unique data for each product instance; there is much less data to handle for every copy.

This white paper is not intended as a security manual. If you want to know more about how these technologies work, how to tie the data into tracking systems, or get recommendations on whether you should use steganography or artwork masking layers for your specific requirements, you should ask your security technology provider; somebody like Digimarc.

Timing of digital watermark application

Just as there are two ways to add a digital watermark, there are also multiple stages in a design, prepress and printing workflow at which they may be applied.

During the design stage

In some workflows the designer may apply digital watermarks to a design by, for instance, using a plugin to an application such as Adobe Illustrator. This is equally appropriate for both steganography and an artwork masking layer, and gives the maximum opportunity for approval of the design with the digital watermark in place, and for any rework to the design that might be requested to realize the greatest benefit from using that watermark.

It will not normally be appropriate for the digital watermark to be added by the designer if each instance of the print requires unique data to be encoded in it; variable data composition is usually performed later in the workflow.

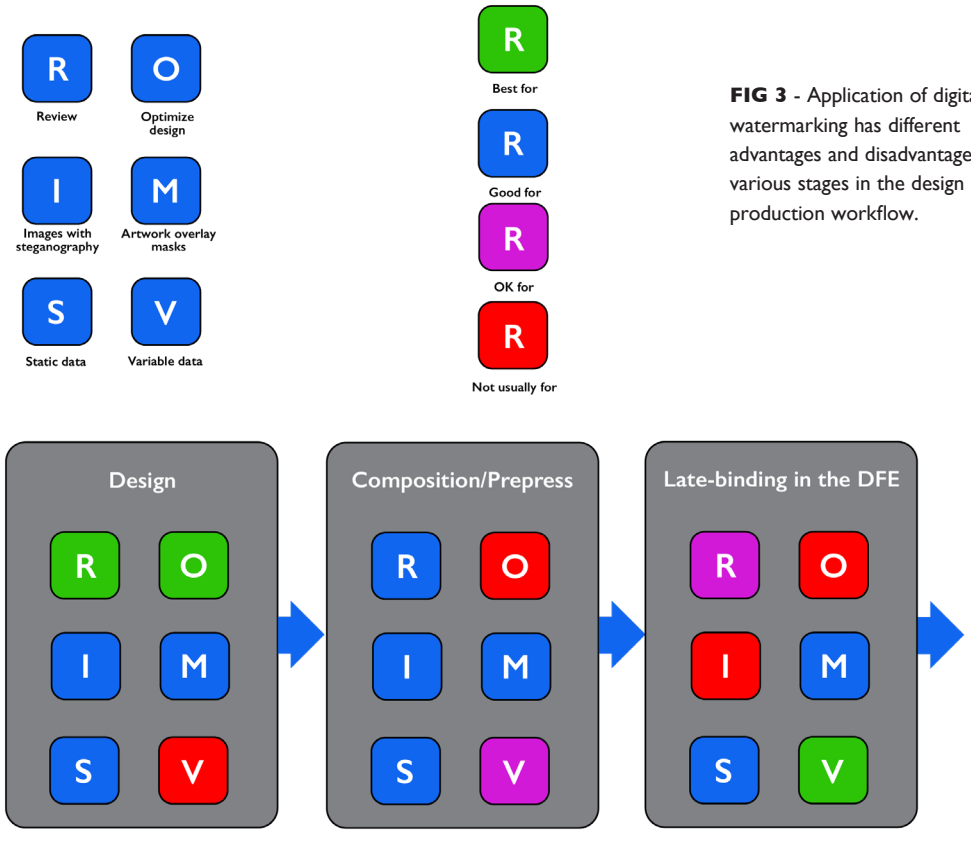

FIG 3 - Application of digital watermarking has different advantages and disadvantages at various stages in the design and production workflow.

In composition / prepress

In other workflows adding the digital watermark may be a function of a variable data composition or prepress department. Just as for application by the designer, this is applicable for both steganography and an artwork masking layer. There is a reasonable opportunity for approval of the design with the digital watermark in place. But it would be slower and more expensive to rework the design if that is required at this stage than if the watermark were added by the designer.

If the digital watermark is added in prepress then it can carry both static and variable data. As discussed above, however, variable data is best suited to use of an artwork masking layer rather than steganography, if only because of the amount of data that must be generated and then incorporated into a PDF file when steganography is used for a significant number of unique codes.

But applying even an artwork masking layer in prepress does bulk up the resulting print-ready PDF file with many copies of that layer, each one carrying different data. And it can also slow down processing in the Digital Front End (DFE) for a digital press. An overprinted graphic covering large areas of each piece of output in the PDF file can make it harder for the variable data optimization in a DFE to break the design apart so that it can minimize the total amount of processing required to read, color manage, render and halftone screen the job. Again, see Global Graphics' Full Speed Ahead guide.

