Signal Processing 109 (2015) 345–361

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Robustness of Double Random Phase Encoding spread-space spread-spectrum watermarking technique

Shi Liu [a], Bryan M. Hennelly [b], Changliang Guo [a], John T. Sheridan [a,*]

[a] School of Electrical, Electronic and Communication Engineering, College of Engineering and Architecture, Communication and Optoelectronic Research Centre, The SFI-Strategic Research Cluster in Solar Energy Conversion, University College Dublin, Belfield, Dublin 4, Ireland

[b] Department of Electronic Engineering, The Callan Institute, National University of Ireland Maynooth, County Kildare, Ireland

ARTICLE INFO

Article history:
Received 18 November 2013
Received in revised form
16 June 2014
Accepted 25 June 2014
Available online 10 July 2014

Keywords:
Digital image watermarking
DRPE SS-SS
Robustness
Informed detection
Blind detection
Additive spread-spectrum

ABSTRACT

In this paper the robustness of a recently proposed image watermarking scheme, namely the Double Random Phase Encoding spread-space spread-spectrum watermarking (*DRPE SS-SS*) technique, is investigated. The watermark, which is chosen to be in the form of a digital barcode image, is numerically encrypted using a simulation of the optical DRPE process. This produces a random complex image, which is then processed to form a real valued random image with a low number of quantization levels. This signal is added to the host image. Extraction of the barcode, involves applying an inverse DRPE process to the watermarked image followed by low pass filtering. This algorithm is designed to utilize the capability of the DRPE to reversibly spread the energy of the watermarking information in both the space and spatial frequency domains. In this way the energy of the watermark in any spatial or spatial frequency bin is very small. To test robustness several common geometric transformations and signal processing operations are performed using both informed and blind detections for different barcode widths and different quantization levels. The results presented indicate that while the *DRPE SS-SS* method is robust to scaling, and JPEG compression distortion, it is especially robust to spatial cropping and both low and high pass filtering. Both *random-watermark* and *random-host* false positive cases are examined. The uniqueness of the watermark is demonstrated, and it is shown that the *DRPE SS-SS* has very low false positive errors, and that the larger the barcode width, the lower the false positive rate. Finally the effects of both printing and scanning are examined.

1. Introduction

The rapid growth of the modern communication techniques, especially internet usage, has stimulated the development of information security and intellectual property protection techniques [1]. Watermarking, which is defined by the practice of imperceptibly altering a host (carrier signal) to embed a message about that host, has been proposed as an effective way to provide copyright protection and data tracking security for many types of information [2]. Watermarking can be traced back to the steganography technique, which is the science of writing covered messages in such a way that the presence of the messages cannot be detected [3]. In particular, steganographic systems hide information that may have no relation to the host, with the aim of preventing detection by any party other than the sender and intended recipient, allowing both parties to communicate secretly.

* Corresponding author.
E-mail address: John.Sheridan@ucd.ie (J.T. Sheridan).

http://dx.doi.org/10.1016/j.sigpro.2014.06.024
0165-1684/

The information hidden by watermarking systems may be associated with the owner or the digital object to be protected, and watermarking does not necessarily hide the fact of secret transmission of information from a third party [4]. Watermarking can be either "visible" or "invisible" [5,6]. Invisible digital watermarking involves the embedding of an imperceptible signal into a multimedia data object, such as image, audio or video data. The watermark can then be detected (or extracted later) to trace the origins of the object and thus to make an assertion about ownership [7,8]. Although copyright protection has been one of the major driving forces behind watermarking research, there are a large number of proposed or actual applications for which watermarking can be used. These include: broadcast monitoring, owner identification, proof of ownership, transaction tracking, authentication, copy control, device control, and legacy enhancements [2]. In order to be effective, a watermark and its associated detection processes should have several important properties: (i) unobtrusiveness (perceptually invisible, i.e. its presence should not interfere with the host being protected); (ii) robustness (difficult to remove and immune to simple signal processing techniques, common geometric distortions, and subterfuge attacks); (iii) universality (applicable to all three media, i.e. image, audio and video data); and (iv) unambiguousness (unique and retrievable) [9,1].

Digital image watermarking is an emerging technology in signal processing and communications which is under active development. The embedding methods used in the watermarking system influence both the robustness and the detection algorithm. Generally watermarks have been embedded either in the spatial domain or in the transform domain of the host image, referred to as "*spatial watermarking methods*" and "*spread-spectrum* (*SS*) *watermarking methods*" respectively [10]. In the first case, the embedded watermark is equivalent to direct noise addition to the host media and will change the characteristics of the watermarked signal. The least significant bit (LSB) [11] and the singular value decomposition (SVD) [12] methods are two common methods of this type. In the spread spectrum case, the watermark is hidden in the host image's spectrum, commonly using either discrete cosine transform (DCT) [13,14], discrete wavelet transform (DWT) [15], or lifting wavelet transform (LWT) [16]. Cox et al. [9] proposed a classic secure spread-spectrum (SS) watermarking technique for multimedia, commonly known as *additive spread-spectrum* (*additive SS*), involving insertion of a watermark (pseudorandom sequence) into the perceptually most significant components of the image spectrum using the DCT. We note that we will apply this well known method in order to compare robustness performance with our *DRPE SS-SS* scheme in this paper.

Recently, digital watermarking systems based on optically inspired techniques have attracted significant interests, as they offer the possibility of high-speed parallel processing of 2D image data and the possibility of hiding information with many degrees of freedom [17]. One particular optical encryption scheme, the "Double Random Phase Encoding (DRPE)" [18], involves multiplication of the image by random phase diffusers (masks) both in the input (space) and Fourier (spatial frequency) domains. The encrypted image can be shown to be a stationary white noise if the two random phases are statistically independent white noises. The DRPE method has stimulated much research in the areas of optical image and signal processing, and many variations of this approach have been developed with extra security keys and degrees of freedom. Extensions have included replacing the Fourier transform (FT) with the fractional Fourier transform (FRT) [19–22], the Fresnel transform (FST) [23,24] and the Gyrator transform (GT) [25,26]. Such methods have also been previously discussed for use in watermarking [27–30]. It should also be noted that, the watermark information can be complex valued, i.e. generated using a digital holographic technique, and that in this case the watermark can be embedded directly into a weighted host image [31–33] or into a digital hologram of the host image [34]. In addition, optical encryption techniques employing phase retrieval algorithms [35] have also been implemented as part of watermarking systems [36,37]. Interest in this area has not slackened and recently a few optical image encryption techniques, involving speckle pattern interference [38], and tree structured Haar transform [39], have been used in digital watermarking field.

In particular, employing the DRPE technique, a novel digital image watermarking technique named *DRPE SS-SS* was proposed recently [40]. This watermarking technique utilizes the capability of the DRPE method to reversibly spread the energy of the input information in both the space and spatial frequency domains, and can therefore be categorized as being a combination of '*spatial watermarking*" and "*spread-spectrum* (*SS*) *watermarking*" methods. The watermark is in the form of a weak (limiting case 1 bit) statistically random real valued white noise that is added directly to the host image. This watermark information is calculated from a unique barcode image that is numerically encrypted using a simulation of the optical DRPE process. This process transforms the barcode into the random noise like image that has its energy spread both in the space and spatial frequency domains. This encrypted barcode image is then further processed to produce a weak real-valued and quantized noise like image that can be easily added to a digital host image, while remaining hidden and imperceptible. In order to detect the original barcode, a numerical inverse DRPE process is applied to the watermarked image (in the case of blind detection) or the quantized watermark (in the case of informed detection). The barcode can be extracted using a low pass filter, once it has been separated from the speckle noise terms. In order to provide a standard method against which our algorithm can be compared, we briefly review the *additive SS* watermarking architecture [9]. The robustness of *DRPE SS-SS* method is then investigated by examining the following common signal processing and geometric distortions tests: (i) image scaling, (ii) JPEG compression, (iii) cropping distortion, (iv) both low and high pass filtering, and (v) printing and scanning. The false positive errors are also examined using both the *random-watermark false positive* and the *random-host false positive* forms. In all cases our algorithm's performance is compared to that of Cox's *additive SS* watermarking method.

In summary this paper is organized as follows: In Section 2 we briefly discuss the *additive SS* watermarking algorithm. In Section 3 both blind and informed detection procedures are described, and the resulting detection bit error rates (BER) are presented. The workload of our algorithm has also been briefly discussed. In Section 4, using the informed detection the robustness of the *DRPE SS-SS* method to the effects of several common signal processing and geometric distortions are investigated and quantitatively compared. In Section 5, using blind detection the robustness performance of the *DRPE SS-SS* to the corresponding tests is also given. However we note that the *additive SS* method is not comparable in this case since the host image is required for watermark detection. Section 6 provides the results of the study of the uniqueness of our method in terms of the false positive rates. The final section offers a brief conclusion.

2. The structure of the *additive SS* algorithm

We wish to provide a comparison between the performance of our DRPE algorithm and the watermarking technique in common use. To do so we have implemented Cox's well-known additive spread spectrum technique, known as the *additive SS* [9]. This algorithm is one of the most widely known classic watermarking techniques. It is a "*spread-spectrum watermarking*" method since the watermark is embedded into the frequency domain of the host signal. Using the *additive SS*, the watermark is imperceptibly inserted into the perceptually most significant spectral components of the host image using a discrete cosine transform (DCT) operation. Fig. 1(a) schematically illustrates this watermarking process, while Fig. 1(b) describes the watermark detecting process during which it is assumed that the host image is known.

