Digital Watermarking of Text, Image, and Video Documents

Jonathan K. Su, Frank Hartung, Bernd Girod

Telecommunications Laboratory
University of Erlangen-Nuremberg
Erlangen, Germany
Phone +49 9131 85 27103
Fax +49 9131 85 28849
Email {su,hartung,girod}@nt.e-technik.uni-erlangen.de

The ease of reproduction, distribution, and manipulation of digital documents creates problems for authorized parties that wish to prevent illegal use of such document. To this end, digital watermarking has been proposed as a last line of defense. A digital watermark is an imperceptible, robust, secure message embedded directly into a document. The watermark is imperceptible both perceptually and statistically. Robustness means that the watermark cannot be removed or modified unless the document is altered to the point of no value. The watermark is secure if unauthorized parties cannot erase or modify it. Current watermarking schemes may be viewed as spread-spectrum communications systems, which transmit a message redundantly using a low-amplitude, pseudo-noise carrier signal. An example highlights the basic mechanisms and properties of spread spectrum and their relation to watermarking. Finally, specific issues in watermarking of text, images, and video are discussed, along with watermarking examples.

1 Introduction

Digital media are replacing traditional analog media and will continue to do so. By *digital media*, we mean digital representations of audio, text documents, images, video, three-dimensional scenes, etc. These media offer many benefits over their analog predecessors (e.g., audio and video cassettes). Unlike analog media, digital media can be stored, duplicated, and distributed with no loss of fidelity. Digital media can also be manipulated and modified easily.

Clearly, digital media offer many benefits, but they also create problems for parties who wish to prevent illegal reproduction and distribution of valuable digital me-

dia (e.g., copyrighted, commercial, privileged, sensitive, and/or secret documents). Two classic methods for protecting documents are *encryption* and *copy protection*. However, once decrypted, a document can be copied and distributed easily, and copy-protection mechanisms can often be bypassed.

As a safeguard against failures of encryption and/or copy protection, *digital watermarking* has been proposed as a "last line of defense" against unauthorized distribution of valuable digital media [1,2]. A digital watermarking system embeds information *directly into a document*. For example, information about copyrights, ownership, timestamps, and the legitimate receiver could be embedded. Digital watermarking cannot by itself prevent copying, modification, and re-distribution of documents. However, if encryption and copy protection fail, watermarking allows the document to be traced back to its rightful owner and to the point of unauthorized use.

2 Digital Watermarking

Digital watermarking requires elements from many disciplines, including signal processing, telecommunications, cryptography, psychophysics, and law. In this paper, we focus on the process of embedding and retrieving watermarks in formatted text documents, images, and video. We therefore emphasize the signal processing and telecommunications aspects of watermarking. Because digital watermarking is a fairly new topic, unless watermarks can be reliably inserted and recovered, higher-level issues such as protocols are moot.

An effective watermark should have several properties, listed below, whose importance will vary depending upon the application.

Robustness. The watermark should be reliably detectable after alterations to the marked document. Robustness means that it must be difficult (ideally impossible) to defeat a watermark without degrading the marked document severely—so severely that the document is no longer useful or has no (commercial) value.

Imperceptibility or a low degree of obtrusiveness. To preserve the quality of the marked document, the watermark should not noticeably distort the original document. Ideally, the original and marked documents should be perceptually identical.

Security. Unauthorized parties should not be able to read or alter the watermark. Ideally, the watermark should not even be detectable by unauthorized parties.

Fast embedding and/or retrieval. The speed of a watermark embedding algorithm is important for applications where documents are marked "on-the-fly" (i.e., when they are distributed). The large bandwidth necessary for video also requires fast embedding methods. However, since ownership disputes will likely take weeks or months to resolve, a watermark recovery algorithm may empha-

size reliable detection over speed.

No reference to original document. For some applications, it is necessary to recover the watermark without requiring the original, unmarked document (which would otherwise be stored in a secure archive).

Multiple watermarks. It may also be desirable to embed multiple watermarks in a document. For example, an image might be marked with a unique watermark each time it is downloaded.

Unambiguity. A watermark must convey unambiguous information about the rightful owner of a copyright, point of distribution, etc. This requirement is a cryptographic and protocol issue [3–6] and not covered in this paper.

Of these properties, robustness, imperceptibility, and security are usually the most important. When speaking of robustness, we often talk about *attacks* on a watermark. An attack is an operation on the marked document that, intentionally or not, may degrade the watermark and make the watermark harder to detect. For text documents, an attack might consist of photocopying. For images and video, compression (e.g., JPEG or MPEG), filtering, cropping, resizing, and other signal processing manipulations (even printing and rescanning) must not destroy the watermark.

