How Signum's Digital Watermarking Combats Counterfeiting and Forgery

Graham Shaw
Signum Technologies Ltd.
Witney, Oxon, United Kingdom

The revolution in digital data processing has brought many benefits to the way we create, organise and manage information, whether in the form of images, documents, audio or video files. The conversion of such information into digital form provides us with capabilities such as online storage and retrieval, efficient search processes and worldwide data transmission. But digital data also brings with it a major problem, namely the ease with which such information can be copied and tampered with. Similarly, in the field of printed material, the availability of low-cost high-quality scanning and reproduction devices has, combined with desk-top imaging tools, enabled valuable documents – ranging from ID cards/passports to cheques and product pack designs – to be counterfeited or forged at little or no expense and with sufficient quality to pass other than professional detailed examination. The need has therefore arisen for technologies which are able both to safeguard the integrity of original digital records and to carry this integrity check through to the printed document. Digital watermarking, developed by Signum Technologies, enables both digital records and printed documents to be protected against counterfeiting and forgery. Through its unique methodology, Signum watermarks can embed information (using highly-secure permutation keys) imperceptibly into original digital data and enable such information to be recovered from printed copies so that not only can fraudulent alteration of the document be detected but also an original document can be distinguished from a high-quality copy.

The Need – Digital Records

At its simplest, the security of digital information is addressed at three discreet levels:

- Security of access – ranging from password-controlled networks to transmission of encrypted data. A vast array of cryptography-based technologies – e,g, smart cards, secure 'envelopes' – are in development to address the concerns of digital confidentiality.
- Security of the parties – it is of no use keeping digital data secure if such data falls easily into or is accessible by "the wrong hands". Of equal importance, therefore, are security measures which authenticate the parties to digital transactions through the use of developing technologies and processes such as digital signatures, biometrics and TTP's (Trusted Third Parties).
- Security of data – the third and vital element is the ability to verify that a digital record or file is true to the original and has not been changed inadvertently or tampered with fraudulently. Such concerns apply in a number of different ways:
- The ability to ensure that data stored in a digital archive has not been altered since origination
- The ability to ensure that data received is identical to data sent should security of access be compromised at some point in the delivery process
- The ability to ensure that data identity, such as ownership or source, has not been compromised

In its broadest sense, security of data is concerned with ensuring that a digital record *is* what it purports to be, whether in respect of content or origination.

From the standpoint of forgery, protection of digital records is of equal importance to the protection of printed documents. Increasingly, the basis of a legal transaction is a digital file – e.g. a cheque image – which replaces transfer of the hard-copy medium. The risk of such files being attacked and altered during capture, transmission and/or receipt adds weight to the need for systems which secure file integrity such that any modification can be detected and reported. Similarly, the replacement of a valid file with unauthorised data also needs to be detected if reliance on digital records is to be well-founded.

Signum digital watermarking, as described below, enables the integrity of digital records to be preserved permanently so that reliance can always be placed on their original content, even if retrieved after several years from long-term archives.

The Need – Printed Documents

A new dimension is added to the issue of security of data when digital records are used for the origination of printed material. In product and image security applications, a number of differing requirements exist across the spectrum of applications:

- The ability to trace the source of a valuable document
- The ability to authenticate photographs in passports and/or other identity documents (driving licences, smart cards etc.)

- The ability to embed unique data codes into product packs, identifying origination and/or distribution channels
- The ability to encode variable data (e.g. cheque monetary values) into the document itself
- The ability to detect an original document from a near-perfect copy

A variety of security techniques have been developed to protect against counterfeiting and/or forgery in respect of the above applications, either for legal reasons (ID documents) or for the protection of hard-earned revenues (pack designs). However, some of these techniques require specialised printing processes or add significantly to product cost through the use of features such as holograms, special laminates etc.

Signum watermarks can be used to permanently identify and authenticate printed documents with minimal change to print processes. The ability to apply unique watermarks to individual prints means they are particularly suited to digital printing applications whilst the incremental cost of adding watermarks to printed material is far below alternative security technologies.