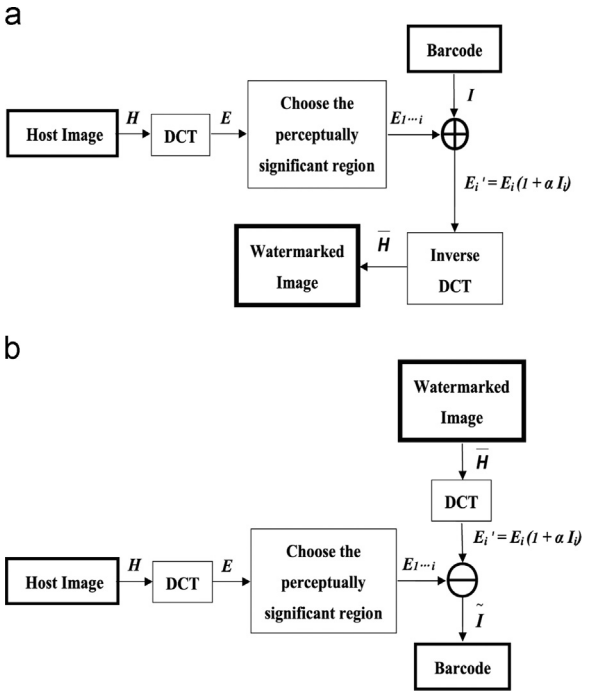

Fig. 1. *Additive SS* algorithm structure: (a) the watermarking process, and (b) and the watermark informed detection process (the host image H is known).

3. Detection of the watermark

For the purpose of investigating the robustness of the *DRPE SS-SS* watermarking algorithm, the watermarking detection and evaluation procedures must be discussed in detail. In this section, two types of watermarking detection algorithms, i.e. blind detection and informed detection, are investigated. In both cases *DRPE SS-SS* results are examined in comparison with the corresponding *additive SS* results.

3.1. Blind detection of the DRPE SS-SS algorithm

Generally, the type of watermarking detection employed depends on the requirements of the watermarking applications [2]. In some applications, the detection process must be applied without access to the original host image, i.e. the *unwatermarked* image. For example, in a copy control application, the detector must be distributed in every consumer recording device. It is thus not practical to distribute the original unwatermarked data to every detector. Such a detection process, that does not require the original host image, is referred to as *"blind detection"*. In the watermarking literature, watermarking systems that use blind detection are generally designated as "*public watermarking systems*".

The procedure for detecting the barcode in a watermarked image involves (i) applying the decryption process ($DRPE_N^{-1}$) to the watermarked image; (ii) applying a low pass filter to the resultant image in order to reduce the noise overlying the barcode image; (iii) removing the zeropadding margins surrounding the barcode to obtain the $M_x \times N_y$ barcode image; and finally in the case of a purely numerical implementation of the method, we finish by (iv) taking the real part only from the extracted image pixel values since the barcode is real valued only. At this point, an appropriate thresholding procedure can be applied. For further information we refer the reader to the Detection Section 5 in Liu et al. [40].

3.2. Informed detection of the DRPE SS-SS algorithm

In some applications of digital watermarking, the original host data is available during the detection procedure. For example, in transaction tracking applications, the owner of the host data usually controls the detector for the purpose of identifying illegally distributed copies. This means that the owner should have access to the unwatermarked data and be able to provide it to the detector along with any possible illegal copy [2]. This type of watermark detection is referred to as *"informed detection"*, and watermarking systems that use informed detection are relatively called "*private watermarking systems*". Informed detection often substantially improves detection performance, since the host image can be subtracted from the watermarked image thereby reducing the degradation of the extracted watermark signal caused by the presence of the dominant host image noise term. In this section,

performing informed detection on the *DRPE SS-SS* watermarking algorithm is discussed. Access to the original host image simplifies the detection process and can also be used to counteract any temporal or geometric distortions that the watermarked image may have undergone. We will discuss this in later sections.

As discussed in Liu et al. [40], during an informed detection process, the host image is first subtracted from the watermarked image $\overline{H}$ to obtain the quantized watermark E_{Q_I}. Then the detection algorithm is applied to the watermark E_{Q_I}. Low pass filtering then extracts $\tilde{I}$ and reduces the speckle noise, eliminating the decryption of $E^*(n_x, n_y)$ and the resulting quantization noise $q_I(n_x, n_y)$. Then the zeropadding margins around the barcode are removed. Finally only the real part of the extracted image is retained and following the thresholding, the detected 1D barcode image is obtained.

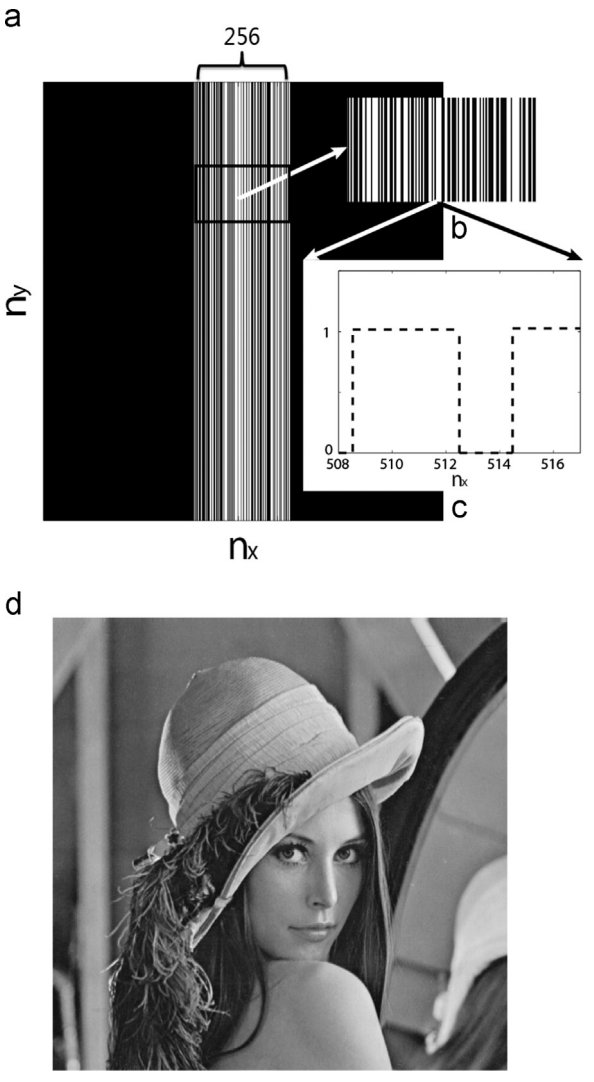

Fig. 2. The illustrations of the watermark and the host image: (a) the barcode image, $I(n_x, n_y)$, where M_x=256 and $N_x = N_y = 1024$; (b) magnified barcode image in a particular region; (c) part of the 1D signal integrated over n_y, where $508 \le n_x \le 517$ and $n_x \in [1, N_x]$; (d) the host image.

3.3. Detection simulation results

In this section, the simulation watermark detection results for different quantization levels and different barcode widths are presented. The barcode watermark of width $W_{Ix} = 256$ is shown in Fig. 2(a). Fig. 2(b) illustrates a magnified barcode image in a particular region. In Fig. 2(c), we show the pixels in the range: $508 \le n_x \le 517$ where 0 corresponds to the black and 1 corresponds to the white in the barcode image. Fig. 2(d) presents the host image, the "Lena" image [41], with $N_x = N_y = 1024$. The detection bit error rate (BER) is calculated to examine performance of the *DRPE SS-SS* method, see Section 5.2 in Liu et al. [40]. We note that throughout this paper we assume that the acceptable value of BER is zero (i.e. BER=0), which represents perfect detection with no errors.

Table 1 lists the *blind detection* BER results for simulations using the *DRPE SS-SS* method with different barcode widths, i.e. $W_{Ix} = 16$, 32, 64, 128, and 256, and different quantization levels, i.e. 2-, 4-, 8-, and 16-level. The narrower the barcode width and the larger the number of quantization levels used, the more accurate the detection process (fewer errors). When $W_{Ix} = 16$, perfect detections with no errors, are achieved in all cases. Such results indicate the feasibility of the proposed *DRPE SS-SS* algorithm.

In order to extract the original barcode using the *additive SS* algorithm, the host image is required to identify the embedding location among the DCT coefficients [42]. This means that the *additive SS* algorithm is not applicable for blind detection [9], and our attempts to detect the original barcode without access to the host image have proved unsuccessful. To the best of our knowledge, following a detailed literature search, blind detection for Cox's

Table 1
The calculated *blind detection* BER (%) percentage for different barcode widths (W_{Ix}) and different numbers of quantization levels (I).

W_{Ix}	Quantization level (I)			
	2-Level	4-Level	8-Level	16-Level
16	0	0	0	0
32	9.3750	6.2500	0	0
64	21.8750	15.6250	7.1250	0
128	29.6875	22.4375	12.5000	3.1250
256	32.0313	26.5625	19.5313	7.8125

Table 2
The calculated *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (I) using both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS−SS*			
		2-Level	4-Level	8-Level	16-Level
16	0	0	0	0	0
32	0	0	0	0	0
64	0	0	0	0	0
128	0	5.4688	4.6875	3.9063	3.9063
256	0	20.3125	19.1406	18.75	17.9688

method is not discussed in the literature. Therefore, we draw the conclusion that the *DRPE SS-SS*, unlike the *additive SS*, can be used in the blind detection case. The *DRPE SS-SS* method therefore has a wider range of applications than Cox's method.