Digital watermarking can, and should, be viewed as a communications problem [7–9]. Figure 1 provides a block diagram of this interpretation. An authorized party wishes to transmit a digital *message* (e.g., copyright, ownership, or timestamp information) through a hostile and extremely noisy communications channel. The document thus acts like noise, and attacks introduce additional distortions. In a well-designed watermarking system, watermark recovery should not require the original document, which is treated as interfering noise.

From the communications viewpoint, a watermark can be defeated in two ways: *erasure/alteration* and *jamming*. In this first case, an attacker estimates a portion of the watermark and removes or alters enough of it so that it cannot be reliably detected. The second case, jamming refers to document alterations that do not remove the watermark but make it more difficult to detect.

In some scenarios, it is desired to distribute the same document and embed a different watermark in each copy. With many marked versions of the same document, an attacker can conduct another type of attack called a *collusion attack* [17]. Items that differ between marked documents are known to be watermark components. Methods for preventing such attacks appear in [18].

3 Spread-Spectrum Embedding and Recovery

Specific techniques for embedding watermarks differ, depending on the type of document (e.g., text, image, or video). However, most current watermarking meth-

ods [2,10–13] can be interpreted—sometimes very loosely—as forms of spread-spectrum communications, or simply *spread spectrum* (SS) [14,15]. Spread spectrum has been studied for years for both military and civilian applications. We present an example of a SS system and then highlight the properties that make SS useful for watermarking.

3.1 An Example Spread-Spectrum System

We now present a discrete-time example [1] of a common form of SS known as *direct-sequence spread spectrum* (DSSS). Although highly simplified, the example is sufficient to convey the basic mechanisms and principles of SS. Even though this example deals with one-dimensional signals, it extends directly to multi-dimensional signals such as images as well.

Transmission (Watermark Embedding). We begin with a *digital message*, represented by a sequence of bits $b_0 b_1 b_2 \cdots$, where each bit may be either $+1$ or -1. The message contains the information that we wish to embed as a watermark. For transmission (i.e., watermark embedding), each message bit b_i is first repeated N times [2] to produce a redundant message $m[n]$. For example, if $N = 3$, then $m[n]$ is the sequence $b_0 b_0 b_0 b_1 b_1 b_1 b_2 b_2 b_2 \cdots$.

Next, the repeated message $m[n]$ is modulated by a carrier signal $c[n]$ and scaled by a factor $\sqrt{E/N}$. Hence, the transmitted signal is $s[n] = \sqrt{E/N}\, m[n] c[n]$; this signal is embedded as a watermark. Figure 2 gives a block diagram of the embedding process.

For watermarking, $s[n]$ is transmitted (embedded) by mapping $s[n]$ into changes in the original document. For example, in text watermarking, $s[n]$ could be used to perturb line spacings. In image watermarking, $s[n]$ might be added directly to pixel values or transform coefficients.

The Spreading Sequence. The carrier $c[n]$ is called the *spreading sequence*, and it has several special properties:

$$c[n] \in \{+1, -1\}, \quad \text{for any } n; \tag{1}$$

$$\sum_{n=0}^{N-1} c[n] c[n + Ni] = N, \quad \text{for any } i; \tag{2}$$

[1] Spread spectrum is usually presented in a continuous-time framework. For digital watermarking, the signals are discrete-time, but the main concepts and results are the same as for continuous time.

[2] N is known as the "chip rate."

$$\frac{1}{N}\sum_{n=0}^{N-1} c[n] = 0; \tag{3}$$

$$\frac{1}{N}\sum_{n=0}^{N-1} c[n]c[n+k] = \delta[k], \quad \text{for } 0 \le k \le N-1. \tag{4}$$

In practice, these properties can be closely approximated, so we assume equality holds. Equation (1) means that $c[n]$ is binary-valued, although non-binary (e.g., Gaussian-distributed) sequences are also possible. Equations (2), (3), and (4) are referred to as the periodicity, zero-mean, and (periodic) autocorrelation properties, respectively.

The statistical behavior of $c[n]$ is similar to that of noise, although $c[n]$ is not a random process. For security reasons, $c[n]$ should be easy to generate with the proper *key*, but without the key, it should be difficult to reconstruct the complete signal $c[n]$ from only a short segment of it. Signals with these properties are known as *pseudo-noise signals*.

The Watermark Channel. After transmission (embedding), $s[n]$ passes through a channel, which introduces various types of interference. The interference is typically modeled as *additive white Gaussian noise* (AWGN) $v[n]$ with variance σ_v^2/N. The received signal is thus $r[n] = s[n] + v[n]$. The channel (and receiver) are diagrammed in Figure 3.

In watermarking, $v[n]$ includes interference from the original document, as well as attacks. An example of a text-document attack is printing and photocopying. Image and video watermarks could be subject to attacks such as compression with JPEG or MPEG, respectively. Although actual do not conform to the AWGN model, the receiver can use pre-filtering to remove most of the correlated noise introduced by the original image [16]. For simplicity, we use the AWGN model in this discussion, although more sophisticated attacks are possible [17,19].