The Technology – Digital Watermarking

Digital watermarking is a modern form of the ancient art of steganography which is, in essence, the ability to hide information inside other information. Earlier examples of steganography range from invisible ink on personal letters to the encoding of hidden messages into normal text files. In its modern form, digital watermarking enables data to be embedded imperceptibly and permanently into digital media files. Such files include images, documents, audio and video data and include a wide range of formats. For example, digital watermarks can be embedded in black & white 1-bit documents as well as full-colour 32-bit images. Remarkably, the embedded watermark can be recovered not only from the digital data but also by rescanning its printed version using low-cost scanning technology, including hand-held devices. In this respect, digital watermarking provides a cross-over technology which spans the protection of both digital and hard-copy data.

Signum Technologies' digital watermarking technology is based on the use of secure permutation keys. It is vital that the application of watermarks for security purposes can be carefully controlled. This approach prevents removal of the watermark once applied and also, through control of the unique application key, unauthorised application of watermarks to adulterated data. It is important to remember that digital watermarking is not a form of data encryption – the original record remains fully accessible – although Signum watermarking can be easily combined with encryption technology.

In essence, digital watermarks can be used in two respects:

- To apply an imperceptible pattern into the digital data such that, any subsequent change can be detected and its location pinpointed. The detection of change can be represented visually on the desktop or as a system flag within a system environment. It is important to note that validation of content applies only to the digital file, not the printed output.
- To embed a unique code into a digital record. Such a code can be used for a variety of purposes, e.g. date/time stamp, identity of source, identity of content, document revision level, transaction status, ownership. The embedded code cannot be modified once applied and, as stated above, can be retrieved from the printed form with low-cost scanning devices.

The embedded code capability is of particular benefit in the fight against counterfeiting or forgery of printed documents. In particular, the application of Signum digital watermarks provides the ability to use the embedded code to detect an original document from a near-perfect copy. This is particularly important where counterfeits, including many visible security technology features are created using high-quality scanning and printing devices. The uses for watermark embedding are widespread.

Case Studies

Banking

In the banking field, there are two primary concerns:

- Counterfeiting and/or copying of the original cheque stock
- Forgery through alteration of the variable data printed on the cheque – name of payee, dollar amount etc.

Using Signum watermarks, a digital code can be embedded into original cheque stock which not only allows unwatermarked counterfeits to be easily identified but also enables copies of original cheque stock to be flagged during the cheque processing workflow. Similarly, at the time of printing variable data onto the cheque a Signum watermark can be embedded during the print process, using patented incorporation of watermarking into printer driver software. Such watermarks carry codes relating to the variable data on the cheque and any subsequent change to this data can be flagged when the cheque is captured as an image.

ID Documents

In respect of ID documents, a number of concerns are prevalent:

- Counterfeiting of the entire document, typically using high-quality copying.
- Fraudulent replacement of elements of the document, typically individual photos
- Fraudulent alteration of data within the ID document, e.g. expiry date.

Signum watermarks can provide a counter to each of these issues. Embedded codes in the original ID document prevent outright counterfeiting and detection of copies. The watermarking of photos protects against their replacement and can also be used to protect against changes to variable data whereby, as with cheques, such data is encoded into the photo watermark, enabling changes to be detected through a simple scan process.

Packaging

In the packaging field, the primary concern relates to counterfeit goods which rob the vendor of revenues and are a major source of danger to the consumer, particularly where products such as pharmaceuticals are involved. A secondary concern is the routing of packaged goods through unauthorised distribution channels. By embedding Signum watermarks into master pack designs, ounterfeits can be readily detected, either through the lack of a watermark being present or through detection of a copy versus an original. Using digital print processes, individual packs can have a unique code embedded, enabling the source of grey imports to be tracked

These are just some examples of how digital watermarks can support the fight against both counterfeiting and forgery. Numerous other examples exist – insurance documents, legal records, audio and video data – all of which have the same concerns of authenticity. As explained above, Signum watermarks protect not only the printed document but bridge the gap between the digital and print domains by providing integrity checking throughout the document cycle.

The Products

Signum has commercialised two forms of its digital watermarking: 'SureSign' for copyright ownership and 'VeriData' for data authentication and anti-counterfeiting. Both share the same essential features:

- Application though a secure permutation key.