Table 2 lists the *informed detection* BER results for simulations using both different barcode widths, i.e. $W_{lx}=16$, 32, 64, 128, and 256, and different quantization levels, i.e. the 2-, 4-, 8-, and 16-level cases. These results are calculated in both the *DRPE SS-SS* and *additive SS* cases using the same barcode and host image.

We note that all the simulations of the *additive SS* method presented here employ a scaling parameter value of $\alpha=0.1$, which is the same as that used by Cox et al. [9]. However, given the significant differences between the two algorithms further justification of the parameter value chosen is necessary. In order to provide a fair comparison when a barcode watermark is used, the influence (effect) of the watermark after embedding in the host image is quantified by examining the difference caused by the presence of the watermark, i.e. by subtracting the host image from the watermarked image as follows:

$$E_{watermark}=\sum_{i=1}^{N_x\times N_y}|\overline{H}_i-H_i|^2, \tag{1}$$

where $E_{watermark}$ quantifies the effect of the resulting residual image. Interestingly our simulations indicate that $E_{watermark}$ for both watermarking algorithms is comparable in size when $\alpha=0.1$, i.e. in both cases $E_{watermark}$ is approximately equals to 4.4e+4. This provides some validation of our choice of the α value used in our simulations.

To calculate the BER for the *additive SS* method a threshold value of 0.5 is used to bin the detected sequence into the binary barcode sequence. As can be seen in Table 2, the informed detected BER is 0 for all the barcode widths examined, i.e., perfect detection is possible in all cases for all the different barcode lengths. On the other hand for the *DRPE SS-SS*, once again as in the case of blind detection, perfect detection takes place when $W_{lx}=16$ for all four quantization levels. However it now also occurs for when $W_{lx}=32$ and 64. Therefore the *additive SS* and the *DRPE SS-SS* perform equally well until wider, i.e. $W_{lx}=128$ and 256, barcodes are used. Furthermore, in the case of informed detection, better detection performance is in general achieved than for the corresponding blind detection case and this is because the host image speckle noise term is no longer present in the detected barcode image in the informed case.

The workload of the encoder refers to the number of bits where a watermark encodes within the host image [2]. A watermark that encodes N bits is referred to as an N-bit watermark. In this paper, in order to provide perfect detection, the workload can be calculated based on the detected BER results shown in Tables 1 and 2. Table 3 summarizes the workloads for different quantization levels and both informed and blind detection. As can be seen, the workload increases with the quantization level when blind detection is performed. In comparison, in the informed detection case, the workloads are equal and of value 64 indicating that higher workloads are in general possible in this case. Furthermore, we note that our *DPRE SS-SS* method when used to process a watermarked Lena image (Fig. 2(d) $N=1024$) with a DELL computer (CPU 3.3 GHz and Internal Memory 4 GB) required 5 s and 4.5 s for encoding and detection (both informed and blind) respectively.

Table 3
The workload of the *DRPE SS-SS* algorithm.

DRPE SS−SS	**Quantization level (*I*)**			
	2-Level	**4-Level**	**8-Level**	**16-Level**
Blind detection	16	16	32	64
Informed detection	64	64	64	64

4. Informed detection robustness

As noted the *DRPE SS-SS* technique utilizes the capability of the DRPE to reversibly spread the energy of the input watermark information in both the space and spatial frequency domains. The energy of the watermark is spread over every space and frequency bin so that the energy in any spatial or frequency bin (pixels) will be very small, thus reducing the impact of the watermark. Therefore the *DRPE SS-SS* method should not only make the watermark imperceptible, but also provide robustness to many common signal and geometric distortions. In order to demonstrate the robustness of our method, in this section we examine the effects of the following operations: (i) image scaling; (ii) JPEG compression distortion; (iii) image cropping; (iv) image filtering in the frequency domain; and (v) image printing (hard copy output) and image scanning distortions. In each case the effects of using different barcode widths and quantization levels to perform the informed detection are presented. It is worth noting that following each of these distortions, the effect of the speckle noise terms overlaying the watermarked image [40] will be reduced significantly due to the use of the low pass filtering operation and therefore contributes little to the extracted barcode information. For the purposes of comparison, the corresponding *additive SS* watermarking operation is also performed employing the same input barcode watermark and host image. All the figures shown in this section are generated using *DRPE SS-SS*.

Based on the simulation results, we conclude that the *DRPE SS-SS* algorithm is robust to scaling and JPEG lossy compression, and is particularly robust to 2D cropping, 2D low pass filtering and high pass spatial frequency filtering. We also conclude that watermarks can be successfully extracted following standard printing and scanning operations. We now examine each distortion in detail.

4.1. Image scaling

In our tests, we apply two different methods to scale the watermarked image into one quarter of its original size:

(1) *Downsampling*: To reduce the number of points (pixels) in the image in both x and y, the sample rate of $\overline{H}$ is decreased by retaining only every second pixel

starting with the first pixel. This leaves an image of one quarter of its original size.

(2) *Decimation*: This method involves applying a low pass filter to the watermarked image and then resampling the resulting smoothed signal at a lower rate, i.e. 1/2 of the original sampling rate. This method ensures that the Nyquist sampling theorem criterion is maintained.

To rescale up, for both scaling methods, nearest-neighbor interpolation is employed to bring the image back to its original size, i.e. 1024×1024. Therefore, in our simulation, the watermarked image $\overline{H}$ is scaled to one quarter of its original size, i.e. 512×512. The result shown in Fig. 3(a) is achieved using downsampling, i.e., method (1) presented above. In order to extract the original barcode, the down scaled image can then be rescaled back up to its original dimensions (1024×1024) as shown in Fig. 3(b).

Tables 4 and 5 list the resulting detection BERs found when using watermarked images that have undergone the two scaling operations described above, i.e. (1) downsampling, and (2) decimation, respectively. As can be seen, perfect detection with no errors can be achieved for the $W_{lx} = 16$ in both cases when using our algorithm and for all the barcode widths using the *additive SS* algorithm.

A detailed series of tests were performed. We note that for the cases examined (barcode widths, quantization levels, scaling methods, and interpolation approach employed), the *DRPE SS-SS* is robust to the scaling operation only when the size of the scaled image is greater than or equal to one quarter of the original size.

4.2. JPEG compression distortion

Next we examine the effects of JPEG compression distortion on the watermarked image $\overline{H}$. In JPEG compression, the quantization process controls the data loss and the size of the resulting compressed file [43]. The quantization table, which is used to round the frequency components of the image to the nearest integer, is often modified by multiplying a scaling constant [44]. This multiplicative scaling factor is generally called the *quality factor*, and most JPEG compressors allow the user to specify it. The range of the *quality factor* values is not standardized across JPEG implementations, and also not directly related to the data loss. The command "imwrite"

Table 4
Down sampling (512×512): the *informed detection* BER (%) for different barcode widths (W_{lx}) and different quantization levels (l), found when using both the *additive SS* and *DRPE SS-SS* algorithms.

W_{lx}	*Additive SS*	*DRPE SS–SS*			
		2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0	0
32	0	12.5	6.25	6.25	3.125
64	0	25	20.3125	18.75	10.9375
128	0	31.25	30.4688	18.728	17.9688
256	0	44.9219	44.1406	38.2813	29.6875

Table 5
The decimation (512×512): the *informed* detection BER (%) for different barcode widths (W_{lx}) and different quantization levels (l), found when both the *additive SS* and *DRPE SS-SS* algorithms.

W_{lx}	*Additive SS*	*DRPE SS–SS*			
		2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0	0
32	0	15.625	12.5	6.25	3.125
64	0	35.9375	25.00	17.1875	15.625
128	0	36.7188	29.6875	25.00	20.3125
256	0	46.0938	46.4844	42.5781	38.2813

Fig. 3. (a) Downsampled 0.5 scaled image of the watermarked image; (b) rescaled image from (a).

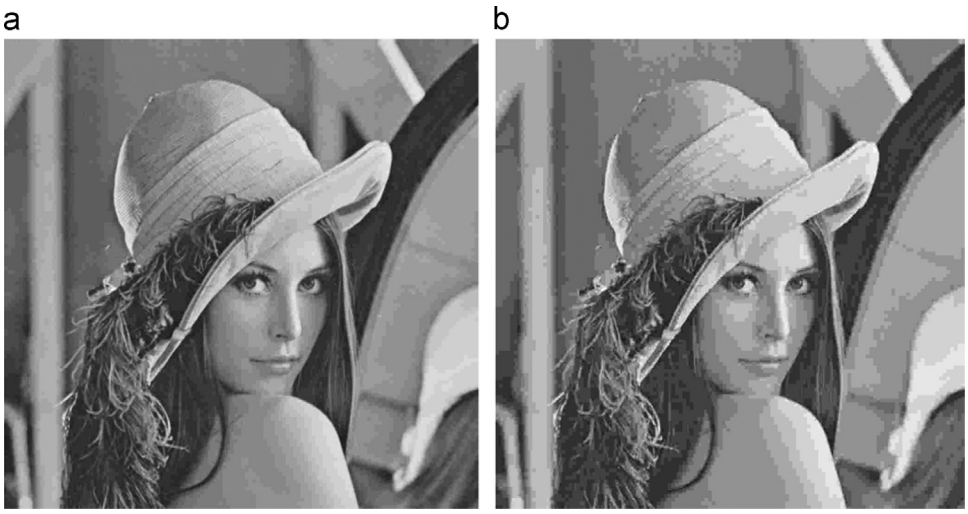

Fig. 4. The JPEG encoded version of the watermarked image with (a) 20% quality and (b) 10% quality.