Reception (Watermark Recovery). Given $r[n]$, a receiver (see Figure 3) attempts to determine the message that was transmitted (i.e., recover the watermark). The receiver is assumed to have its own copy of the spreading sequence $c[n]$ and to be synchronized with the transmitter. The receiver uses a *correlation detector*, which computes $\rho_i = \sqrt{E/N}\sum_{n=0}^{N-1} r[n-Ni]c[n]$ for each i. From the properties of $c[n]$, we find that $\rho_i == Eb_i + \sqrt{E/N}\sum_{n=0}^{N-1} v[n]c[n]$. If $\rho_i \ge 0$, the receiver decides $\hat{b}_i = +1$; otherwise, the receiver decides $\hat{b}_i = -1$.

One measure of performance is the *signal-to-noise ratio* (SNR), which in this case is $\text{SNR}_{\text{std}} = E/\sigma_v^2$. Another measure is the *probability of error* (P_E), which is the probability that $\hat{b}_i$ is incorrectly received ($\hat{b}_i = -b_i$). For this scenario, $P_{E,\text{std}} = Q\left(\sqrt{E/\sigma_v^2}\right)$, where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-y^2/2}\,dy$.

For AWGN with unlimited power, SS performs no better than other modulation schemes. However, when the AWGN power σ_v^2/N is limited, SS has several advantages, discussed below.

Imperceptibility. Note that $|s[n]| = \sqrt{E/N}$ for all n. By choosing N sufficiently large, $\sqrt{E/N}$ can be made as small as desired, but the total power over N samples remains E. The watermark can thus be transmitted (embedded) with a large total power E via many low-amplitude changes.

It can be shown that the power spectrum of $s[n]$ is $\Phi_{ss}(e^{j\omega}) = E$, which means that $s[n]$ behaves like white noise. There is no peak in the spectral domain to indicate to an unauthorized observer that transmission (embedding) has taken place. These abilities allow a watermark to be *imperceptible* [3].

Security. Without the spreading sequence $c[n]$, it is impossible to recover the embedded message $m[n]$. Because $s[n]$ behaves like white noise and has low amplitude, an attacker will have great difficulty estimating $c[n]$ from the marked document. Even if the attacker can estimate a portion of $c[n]$, its pseudo-noise properties make it difficult to determine the entire spreading sequence $c[n]$. Therefore, the watermark is *secure*.

Robustness. An attacker does not know what elements of a marked document were altered by $s[n]$; nor does he or she know the values of $s[n]$. Therefore, to jam the watermark, the attacker must alter *every* element of the marked document. However, the attacker cannot alter the marked document excessively; otherwise, the attacked document will no longer be valuable.

Knowledge of $c[n]$ gives a SS receiver a power advantage against limited-power jamming. This advantage is called the *processing gain*, $G_p = N$. With appropriate processing, the receiver has an effective SNR of $\text{SNR}_{\text{proc}} = G_p \text{SNR}_{\text{std}}$, or an effective P_E of $P_{E,\text{proc}} = Q\left(G_p\sqrt{E/\sigma_v^2}\right)$. For sufficiently large values of N, the watermark is *robust* [4] against attacks. Additional robustness can be achieved by using *error control coding* (ECC) rather than directly modulating the original message $b_0 b_1 b_2 \cdots$.

Multiple Watermarks. It is possible to extend the example to consider multiple messages $m_k[n]$ and pseudo-noise sequences $c_k[n]$. The sequences can be designed to be mutually orthogonal, i.e., $\sum_{n=0}^{N-1} c_k[n]c_\ell[n] = 0$, for $k \neq \ell$. The orthogonality property allows each message $m_k[n]$ to be embedded and recovered independently of the others. For watermarking, it means that multiple watermarks can be employed.

[3] In SS literature, this property is known as "low probability of intercept" (LPI).

[4] This is the "antijamming" property of SS.

The SNR and P_E of a SS system measure its robustness. For fixed σ_v^2, the SNR and P_E improve as the embedding power E and chip rate N are increased. However, if $\sqrt{E/N}$ becomes too large, it becomes less likely that the watermark will remain imperceptible. If $c[n]$ is poorly chosen, an attacker may even be able to reconstruct $c[n]$. Also, as N increases, the number of message bits that can be embedded decreases. A watermarking algorithm must thus balance robustness, imperceptibility, and security against the desired message length.