Late-binding in the DFE

A new development in the application of digital watermarking is to add the marks right at the very last minute before the data is printed. This can be done in parallel with or after the color management and rendering in the SmartDFE from Hybrid Software Group..

Applying the watermarks in parallel with color management and rendering (in the RIP) allows full access to all color channels for the output, while also removing the need to generate a fully resolved "optimized PDF" or PDF/VT file containing all of the variable data further upstream. In turn, this can reduce the overhead of optimizing variable data processing in the RIP. The final result is increased throughput, both in composition/prepress and in the DFE.

Applying marks after the RIP enables even higher performance through the DFE, with the added benefit of providing a more predictable processing speed because the amount of processing required is more deterministic than is rendering PDF. This might restrict the watermark to be painted in only one color channel, though.

Increasing speed and predictability in the DFE allows the use of lower cost hardware in those DFEs, or assists with printing at full engine speed for a larger proportion of jobs.

Late-binding application of digital watermarks will also always occur in an environment where the characteristics of the press that will be used to print the items are known, including resolution, bit-depth etc.

These benefits make this the optimum choice for highly efficient printing workflows for variable data digital watermarks, driving digital presses at full engine speed. The trade-offs are that it's a little harder to review and approve proofs of the output, and that use for images with steganography is not usually appropriate.

Quality control

Wherever the digital watermarks are applied in the workflow it's usually recommended to review a selection of the final prints, manually and/or using automated tools.

If late-binding application in the DFE is used, then it's very important that at least some production copies are pulled for inspection. This is still advisable even if proofing and approval has been done earlier in the workflow, especially if that proofing was not performed on the press used for the real production run and at full speed.

In-line or near-line vision systems may need to be tested to ensure that they are not confused by artwork masking overlays.

Summary

Digital watermarks are an emerging technique available and beneficial to more and more brands and graphic arts professionals.

Software companies and digital press vendors are looking at how to differentiate product capabilities by supporting digital watermarks.

Each choice of where in the workflow digital watermarks should be applied brings different costs and benefits. A wider debate about the value of each option would be valuable in designing and developing future product.

To discuss your requirements around digital watermark creation and back-office systems for tracking, authentication, etc, contact Digimarc: info@digimarc.com or 1-800-DIGIMARC.

To discuss your requirements for application of digital watermarks late in the production workflow, contact Global Graphics Software: www.globalgraphics.com or info@globalgraphics.com.

About the author

Martin Bailey, Distinguished Technologist, Global Graphics Software

Martin Bailey works to analyze and understand current and future needs for workflows across many sectors of print. This enables him to guide Global Graphics' industry-leading printing technology. He represents Global Graphics on a number of industry bodies and standards committees including acting as the primary UK expert on the committees working on PDF, PDF/X and PDF/VT.

Martin has over 30 years of experience building, using, supporting and improving products for processing digital documents and the print industry in technical support, product management and programming as well as in consulting, and production environments.

About Global Graphics Software

Global Graphics Software http://www.globalgraphics.com is a leading developer of innovative software components for digital print, including Harlequin RIP, ScreenPro, Direct, SmartDFE and Mako. Customers include HP, Canon, Durst, Roland, Kodak and Agfa. The roots of the company go back to 1986 and to the iconic university town of Cambridge, and, today the majority of the R&D team is still based near here. Global Graphics Software is a subsidiary of Hybrid Software Group PLC (Euronext: HYSG).

About Digimarc

Digimarc is a global leader in product digitization, delivering business value across industries through unique identifiers and cloud-based solutions. A trusted partner in deterring digital counterfeiting of global currency for more than 20 years, Digimarc illuminates a product's journey to provide intelligence and promote a prosperous, safer, and more sustainable world. With Digimarc, you can finally see everything. And when you see everything, you can achieve anything. For more information, visit us at www.digimarc.com.

GLOBAL GRAPHICS® software

August 2022 v1

Contact us.
info@globalgraphics.com

www.globalgraphics.com

Global Graphics Software Inc.
5996 Clark Center Avenue
Sarasota, FL 34238
United States of America
Tel: +1(941)925-1303

Global Graphics Software Ltd
Building 2030
Cambourne Business Park
Cambourne, Cambridge
CB23 6DW UK
Tel: +44 (0)1954 283100

Global Graphics KK
610 AIOS Nagatacho Bldg.
2-17-17 Nagatacho, Chiyoda-ku,
Tokyo 100-0014
Japan
Tel: +81-3-6273-3198