Table 6
JPEG compression (quality factor 20): the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l). Results are for both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0	0
32	0	12.5	9.375	3.125	0
64	0	20.3125	18.75	4.6875	1.5625
128	0	26.5625	24.2188	15.625	7.0313
256	2.734	36.3281	34.375	28.5156	23.8281

[45], which is available in a current version of MATLAB [46], specifies the range of the *quality factor* to be [0,100], where 0 represents lower quality and higher compression, and 100 represents higher quality and lower compression. In all the cases reported here, MATLAB JPEG compression is used.

In Fig. 4, two JPEG encoded versions of the watermarked image with *quality factors* of (a) 20 and (b) 10 respectively, are presented. As can be seen, the images undergo clearly visible degradations after JPEG compression, i.e. Fig. 4(b) has noticeably lower image quality than Fig. 4(a).

Table 6 lists the detection BER results after the JPEG compression with quality factor 20 for different barcode widths and quantization levels. According to the results, the original barcode can still be perfectly extracted for the $W_{Ix}=16$ case (for all the quantization levels examined) using the *DRPE SS-SS*, and in all cases using *additive SS*. An exhaustive set of tests were performed using different compression quality factor values. For the cases examined, it was found that the *DRPE SS-SS* algorithm is robust to JPEG compression distortion only when the quality factor is greater than or equal to 20. We also note that in the lower quality factor 10 case, perfect detection (BER=0) was found only when $W_{Ix}=16$ in the $l=8$ and $l=16$ cases.

4.3. Cropping

Fig. 5(a) shows a cropped version of the watermarked image in which only the central quarter of the image, which has the size of 512×512, is retained. Performing *informed detection*, the missing fractions of the image are replaced by the corresponding fractions from the *unwatermarked* image, i.e. the original host image H. The resulting image is presented in Fig. 5(b).

The corresponding BER results are listed in Table 7. Perfect detection with no errors is achieved for the $W_{Ix}=16$, 32, and 64 cases using the *DRPE SS-SS*, indicating great robustness to cropping. We emphasis that these results are achieved despite removal of 75% of the data (watermarked image information). However, for the *additive SS* method, perfect detection is never achieved for any of the barcode widths examined. Thus we can draw the conclusion that our algorithm is much more robust to cropping than the *additive SS* method. We note that in the informed case although the host image is available, the cropped (missing) area can just be replaced by zeroes instead of the corresponding fractions from the host image. If this is done, it is observed that the BER results are worse than those in Table 7, i.e. for $W_{Ix}=64$ and $l=2$, the resulting BER=6.25%.

It is interesting to study the robustness for the limiting case of the cropping operation, i.e., how small can the portion of the watermarked image be, i.e. how severe can it be cropped, but the original 1D barcode still extracted perfectly. We note that in our simulations, perfect detection could only be obtained where at least the central 1/16 of the watermarked image is retained and this was only true for the case when $W_{Ix}=16$. Such extreme cropping corresponds to a loss of approximately 93.75% of the watermarked image data. This result has also been confirmed in the cases when any of the four corners areas, with a 1/16 of the watermarked image (size of 256×256), are retained. These limiting results further support our conclusion that the *DRPE SS-SS* is extremely robust to cropping.

Fig. 5. (a) Cropped version of the watermarked image (1/4) with only the central quarter remaining; (b) restored version of the watermarked image using the original host image H (informed detection).

Table 7
Cropping (only the central quarter is left): the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (I). Results are for both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	50	0	0	0	0
32	50	0	0	0	0
64	48.8281	0	0	0	0
128	44.5313	9.375	8.5938	7.8125	7.8125
256	42.187	22.2656	21.0938	19.9219	19.5313

Table 8
Down sampling (512×512 Einstein image): the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (I), found when using both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	0	0	0	0	0
32	0	3.125	3.125	3.125	0
64	0	4.6875	3.1255	3.125	3.125
128	0	16.4063	14.0625	7.0313	6.25
256	0	34.375	33.2031	27.3438	21.875

A detailed series of numerical experiments have also been carried out using two other images, "Einstein" [47], and "Cameraman" [48], and the results compared to those found when using the Lena image. Two tables which provide an illustrative subset of the results found for these two images, in the cases of image scaling (see Table 8) and cropping (see Table 9). It can be seen that the host image watermark only marginally affects watermark performance in both cases. The results have been found for the other types of distortions but are not presented for the purpose of brevity.

Table 9
Cropping (only the central quarter is left, 512×512 Cameraman image): the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (I). Results are for both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	37.5	0	0	0	0
32	21.875	0	0	0	0
64	26.5625	0	0	0	0
128	23.4375	6.25	6.25	6.25	5.4688
256	34.375	21.0938	20.7031	22.6563	19.5313

4.4. Image filtering in the frequency domain

Since the *DRPE SS-SS* has been shown to be extremely robust to spatial cropping, it is important to examine its robustness to the cropping process in the frequency domain. In this section, we test the robustness of our watermarking algorithm to 2D spatial frequency filtering of the watermarked image. The watermarked image is first Fourier transformed, multiplied by a 2D hard edged filter function, and then the result is transformed back to the space domain. The effects of both low pass and high pass filtering are examined.

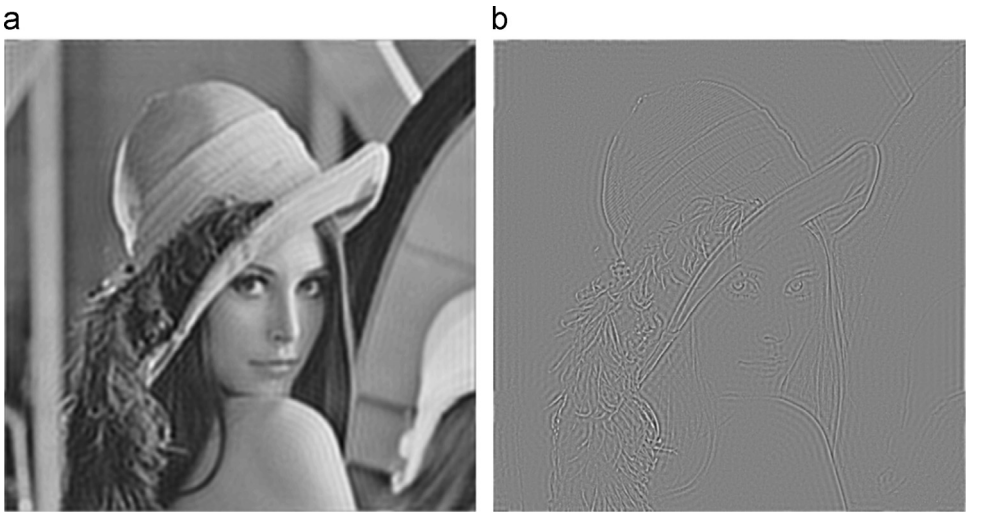

Fig. 6. (a) Low pass filtered watermarked image with cut-off frequency $k_c=128$; (b) high pass filtered watermarked image with cut-off frequency $k_c=128$.

Table 10
Low pass filter with cut-off frequency $k_c=128$: the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l). Results are for both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	0	0	0	0	0
32	0	0	0	0	0
64	0	0	0	0	0
128	0	11.7188	9.375	8.5938	7.8125
256	0	22.2656	21.0938	19.9219	19.5313

Table 11
High pass filter with cut-off frequency $k_c=128$: the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l). Results are calculated for both the *additive SS* and *DRPE SS-SS* algorithms.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	50	0	0	0	0
32	50	0	0	0	0
64	51.5625	0	0	0	0
128	54.6875	11.7188	10.1563	9.375	8.5938
256	56.25	34.375	31.25	29.2969	28.9063

4.4.1. Low pass filter (LPF)

An ideal low pass filter removes all frequency components above some pre-determined cut-off frequency, while leaving the low frequencies unaffected. Such a LPF is now applied to a watermarked image. For a 2D image signal, an ideal low pass filter takes the form of a cylindrical shaped "can", or "hockey puck" of amplitude 1, centered at the origin $k_x=0$ and $k_y=0$ in the spatial frequency domain. The DC component (average value or zeroth order) of the image spectrum is located at the origin of the spectrum. In the Fourier domain, the further the frequency component is from the origin, the higher the spatial frequency it represents. Therefore the distance from the DC component of the roll off point of the filter, denoted by k_c, indicates the cut-off frequency. In a LPF all the high frequency components above this value in both k_x and k_y are removed. For our numerical test, k_c must lie in the range of $0<k_c<N_x/2=512$. Fig. 6(a) is a low pass filtered watermarked image for a cut-off frequency of $k_c=128$, i.e. k_c is equal to 0.125 times of the maximum spatial frequency present.

Table 10 lists the simulation detection BER results after ideal low pass filtering with $k_c=128$, for cases having different barcode widths and quantization levels. The BER results suggest that our algorithm is robust to low pass filtering operations when $W_{Ix}=16$, 32, and 64. The *additive SS* is very robust to low pass filtering for all the barcode widths examined. In relation to this however we note that in the *additive SS* method the watermark information is embedded into the low frequencies of the host image.

4.4.2. High pass filter (HPF)

The application of a 2D high pass filter (HPF) operates in very much the opposite way to that of a LPF, i.e., the power in all the frequencies below some cut-off frequency are removed. For the purpose of comparison, we choose the same cut-off frequency as for the LPF case, i.e. $k_c=128$, and obtain the high pass filtered watermarked image shown previously in Fig. 6(b). It can be observed that application of a HPF acts to emphasize the fine detail information and the edges in the image while the more slowly changing (larger scale) gradients are eliminated.