In the example, the receiver was assumed to be synchronized with the transmitter. Because of the autocorrelation property (4), if the receiver and transmitter are not synchronized, the receiver will not be able to recover the message $m[n]$. A sliding correlation detector can be used to regain synchronization by computing the correlation between $r'[n] = r[n - n_0]$ and $c[n - \Delta n]$ for various values of Δn. When $\Delta n \neq n_0$, only small values will result; when $\Delta n = n_0$, a large value will occur, and synchronization is re-acquired. The sliding correlator can be modified to operate in a blockwise or similar fashion. In this way, attacks that rearrange or interchange small parts of a document can be resisted.

4 Watermarking Examples

This section presents examples of watermarking methods for text, images, and video. These media differ in ways that present unique problems for watermarking, but the principle of watermarking remains that of embedding a redundant message via many low-amplitude, pseudo-noise modifications of the original document.

4.1 Text Watermarking

Many paper documents (e.g., contracts, wills, etc.) are more valuable than multimedia like sound clips and images. Digital libraries and archives distribute copyrighted articles, journals, and books in electronic form. Watermarking of text documents provides a means of tracing documents that have been illegally copied, distributed, altered, or forged.

Raw text, such as an ASCII text file or computer source code, cannot be watermarked because there is no "perceptual headroom" in which to embed hidden information. However, final versions of documents are typically formatted (e.g., PostScript, PDF, RTF), and it is possible to hide a watermark in the layout information (e.g., word and line spacings) and formatting (e.g., serifs). Although *opti-*

cal character recognition (OCR) can theoretically remove any layout information, OCR is expensive, imperfect, and often requires manual supervision.

Brassil *et al.* [20–22] have investigated text watermarking and proposed a variety of methods for embedding hidden messages in PostScript documents. The work of Brassil *et al.* currently does not use SS embedding, but it could be added to the system to strengthen robustness and security.

In [20–22], the message is embedded by altering different parts of the document. Line shifting moves entire lines of text up or down by a small amount, typically 1/150 or 1/300 inch (0.170 or 0.085 mm). Similarly, word shifting may horizontally shift individual words or blocks of words; words at the ends of a line are not shifted to preserve justification. Figure 4 provides an example of word shifting. Finally, feature coding modifies small parts of characters themselves.

Recovery of the message from a printed or photocopied document requires a number of post-processing steps (scanning, skew correction, and noise removal). After post-processing, the message receiver automatically measures line shifts, word shifts, and/or feature alterations to detect the message.

In experiments, these methods have shown promise. Line shifts could be correctly detected even after photocopying ten times. Word shifts on a single page were correctly detected 75 percent of the time, after photocopying four times or after fax transmission. With simple ECC, 26–30 of 30 embedded message bits per page could be decoded, depending upon the amount of degradation (e.g., photocopying multiple times).

4.2 Image Watermarking

Digital images can be produced from many sources, such as everyday photographs, satellite pictures, medical scans, or computer graphics. Watermarks for natural images typically modify pixel intensities or transform coefficients, although it is conceivable that a watermark could alter other features such as edges or textures.

An image may be viewed for an extended period of time, and it may also be subject to a great deal of manipulation, such as filtering, cropping, geometric transformations, compression, and compositing with other images, and hostile attacks. Thus, imperceptibility, robustness, and security are usually the most important properties of image watermarks; speed and complexity are often secondary. Also, since many images are compressed (e.g., JPEG or GIF), watermarking algorithms that operate in the transform or wavelet domain may be useful.

One potential difficulty in image watermarking is the finite bandwidth available. As the image size decreases, the permissible message length decreases unless E is

increased (weakening imperceptibility) or N is decreased (weakening robustness).

The example watermarking system in Figures 2 and 3 has been directly developed into a system that embeds a spatial-domain DSSS image watermark. Figure 5 compares an original, unmarked image with its watermarked counterpart. The two images are indistinguishable perceptually. The original image is a 256×256 8-bit grayscale image. The watermark was embedded a chip rate of $N = 4096$ and per-pixel amplitude $\sqrt{E/N} = 2$. Hence, the total power per message bit was $E = 16384$.

The marked image was then subjected to a number of different attacks. Example marked images after attack appear in Figure 6. The watermark message remained recoverable after addition of Gaussian noise with variance 400, a sinusoidal pattern with amplitude 30, and a constant offset of 30. The watermark also survived JPEG compression with a quality factor of 20 percent (compressed to 4959 bytes, or 13:1 compression).

A free software program called StirMark [19,23] is available for testing watermark robustness. StirMark simulates printing and rescanning of an image, and its producers claim that it can defeat several commercial watermarking systems. The SS watermark, however, survived StirMark and the embedded message was recovered without any bit errors.