Signum watermarks can only be applied and detected through the use of a unique application key. This prevents the unauthorised application of watermarks and, should the key be compromised, it can be easily and quickly replaced. Without knowledge of the unique application key, embedded watermarks cannot be detected and are therefore wholly invisible to prospective counterfeiters and/or forgers.

- No requirement for additional metadata
- No increase to data file sizes

Digital watermarks do not affect print workflows in any way. File formats are not altered and watermarks can be added to numerous standard and proprietary formats.

- Embedded codes survive high levels of data compression

Where watermarks are applied early on in the production process, subsequent compression of the image or document data does not affect their detection.

The Validation Method

Digital Records

Signum provides a complete version of the VeriData algorithm which includes Signum's own hashing, encryption and embedding algorithms. These operate at a high level of security and are more than adequate for most customers. However, for those customers who wish for the extra reassurance of algorithms which have gained global acceptance, it is possible to replace the Signum algorithms with industry-standard algorithms (e.g. MD5, SHA-1) whilst working within the framework which this software provides.

It is not essential to have high security at every possible stage of the process. One properly administered security feature will protect overall security. If an asymmetric algorithm such as RSA is used for encryption of the signature then the reading software that actually confirms the authentic nature of the file can be freely distributed without providing the means to authenticate the file.

The VeriData method consists essentially of two parts. The first part is the calculation of a "signature" or "digest" of the data in the file concerned. This is similar to the method used in several other applications. The second part is the embedding of the signature back into the data file. This is carried out in such a way that the format of the file is not altered and the quality of data is not degraded. It is this second part which gives the uniqueness to the VeriData algorithm.

- Each user has a unique key, typically of 128 bit length.
- The encrypted signature is embedded within the file at selected sites. The selection of the sites is carried out by an algorithm that depends upon the key. VeriData uses an algorithm based upon permutations and it is possible to customise the permutations for any user.
- Signum provides a non-linear hashing algorithm which can be rapidly executed. SHA1 and MD5 algorithms are included for possible selection. Alternatively, the user can supply an algorithm of their own choice.
- The signature is encrypted before embedding into the file. Signum supplies a simple symmetric encryption algorithm for this purpose. RSA asymmetric encryption can be included as an alternative.
- The algorithm results in a binary string of n bits and n sites into which it may be embedded. The method of embedding is again customisable and provides another opportunity for adding security.

Printed Documents

The method of embedding unique codes for detection from printed documents is called VeriData ID. The watermark becomes an integral part of the image and is so constructed as to minimise any degradation of the image data. The method of encoding provides a high level of security, comparable with techniques employed in other areas.

The watermarking process has three stages. Firstly, the conversion of any embedded code into a binary stream. Secondly, the calculation of sets of permutations, each set corresponding to a particular key. Thirdly, the addition of the permuted code to the original digital data. The third part may be further subdivided into two processes. The first is that of dividing the data into suitable subsets, in the case of images those subsets comprise tessellable shapes, in the case of audio or other linear data the subsets comprise repetitively defined chunks of data. The second process is that of adjudicating at each part of the data how large a change in the original data will be acceptable to any user.

The strengths of the permutation method lie in its universality and flexibility. It may be applied to different types of data and, for any one data type, it may be applied in many different ways.

- Code Conversion to Binary - the process results in a binary code which in present implementations will normally have between 20 and 50 bits.
- Conversion of a Key into a Permutation - the lynchpin of the method is the use of permutations to conceal the embedded code. Even with 20 bits the number of possible permutations is 2.4 x 10^{18}, clearly enough to prevent any systematic trial and error search. The most secure method for producing permutations is one in which there are initially chosen arbitrary permutations from which all others are generated, and this is the method used by Signum. The choice of the arbitrary originating permutations is roughly equivalent to the key, computed from two arbitrarily chosen prime numbers, which is used for RSA coding.
- Addition of Code To Original Data - this involves taking the binary message and scrambling it with a permutation.

Summary

The potential use of digital watermarks to prevent counterfeiting and forgery is very broad and highly customisable to particular application. Their ability to secure both digital and printed data is important in protecting the complete workflow with minimal impact on current procedures and costs. Digital watermarks also provide detection of high-quality copies of originals. Combined with digital print processes, digital watermarks offer the ability to embed unique codes into individual print items.