The corresponding BER results are listed in Table 11. According to the results, perfect detection can be found using the *DRPE SS-SS* method when $W_{Ix}=16$, 32, and 64. While our algorithm remains robust, the *additive SS* method is adversely effected by high pass filtering. In fact all the watermarking information (located in the low frequency components of the image), is removed in the *additive SS* case. Thus we conclude that our algorithm is more robust to high pass filtering than the *additive SS* method.

4.5. Printing and scanning

The print-and-scan process is commonly used for image reproduction and distribution. Printing can be considered as digital-to-analog conversion while scanning can be considered as analog-to-digital conversion. In this section we examine the robustness to commonly encountered printing and scanning distortions of our *DRPE SS-SS* watermark algorithm. A variety of unintended geometric distortions, such as rotating, scaling, and cropping are often introduced during the printing and scanning processes [2]. In addition, distortion also occurs in the individual pixel values of the rescanned image due to the introduction of both external noise and JPEG compression effects introduced during the printing and scanning operations [49]. Both geometric and pixel value distortions affect the quality of the rescanned watermarked image and make it difficult to extract the original barcode without errors.

In our experiments, we first printed out a hard copy of a watermarked image using a standard commercial printer, HP LaserJet CM2320 MFP Series [50]. The paper size "A4" is one of the international ISO paper size standards and is widely used. A square digital watermarked image of size 215.9 mm $\times$ 279.4 mm is printed on an A4 paper sheet. Next, the printed watermarked image is scanned using a Kyocera Mita TASKalfa 520i scanner [51]. The output file format "JPEG" is selected, the dots per inch (DPI) is set to 600 $\times$ 600, and the quality factor is set to 100% (we recall that a quality factor of 100 does not actually produce a lossless JPEG image [44]). One example of a resulting scanned version of a watermarked Lena image, with the edges of the A4 page located as indicated, is shown in Fig. 7(a).

In this case the barcode embedded has a width of $W_{lx} = 16$ pixels and a quantization level of $l=8$. The watermarked image is surrounded by a white margin in the rectangular scanned image. To illustrate this, a black border line is introduced in the figure corresponding to the A4 page boundaries (edges). One example of a typical distortion arises when a user places the printed image on the flatbed of the scanner and the image suffers a small mis-orientation or rotation if it is not well placed. An example of this situation, involving an orientation angle of 8.6°, is shown in Fig. 7(b).

We note that the scanned image has a full size of 3507 $\times$ 2480. This indicates that the scanner applies an image scaling process [2], which often involves using a decimation with a low pass filter. In order to detect the original barcode information, the following procedure can be used:

(i) *Image rotation correction*: First, the rotated scanned image must be re-aligned to its original orientation (horizontal). This involves the application of the Hough transform to detect lines in the image and thus identify the rotation angle [52].

(ii) *Image cropping*: Once the image orientation is correct, the white border of the resulting scanned image is removed in order to obtain the square watermarked image in the center. This can be realized using the Harris corner detector [53], where the maximum number of corners to detect is in this case 4. Using the positions of the four detected corners the rectangular scanned image can be appropriately cropped to obtain the central image.

(iii). *Image scaling*: Finally, the resultant image is rescaled (down sampled) back to the original size of the watermarked image (1024 $\times$ 1024).

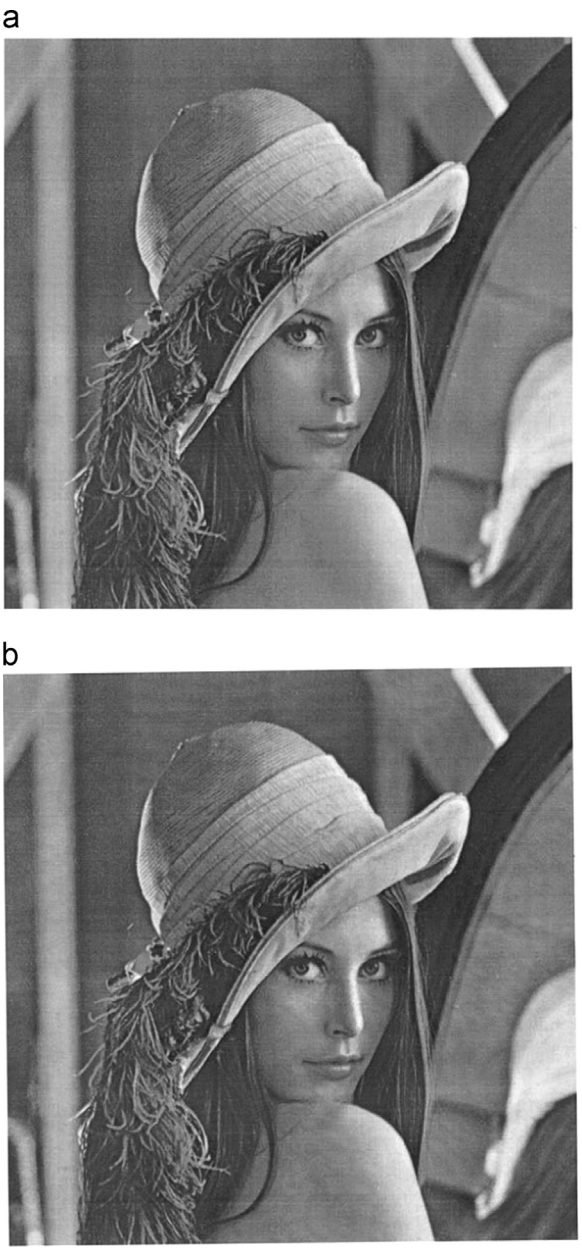

Fig. 7. An example of the scanned watermarked image: (a) perfectly scanned image; and (b) slightly rotated scanned image, i.e. 8.6°. The A4 page edges are indicated by the black border.

Table 12 presents the BER (%) results after applying *informed detection* to extract the watermarks from the

Table 12
Printing and scanning (CM2320 and CanoScan5200F): the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l). JPEG quality factor is chosen to be 100 and DPI is selected to be 600×600.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	18.75	37.5	31.25	31.25	25
32	43.75	43.75	59.375	43.75	46.875
64	37.5	59.375	60.9375	53.125	45.3125
128	38.2813	46.0938	44.5313	50	49.2188
256	37.1094	53.125	55.8594	54.2969	52.7344

Table 13
Printing and scanning (8100DN and TASKalfa520i): the *informed detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l). JPEG quality factor is chosen to be 75 and DPI is selected to be 300×300.

W_{Ix}	*Additive SS*	*DRPE SS–SS*			
		2-Level	4-Level	8-Level	16-Level
16	18.75	50	43.75	37.5	31.25
32	43.75	59.375	46.875	43.75	43.75
64	37.5	54.835	44.5313	46.0938	47.695
128	38.2813	59.375	60.9375	53.125	45.3125
256	37.1094	53.272	54.25	55.625	56.535

resulting printed and scanned images for both the *DRPE SS-SS* and *additive SS* cases. Both algorithms show a loss of performance under real world conditions. The main reason for this is that the distortions and noises added during the printing and scanning processes affect a large number of pixel values in the original watermarked image. We note that the performance of both improves for lower barcode widths and larger numbers of levels.

Continuing our experiments, we examine the results for another type of HP printer: HP LaserJet 8100DN series printer [54], and another type of scanner: CanoScan 5200F [55], used. In this case the JPEG compression quality factor is set to 75 and the DPI is set to 300×300. The BER results in Table 13 are worse than those in Table 12 because of the lower quality options chosen in the printing and scanning processes. Once again the wider the barcode and the fewer the number of levels, the worse the performance.

5. Blind detection robustness

As previously noted, see Section 3.1, for some applications involving digital image watermarking, e.g. copy control application, detection must be performed without access to the original host image. Now we examine the robustness of our algorithm to *blind detection* by repeating the same tests as were performed above for the *informed detection* case. Once again the BER results using *DRPE SS-SS* are tabulated for various cases. We note that the *additive SS* algorithm is not well suited for application to blind detection, as indicated in Section 3.3, and therefore no results can be shown for comparison.

- *Scaling*: The same image scaling operations, i.e. down sampling and decimation to one quarter size of the original image, as described in Section 4.1, are applied to the watermarked image. The blind detection BER results using the *DRPE SS-SS* method are shown in Table 14 for the down sampling method employed. We note that the results for the decimation in the blind detection case are not shown in this paper for brevity. The results indicate that our method is robust to the image scaling operation when $W_{Ix} = 16$ and $l = 8$ and $l = 16$. It is observed that the blind detection shows worse performance than the corresponding informed detection case.
- *JPEG compression*: Robustness to lossy compression is also examined. Since informed detection has been found to usually perform better than blind detection (see Section 4.3), a larger compression quality factor (greater than the values of 20 and 10 used previously) is required for the blind detection test here. The corresponding BER values are listed in Table 15 using JPEG compression with quality factor equals to 60. As can be seen when $W_{Ix} = 16$ and $l = 16$, $BER = 0$. Thus we conclude that the *DRPE SS-SS* algorithm is also robust to JPEG compression in the blind detection case. We also examine the limiting case. It is found that perfect detection can be achieved only when the quality factor is larger than 60.
- *Cropping*: Since the original host image is not available for detection, we arbitrarily choose to replace the missing portions of the watermarked image with zero

Table 14
Down sampling (1/4): the *blind detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l) using the *DRPE SS-SS* algorithms.