4.3 Video Watermarking

Digital video is a sequence of still images, and many image watermarking techniques can be extended to video in a straightforward manner. In contrast to single images, the large video bandwidth means that long messages can be embedded in video. Speed is also an important issue because of the huge amounts of data that must be processed. Except for video production (which takes place before distribution), digital video is typically stored and distributed in compressed form (e.g., MPEG). Hence, it is often desired that the marked, compressed video should not require more bandwidth than the unmarked, compressed video. This bit-rate constraint could also be an issue for single images. Compressed-domain video watermarking is especially attractive. Operating on the compressed bitstream obviates the need for compute-intensive, time-consuming decompression and recompression, such that the watermark can be embedded at the time of distribution or reception.

An example of a compressed-domain video watermarking system is briefly described here; a more thorough treatment appears in [24,25]. This system operates on video compressed using the MPEG-2 compression standard [26].

MPEG-2 uses *block motion compensation* (BMC) to indicate movement and block

discrete cosine transform (DCT) compression to describe the residual error after BMC. This is known as a hybrid video compression system. In BMC, decompressed image blocks available to both the encoder and decoder are translated to new positions to form an approximation of the current video frame being transmitted. The difference between the original current frame and the approximation formed via BMC is the residual error. In block DCT compression, the residual error image is divided into 8×8 blocks. Each block is transformed, and the DCT coefficients are quantized. Typically, most of the quantized DCT coefficients are zero, so only non-zero quantized DCT coefficients must be transmitted.

The example watermarking system operates on the MPEG-2 bitstream as shown in Figure 7. The system does not alter the motion vectors or any side information contained in the bitstream. The system embeds a spatial-domain DSSS watermark in each video frame and must decode only the block-DCT portion of the bitstream. The system computes the DCT of each 8×8 block of the spatial-domain watermark and adds it to the corresponding decoded block DCT. To preserve compression efficiency, the watermark is only added to the non-zero coefficients in the decoded block DCT. Because MPEG-2 includes predictive compression, watermarks that were embedded in preceding frames could propagate into the current frame and create visible distortion. The drift compensation signal accounts for these previously embedded watermarks and removes them from the current frame.

Finally, if a bit-rate constraint is desired, an additional step is required. Let n_0 denote the number of bits for the compressed, unmarked DCT coefficient and n_1 denote the number of bits for the compressed, watermarked DCT coefficient. If $n_1 \leq n_0$, the watermarked coefficient replaces the unmarked coefficient in the bitstream. If $n_1 > n_0$, however, the unmarked coefficient is left unchanged.

Thus, only non-zero DCT coefficients are altered, and some of these changes may be negated due to the bit-rate constraint. Figure 8 shows example frames. Only a small portion of the watermark is actually embedded; sometimes as much as 90 percent of the watermark may be discarded. However, the chip rate N can be made very large to ensure that it is possible to recover the watermark that was actually embedded. For video of reasonable duration, a watermark data rate of a few bytes per second is sufficiently high. The system presented here has low complexity compared to MPEG-2 compression.

5 Conclusions

We have presented a basic introduction to digital watermarking of text, image, and video documents. Watermarking embeds ownership information directly into the document, and it is proposed as a "last line of defense" against unauthorized distribution of digital media. Desirable properties of watermarks include imperceptibil-

ity, robustness, and security. From a communications viewpoint, most watermarking systems are similar to spread-spectrum communications. Spread spectrum watermarking uses a redundant message that is transmitted via many low-amplitude, noise-like modifications to a document. A number of examples showed how watermarking has been implemented for text, image, and video watermarking. Each type of document presents unique problems for embedding and recovery. The success of these methods encourages the development of more sophisticated watermarking algorithms as part of a larger system for protecting valuable digital documents.

References

[1] van Schyndel, R. G., Tirkel, A. Z., and Osborne, C. F., A digital watermark. *Proceedings of the 1994 IEEE International Conference on Image Processing*, 1994, **2**, pp. 86–89.

[2] Cox, I. J. Kilian, J., Leighton, T., and Shamoon, T., Secure spread spectrum watermarking for images, audio, and video. *Proceedings of the 1996 IEEE International Conference on Image Processing*, 1996, **3**, pp. 243–256.

[3] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M. M., On the invertibility of invisible watermarking techniques. *Proceedings of the 1997 IEEE International Conference on Image Processing*, 1997, **1**, pp. 540–543.

[4] Zeng, W., and and Liu, B., On resolving rightful ownerships of digital images by invisible watermarks. *Proceedings of the 1997 IEEE International Conference on Image Processing*, 1997, **1**, pp. 552–555.

[5] Wolfgang, R. B., and Delp, E. J., A watermarking technique for digital imagery: Further studies. *Proceedings of the International Conference on Imaging Science, Systems, and Technology*, 1997, Las Vegas, pp. 279–287.

[6] Qiao, L., and Nahrstedt, K., Watermarking schemes and protocols for protecting rightful ownership and customer's right. Submitted to *Academic Press Journal of Visual Communication and Image Representation*, 1998.