W_{Ix}	*DRPE SS–SS*			
	2-Level	4-Level	8-Level	16-Level
16	18.75	6.25	0	0
32	25	25	15.625	15.625
64	39.0625	35.9375	28.125	21.875
128	43.75	42.9688	41.4063	36.7188
256	50	43.75	37.8906	29.6875

Table 15
JPEG compression (*quality factor* 60): the *blind detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l) using the *DRPE SS-SS* algorithms.

W_{Ix}	*DRPE SS–SS*			
	2-Level	4-Level	8-Level	16-Level
16	25	18.75	6.25	0
32	15.625	12.55	9.375	6.25
64	28.125	26.5625	15.625	9.375
128	40.625	36.7188	32.8125	18.75
256	39.4531	37.8906	33.5938	27.7344

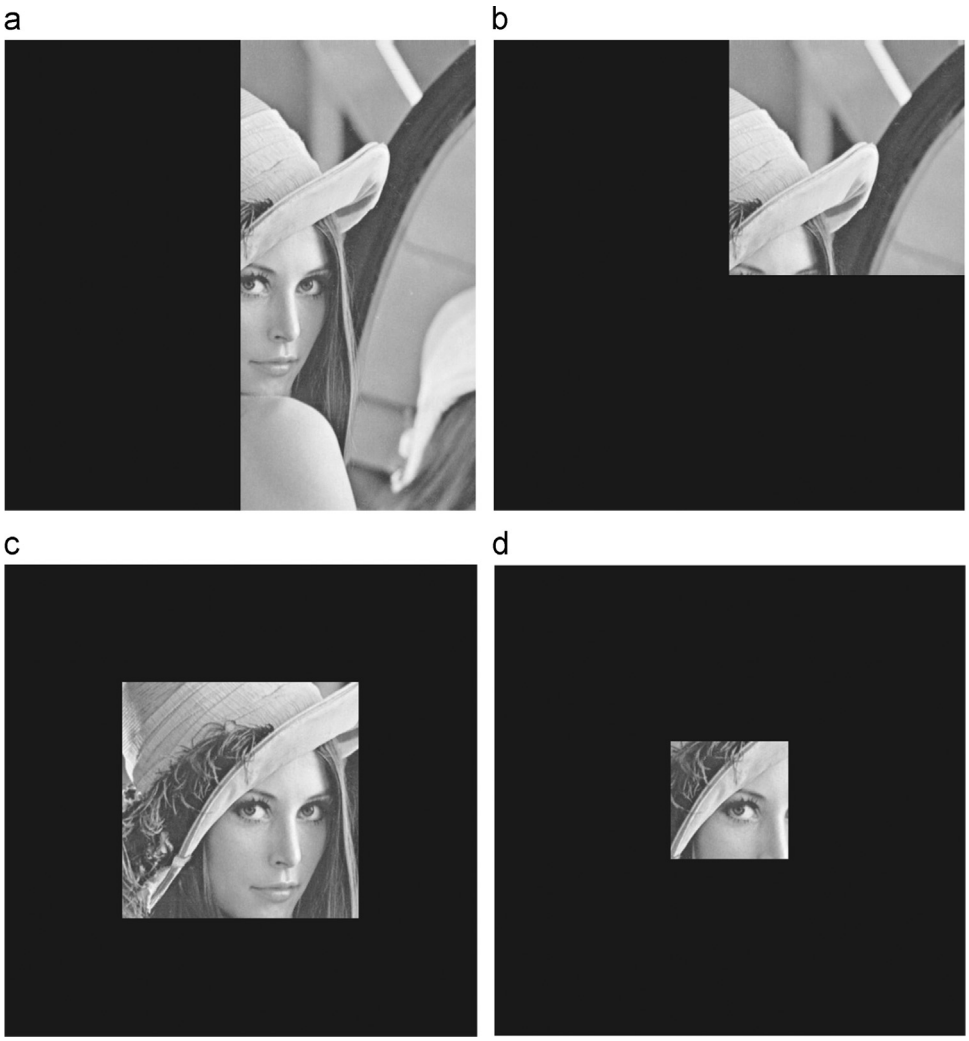

Fig. 8. Cropping for blind detection: (a) cropping half of the watermarked image (see Table 16); (b) cropping three quarters of the watermarked image; (c) only the central quarter of the watermarked image remains (see Table 17); and (d) only the central 1/16 of the watermarked image is retained.

Table 16
Cropping (only the right half of the image is left, see Fig. 8(a)): the *blind detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l) using the *DRPE SS-SS* algorithms.

W_{Ix}	*DRPE SS–SS*			
	2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0
32	0	0	0	0
64	3.125	0	0	0
128	17.9688	15.625	7.0313	3.9063
256	37.8906	37.5	28.125	24.6094

Table 17
Cropping (only the central quarter of the image is left, see Fig. 8(c)): the *blind detection* BER (%) for different barcode widths (W_{Ix}) and different quantization levels (l) using the *DRPE SS-SS* algorithms.

W_{Ix}	*DRPE SS–SS*			
	2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0
32	3.125	3.125	0	0
64	12.5	9.375	0	0
128	28.125	25	12.5	5.4688
256	41.4063	39.8438	31.6406	24.6094

grayscale level (black). Fig. 8 illustrates the four possibilities examined. These include (a) only the right half of the image is available; (b) only the right top quarter of the image is available; (c) only the central quarter of the image remains; and (d) only the central 1/16 portion of the image is retained.

In Tables 16 and 17, we list the blind detection BERs for cases (a) and (c) in order to illustrate the robustness to cropping. The results found, including those listed in Tables 16 and 17, show that perfect detection is achieved when $W_{Ix} = 16$ for all four cropping cases (a)–(d). This indicates good robustness against cropping

in the blind detection case. Furthermore, the limiting case of cropping for the blind detection case is found when at least 1/16 of the watermarked image remains available. This is the same level as in the case of the informed detection (see Section 4.3). If less than 1/16 of the original image remains then the original barcode information cannot be successfully recovered, i.e. BER=0.

- *Image filtering*: The same low pass and high pass filtering operations, used in Section 4.4 with a cut-off frequency in both cases of $k_c=128$ is employed, and the corresponding blind detection BER are listed in Tables 18 and 19 respectively.
  As can be seen, for the LPF case perfect detection can again be achieved for both the $W_{lx}=16$ and 32 cases. For the HPF case $BER=0$ when $W_{lx}=16$. The simulation results indicate the robustness to both filtering operations. We note that for the same cut-off frequency the *DRPE SS-SS* shows better performance to the application of the LPF than that to that of the HPF. In conclusion, the *DRPE SS-SS* algorithm has again been shown to be very robust to both space (occlusion) and spatial frequency (filtering) cropping.
- *Printing and scanning*: Since our algorithm is not robust to printing and scanning in the informed detection case, there is little possibilities that will be robust in the blind detection case. Our results, shown in Table 20, validate this assertion. A CM2320 printer and a CanoScan5200F scanner with JPEG quality factor chosen to be 100 and DPI selected to be 600×600 are used to generate these results. However given the high BER values we note that only when $W_{lx}=16$ and $l=16$ a relatively better results are obtained. This agrees with the conclusions presented in Liu et al. [40], where the narrower the barcode width and the larger number of quantization levels used, the more accurate the detection process (fewer errors).

Table 18
Low pass filtering with cut-off frequency $k_c=128$: the *blind detection* BER (%) for different barcode widths (W_{lx}) and different quantization levels (l) using the *DRPE SS-SS* algorithms.

W_{lx}	*DRPE SS−SS*			
	2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0
32	0	0	0	0
64	3.125	1.5625	0	0
128	19.5313	18.75	10.1563	4.6875
256	42.9688	42.9688	37.8906	28.9063

Table 19
High pass filtering with cut-off frequency $k_c=128$: the *blind detection* BER (%) for different barcode widths (W_{lx}) and different quantization levels (l) using the *DRPE SS-SS* algorithms.

W_{lx}	*DRPE SS−SS*			
	2-Level	**4-Level**	**8-Level**	**16-Level**
16	0	0	0	0
32	3.125	3.125	0	0
64	23.4375	17.1875	15.625	0
128	28.125	25.7813	24.2188	19.5313
256	36.3281	35.5469	34.7656	38.2813

Table 20
Printing and scanning: the *blind detection* BER (%) for different barcode widths (W_{lx}) and different quantization levels (l)using the *DRPE SS-SS* algorithms.

W_{lx}	*DRPE SS−SS*			
	2-Level	**4-Level**	**8-Level**	**16-Level**
16	56.25	50	37.5	31.25
32	59.375	54.6875	46.875	45.3125
64	56.25	53.125	48.4375	46.0938
128	56.25	55.8594	53.125	50
256	48.4375	52.7344	46.4844	45.3125

6. Uniqueness of the watermark

Quantifying the false positive error rate is an important way to test the performance of a watermarking process. In this section we investigate the false positive rate behavior of both the *DRPE SS-SS* and *additive SS* algorithms. A "false positive" occurs when a watermark detection process indicates the presence of a watermark in an *unwatermarked* host image, i.e., a 1D barcode sequence being falsely detected when in fact no barcode image has been embedded [2]. The probability of a false positive is the likelihood of such an occurrence, and the false positive rate is the frequency of false positives, i.e. the number of false positives expected to occur for a given number of runs of the detector. Both the watermark detection algorithm and the purpose for which a detector is performed affect the false positive rate. In this section two types of detection are examined: (i) the detector may be used to identify one of many random watermarks in a single host image, or (ii) to look for a single watermark in many random host images. In the first case, the watermark can be considered to be a random variable. In the second case, it is the host image that is considered to be the random variable. Correspondingly, the concept of false positive can be categorized into two forms: (i) the *random-watermark false positive* and (ii) the *random-host false positive* [2].

6.1. Random-watermark false positive

In a transaction tracking (fingerprinting) application, i.e. using watermarks to identify people who obtain content legally but illegally redistribute it (e.g. pirating), the detection of a particular watermark in a given host image might lead to a false accusation of copyright piracy. In this situation, the host image is available to the owner, and the number of different watermarks used to identify each customer may be very large and can be treated as though generated in some random way. Such a false positive model is often referred to as the *random-watermark false positive*. In this case, the watermark is effectively a random variable and the host image is treated as a constant. This

form of false positive is examined for both algorithms (*DRPE SS-SS* and *additive SS*) using the following procedure:

(i) *Generating random barcode watermarks*: Retaining a fixed host image, 1000 barcode watermark sequences are randomly generated, chosen using a certain probability distribution. For the 1D barcode case, each of the 1000 random barcode sequences only contains the binary values 0 or 1. Thus we first generate pseudo-random uniformly distributed numbers on the interval [0,1], and then round each number into a 0 or 1 using an arbitrarily chosen threshold value, denoted by T. All of the values greater than T are assigned the value 1, and the rest are set to 0. Barcodes generated in this way follow the Binomial distribution [56]:
If I_i denotes each random uniformly distributed sequence on the interval $[0, 1]$, where $1 \le i \le W_{Ix}$, then the probability density function of I_i is

$$f(I_i) = \begin{cases} 1 & \text{for } [0,1], \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Based on the rounding process with the threshold T, the probability of the value 0s appearing, p, can be calculated by

$$p = \int_0^T f(I_i) = T. \tag{3}$$

Therefore the threshold value represents the probability that a value 0 appears in the generated barcode sequences. For instance, if we choose T to be equal to 0.4, then the barcode will be made up of 60% of 1 values and 40% of 0 values. This indicates that each barcode of width n can be viewed as an n independent success/failure (1/0) experiments (Bernoulli trials), each of which yields success with probability $1-p$, and failure with probability p [57]. In our test we choose the probability $p=0.5$, therefore indicating that half $(n/2)$ of the barcode values are 1s.

(ii) *Choosing the evaluating metric – BER*: In the *additive SS* algorithm as described by Cox, a standard normal distributed vector (Gaussian vector) is used as the watermark, and it has been demonstrated that it is unlikely that exactly the same watermark will be extracted due to machine errors [9]. Thus in order to examine the false positive behavior, a *similarity metric (sim)* acting as a correlation function was employed by Cox in order to evaluate the similarity between the original and detected (randomly generated) watermarks. However, for the 1D barcode case examined here, the similarity metric is not applicable when comparing two binary sequences containing only 0s and 1s. Therefore, as described in Section 3.3, the BER metric is used instead. Each of the 1000 randomly selected barcode sequences is compared to the original barcode and the corresponding BER values are calculated. In this case the total numbers of pixel values in error (when calculating BER) can be obtained simply by subtracting the corresponding pixel values and comparing the result to the value 0.

(iii) *Calculating the false positive rate*: As noted in the case of *random-watermark false positive*, the host image is a constant and the watermark is a random variable. Thus the false positive probability is actually independent of the host image and depends only on the method of watermark generation. In other words, the detector output distribution is primarily determined by the distribution governing the way in which the randomly chosen watermark reference patterns are generated. Therefore in our simulation, it is the thresholding value T and thus the Binomial probability value p that will affect the false positive rate.
The calculated BER results for 1000 randomly generated barcodes are compared when using both the *DRPE SS-SS* and *additive SS* algorithms. For the purpose of illustrating the false positive performance, the results for a standard host image containing the correct original barcode are inserted as one of the 1000 randomly generated barcodes, at location 500 as shown in Fig. 9.
The x-axis represents the sequence of randomly selected reference barcodes, and the y-axis shows the resulting BER values. As noted in our simulation the barcode sequence located at the 500th position on the x-axis is in fact the original barcode, and therefore gives a BER value of zero. In Fig. 9, the results for two barcode widths are examined for both watermarking algorithms: (a) *DRPE SS-SS* with $W_{Ix}=16$ and $l=16$; (b) *additive SS* with $W_{Ix}=16$; (c) *DRPE SS-SS* with $W_{Ix}=256$ and $l=16$; and (d) *additive SS* with $W_{Ix}=256$. As can be seen, a value of BER=0 only appears at the 500th position. None of the random generated barcodes give BER values close to that for the original barcode, i.e. for both algorithms when $W_{Ix}=16$, $BER \ge 10\%$ and when $W_{Ix}=256$, $BER \ge 40\%$. Calculating the false positive probability for both algorithms, it can be shown that when $W_{Ix}=16$ the false positive probability is $1/2^{16}$, and when $W_{Ix}=256$ the false positive probability of $1/2^{256}$. This is because the randomly generated barcodes are independent of each other and the probabilities of 1s and 0s appearing are equal, i.e. $p=0.5$. In general, if there are k 1s and $(W_{Ix}-k)$ 0s in the original barcode then the Binomial probability of 0s is $p=(W_{Ix}-k)/W_{Ix}$, and the false positive probability is calculated to be $(1-p)^k p^{W_{Ix}-k}$. Therefore we conclude that both watermarking algorithms have very similar low false positive response rates. In addition, the greater the barcode width, the lower the false positive rate will be for both.

6.2. Random-host false positive

We now consider the situation in which many different host images (none of which contain any watermarks) are being tested for the presence of one particular watermark. As previously noted given a fixed watermark and randomly selected host images, the chance of finding the

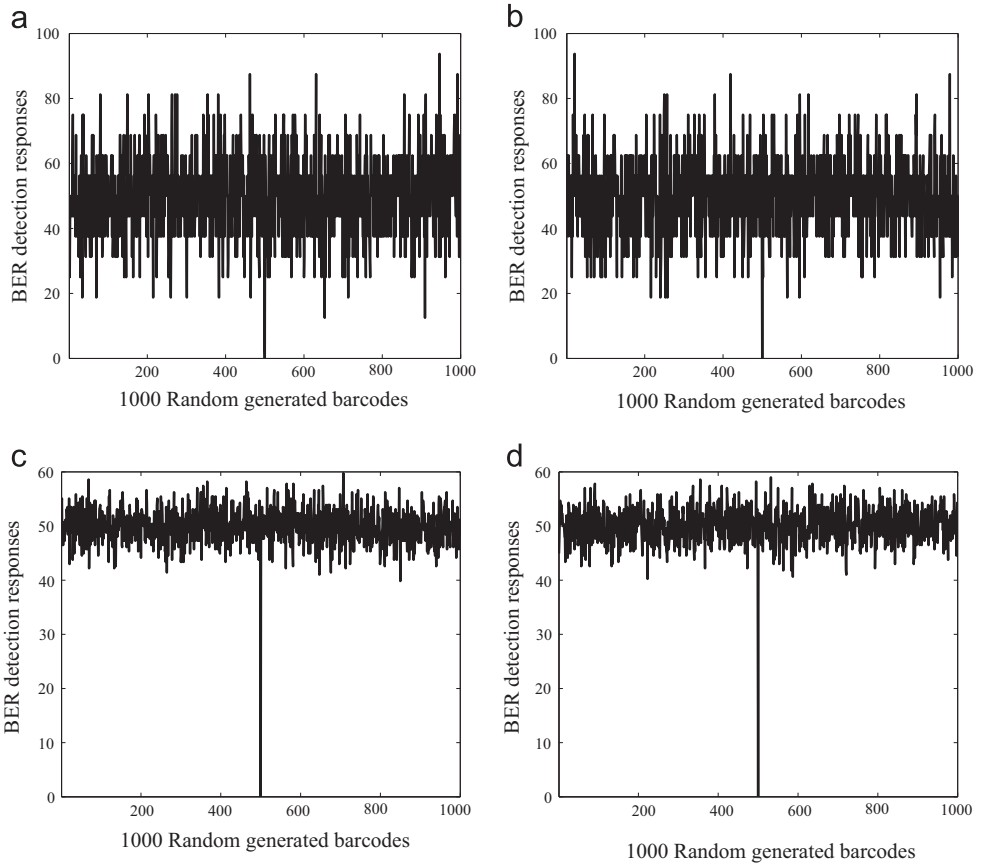

Fig. 9. *Random-watermark false positive*: the BER responses to 1000 randomly generated barcodes using both watermarking algorithms: *DRPE SS-SS* (a) and (c); and *additive SS* (b) and (d). The barcodes widths chosen for cases (a) and (b) are $W_{lx}=16$, and for cases (c) and (d) are $W_{lx}=256$.