[7] Smith, J. R., and Comiskey, B. O., Modulation and information hiding in images. *Proceedings of the First Information Hiding Workshop*, Cambridge, U. K., May 1996.

[8] Ó Ruanaidh, J. J. K., Dowling, W. J., and Boland, F. M., Watermarking digital images for copyright protection. *IEE Proceedings on Vision and Image Signal Processing*, 1996, **143**, 250–256.

[9] Hernández, J. R., Pérez-González, F., and Rodr´guez, J. M., The impact of channel coding on the performance of spatial watermarking for copyright protection, *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1998.

[10] Ó Ruanaidh, J. J. K., and Pun, T., Rotation, scale, and translation invariant digital image watermarking. *Proceedings of the 1997 IEEE International Conference on Image Processing*, 1997, **1**, pp. 536–539.

[11] Xia, X.-G., Boncelet, C. G., and Arce, G. R., A multiresolution watermark for digital images, *Proceedings of the 1997 IEEE International Conference on Image Processing*, 1997, **1**, pp. 548–551.

[12] Swanson, M. D., Zhu, B., Chau, B., and Tewfik, A. H., Multiresolution video watermarking using perceptual models and scene segmentation. *Proceedings of the 1997 IEEE International Conference on Image Processing*, 1997, **2**, pp. 558-561.

[13] Piva, A., Barni, M., Bartolini, F., and Cappellini, V., DCT-based watermark recovering without resorting to the uncorrupted original image. *Proceedings of the 1997 IEEE International Conference on Image Processing*, 1997, **1**, pp. 520–523.

[14] Pickholtz, R. L., Schilling, D. L., and Milstein, L. B., Theory of spread-spectrum communications—A tutorial. *IEEE Transactions on Communications*, 1982, **COM-30**, 855–884.

[15] Flikkema, P. G., Spread-spectrum techniques for wireless communications. *IEEE Signal Processing Magazine*, 1997, **14**, 26–36.

[16] Hartung, F., and Girod, B., Digital Watermarking of Raw and Compressed Video. *Proceedings of the European EOS/SPIE Symposium on Advanced Imaging and Network Technologies*, Berlin, Germany, Oct. 1996.

[17] Stone, H. S., Analysis of attacks on image watermarks with randomized coefficients. NEC Technical Report, May 1996.

[18] Boneh, D., and Shaw, J., Collusion secure fingerprinting for digital data. *Proceedings of Crypto '95*, 1995, Springer LNCS 963, pp. 452–465.

[19] Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G., Attacks on copyright marking systems. *Proceedings of the Second Workshop on Information Hiding*, Portland, Oregon, USA, Apr. 1998.

[20] Brassil, J., Low, S., Maxemchuk, N., and O'Gorman, L., Electronic marking and identification techniques to discourage document copying. *Proceedings of IEEE INFOCOM '94*, 1994 **3**, pp. 1278–1287.

[21] Low, S., Maxemchuk, N., Brassil, J., and O'Gorman, L., Document marking and identification using both line and word shifting. *Proceedings of IEEE INFOCOM '95*, 1995.

[22] Brassil, J., Low, S., Maxemchuk, N., and O'Gorman, L. Hiding information in document images. *Proceedings of the 29th Annual Conference on Information Sciences and Systems*, 1995, pp. 482-489.

[23] Petitcolas, F. A. P., *StirMark*, vers. 1.0. URL `http://www.cl.cam.ac.uk/fapp2/watermarking/image_watermarking/stirmark/`, 1998.

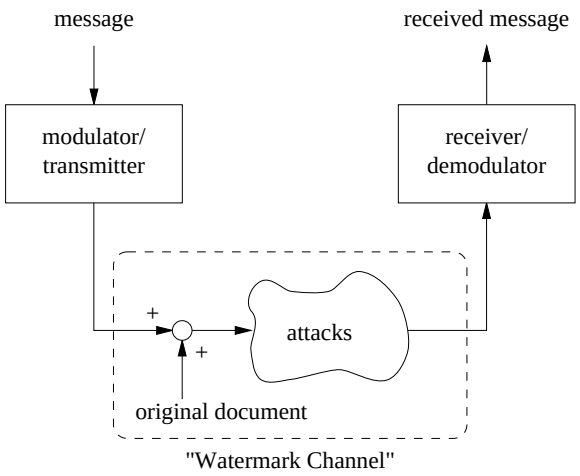

Fig. 1. Communications model of watermarking.

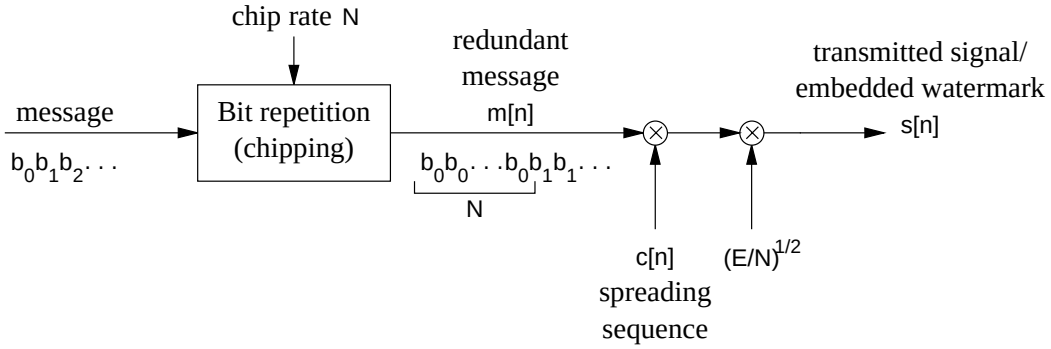

Fig. 2. Spread spectrum watermark embedding example.

[24] Hartung, F., and Girod, B., Digital watermarking of MPEG-2 coded video in the bitstream domain. *Proceedings of the 1997 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1997, **4**, pp. 2621–2624.

[25] Hartung, F., and Girod, B., Watermarking of uncompressed and compressed video. *Signal Processing*, 1998, **66**, 283–301.

[26] ISO/IEC 13818-2, *Generic Coding of Moving Pictures and Associated Audio, Recommendation H.262 (MPEG-2)*, International Standard, 1995.

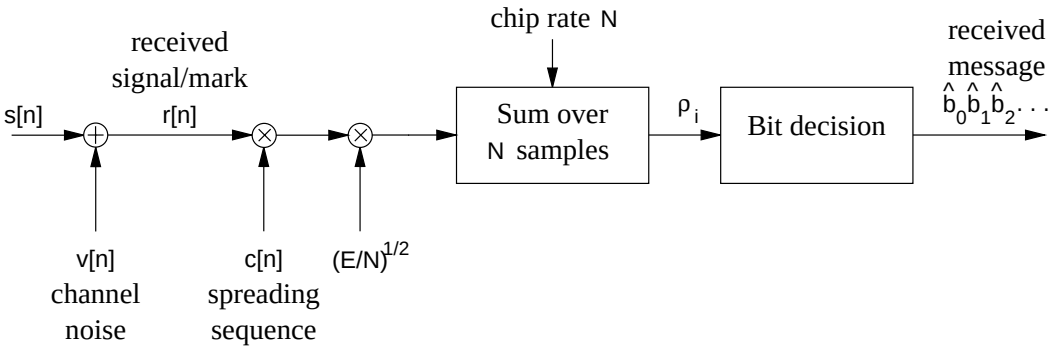

Fig. 3. Spread spectrum watermark recovery example.

Recovery of the watermark from a printed or photocopied document

Recovery of the watermark from a printed or photocopied document

Recovery of the **watermark** from a **printed** or **photocopied** document

Fig. 4. Example of word shifting. The shift is exaggerated for the sake of example. Normal text line (top); word-shifted line (middle); overlaid lines to emphasize shift (bottom).

Fig. 5. Example of DSSS image watermarking. Original image (left) and watermarked image (right). Detail of the images appear below the full-size images.

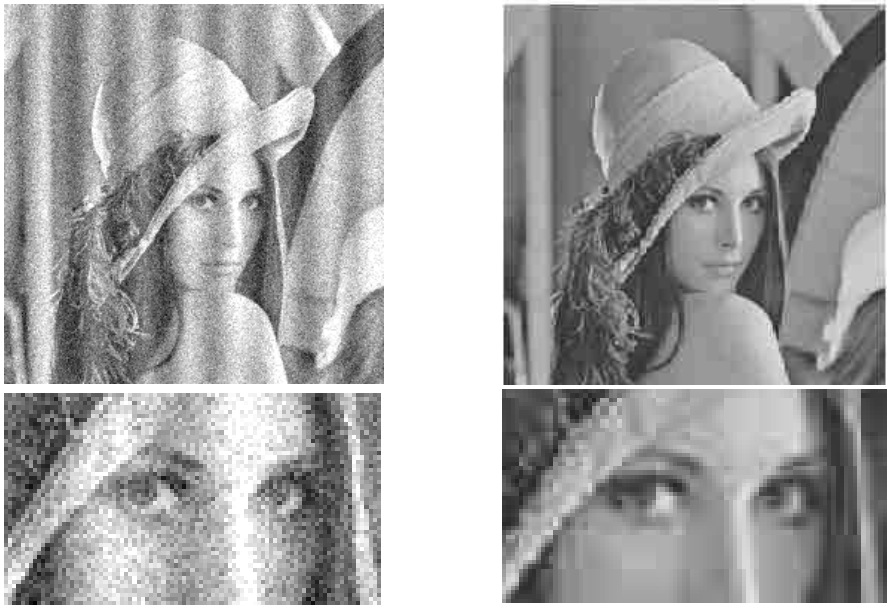

Fig. 6. Example of attacks on DSSS image watermarking. Additive noise (left); JPEG compression (13.2:1 compression) (right). The watermark was recovered in both cases.

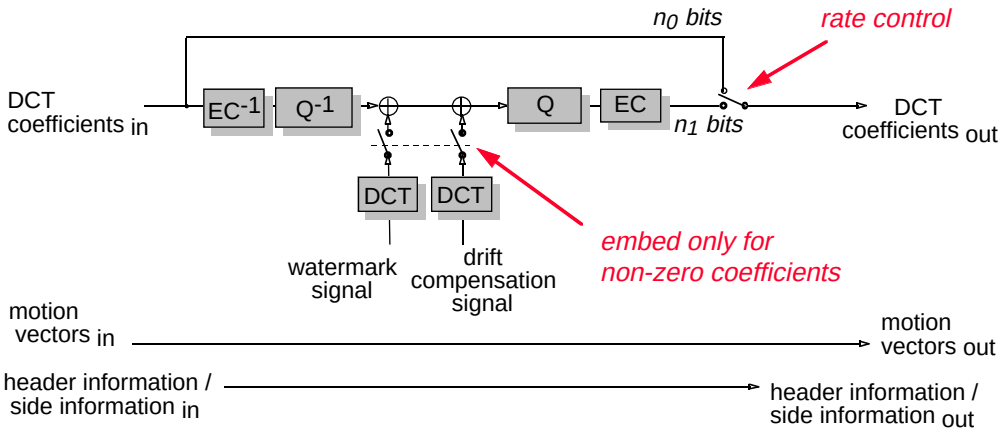

Fig. 7. Compressed-domain MPEG-2 video watermarking system. EC = entropy coding, Q = quantization; a superscript -1 indicates the inverse operation.

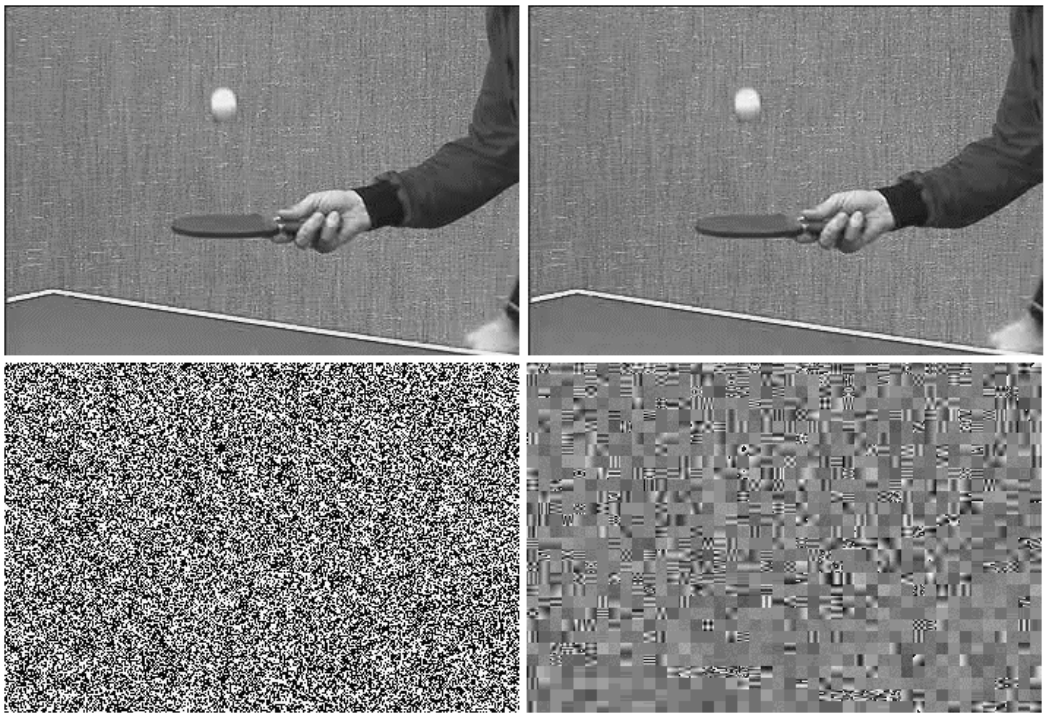

Fig. 8. Comparison of uncompressed video watermarking and compressed-domain video watermarking. Frames on the left show the watermarked frame and the noise-like watermark (in the spatial domain) with all watermarked DCT coefficients. Frames on the right show the same frames after compression with MPEG-2 and compressed-domain watermarking.