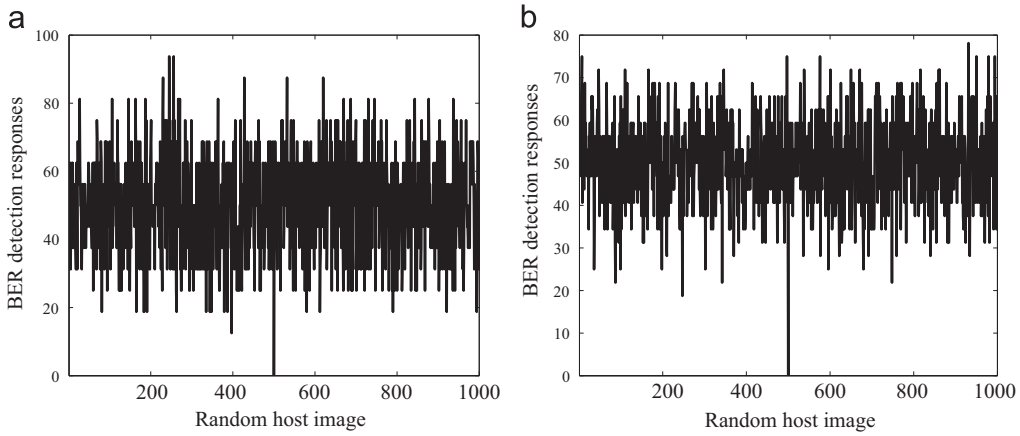

Fig. 10. *Random-host false positive*: the BER responses of the *DRPE SS-SS blind detection* algorithm to 1000 random host (unwatermarked) image, using a fixed barcode with (a) $W_{lx}=16$ and (b) $W_{lx}=32$ both for the $l=16$ case.

specific watermark in an unwatermarked host image is referred to as the *random-host false positive probability*.

This type of false positive is of concern for many common watermarking applications. For instance, in a copy control watermarking application, all possible images (or other types of data media) must be examined for the presence of a particular watermark in order to indicate the copyright owner or to validate some recording permission assignments. In this case, the watermark can be considered as the constant while the large variety of possible host images are the random variables.

In our simulations, we test this random-host false positive probability for one specific barcode sequence using 1000 randomly chosen images from the Corel database

[58]. These images act as the host image (unwatermarked) to be tested. We then apply our *DRPE SS-SS blind detection* method [40]. We note that only the blind detection method of the *DRPE SS-SS* is examined in this *random-host false positive* case, since in the informed detection process the deduction of the known host image by itself would result in zero (the host image is first subtracted from the watermarked image $\overline{H}$ to obtain the watermark). Furthermore, as noted the *additive SS* cannot be used with blind detection. In Fig. 10, we present the BER value calculated for the 1000 random host images using *DRPE SS-SS* with: (a) $W_{lx}=16$, and (b) $W_{lx}=32$, and in both cases with a quantization level of $l=16$. Once again for illustration purposes, the 500th host image is replaced with a watermarked image containing the required original watermark, giving a BER value of 0 in agreement with the results in Table 1. As can be seen, none of the other 999 randomly selected host images produce a false positive, i.e. when $W_{lx}=16$, $BER\geq 10\%$ and when $W_{lx}=32$, $BER\geq 20\%$. These results suggest very low false positive rates for our algorithm in the *random-host false positive probability* case.

7. Conclusion

In this paper we present a detailed investigation of the robustness of the Double Random Phase Encoding spread-space spread-spectrum (*DRPE SS-SS*) watermarking technique introduced in Liu et al. [40]. It is shown how the even spreading of the watermark energy in both the space and spatial frequency domains makes the *DRPE SS-SS* watermarking algorithm robust to most commonly encountered distortions. The effects of several common geometric transformations and of the signal processing methods used are quantified for the *informed detection* case and for different barcode widths and different quantization levels. The results presented demonstrate that the *DRPE SS-SS* method is robust to scaling, and JPEG compression distortion, and particularly robust to cropping, and low pass and high pass filtering. In all cases possible the performance of this method is compared to that of a classic spread spectrum technique, the *additive SS* method [9]. In particular the *DRPE SS-SS* is shown to be more robust to cropping than the *additive SS*. For the limiting case of cropping, when 93.75% of the watermarking data has been removed, perfect detection can still be achieved when the barcode width is $W_{lx}=16$. This conclusion suggests that our algorithm performs much better in terms of both space and spatial frequency cropping than Cox's method. We note that this conclusion is based solely on tests involving informed detection. Furthermore, the narrower the barcode width and the larger number of quantization levels used, the more accurate the detection process (fewer errors). A detailed quantitative examination of the robustness of the method to printing and scanning is reported. The performance of the *DRPE SS-SS* is shown to compare well to that of the *additive SS* across a range of hardware platforms.

It has also been demonstrated that our algorithm has very low false positive rates both for random-watermark and random-host false positive types. In addition, the larger the barcode width, the lower the false positive rate. We note that this conclusion is drawn on results for the informed detection case. In the blind detection case on the other hand, our method can be applied while the *additive SS* algorithm cannot be used. In summary, in the cases of JPEG, spatial and spatial frequency cropping, as well as blind detection, the *DRPE SS-SS* performs better than the *additive SS*.

Future work should include examining the use of error detection codes to improve the detection performance of the *DRPE SS-SS* algorithm. Furthermore, in this paper the role of the diffusers employed in the DRPE method is not discussed in terms of their influence on the watermark robustness. In [60] we have discussed how the design of narrow band diffusers can be used to control the spreading of the input information in both the space and spatial frequency domains. The bandwidths of the diffusers will almost certainly impact on the results presented particularly in relation to the printing and scanning test. We note that narrower band diffusers will result in less spreading of the information in phase space, which might be expected to make the watermark relatively immune to slight misalignment in the printing and scanning process. However this may be at the expense of reducing the watermarks robustness to cropping. Finally it is necessary to compare the *DRPE SS-SS* to an accepted watermarking technique which is capable of operating in both the blind and informed detection regimes.

Acknowledgments

We acknowledge the support of Erasmus Mundus Programme of European Commission. This publication has emanated in part from research conducted with the financial support of Science Foundation Ireland (SFI) under Grant Number 11/SIRG/I2140. JTS acknowledges further support from Enterprise Ireland and SFI through the National Development Plan.

References

[1] M.K. Arnold, M. Schmucker, S.D. Wolthusen, Techniques and Applications of Digital Watermarking and Content Protection, Artech House Publishers, London, UK, 2003.
[2] I.J. Cox, M.L. Miller, J.A. Bloom, J. Frindrich, T. Kalker, Digital Watermarking and Steganography, 2nd ed. , 2008.
[3] C. Podilchuk, E. Delp, Digital watermarking: algorithms and applications, IEEE Signal Proc. Mag. 18 (2001) 33–46.
[4] F. Petitcolas, R. Anderson, M. Kuhn, Information hiding—a survey, Proc. IEEE 87 (1999) 1062–1078.
[5] I.J. Cox, M.L. Miller, Review of watermarking and the importance of perceptual modeling, in: SPIE Conference on Human Vision and Electronic Imaging II, 1997, pp. 92–99.
[6] R. Wolfgang, C. Podilchuk, E. Delp, Perceptual watermarks for digital images and video, Proc. IEEE 87 (1999) 1108–1126.
[7] C.-T. Hsu, J.-L. Wu, Hidden digital watermarks in images, IEEE Trans. Image Process. 8 (1999) 58–68.
[8] G. Langelaar, I. Setyawan, R. Lagendijk, Watermarking digital image and video data. A state-of-the-art overview, IEEE Signal Process. 17 (2000) 20–46.
[9] I. Cox, J. Kilian, F. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (1997) 1673–1687.
[10] C. Fung, A. Gortan, W.G. Junior, A review study on image digital watermarking, in: The Tenth International Conference on Networks, 2011, pp. 24–28.
[11] R. van Schyndel, A. Tirkel, C. Osborne, A digital watermark, ICIP-94, vol. 2, 1994, pp. 86–90.

[12] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimed. 4 (2002) 121–128.
[13] M. Barni, F. Bartolini, V. Cappellini, A. Piva, A DCT-domain system for robust image watermarking, Signal Process. 66 (1998) 357–372.
[14] J. Hernandez, M. Amado, F. Perez-Gonzalez, DCT-domain watermarking techniques for still images: detector performance analysis and a new structure, IEEE Trans. Image Process. 9 (2000) 55–68.
[15] M. Barni, F. Bartolini, A. Piva, Improved wavelet-based watermarking through pixel-wise masking, IEEE Trans. Image Process. 10 (2001) 783–791.
[16] K. Loukhaoukha, J.-Y. Chouinard, Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification, in: 11th CWIT, 2009, pp. 177–182.
[17] O. Matoba, T. Nomura, E. Perez-Cabre, M. Millan, B. Javidi, Optical techniques for information security, Proc. IEEE 97 (2009) 1128–1148.
[18] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.
[19] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25 (2000) 887–889.
[20] S. Liu, L. Yu, B. Zhu, Optical image encryption by cascaded fractional Fourier transforms with random phase filtering, Opt. Commun. 187 (2001) 57–63.
[21] B.M. Hennelly, J.T. Sheridan, Image encryption and the fractional Fourier transform, Optik—Int. J. Light Electron Opt. 114 (2003) 251–265.
[22] S. Liu, J.T. Sheridan, Optical encryption by combining image scrambling techniques in fractional Fourier domains, Opt. Commun. 287 (2013) 73–80.
[23] B.M. Hennelly, J.T. Sheridan, Random phase and jigsaw encryption in the Fresnel domain, Opt. Eng. 43 (2004) 2239–2249.
[24] G. Situ, J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett. 29 (2004) 1584–1586.
[25] J.A. Rodrigo, T. Alieva, M.L. Calvo, Gyrator transform: properties and applications, Opt. Express 15 (2007) 2190–2203.
[26] Z. Liu, Q. Guo, L. Xu, M.A. Ahmad, S. Liu, Double image encryption by using iterative random binary encoding in Gyrator domains, Opt. Express 18 (2010) 12033–12043.
[27] S. Kang, Y. Aoki, Image data embedding system for watermarking using Fresnel transform, in: ICMCS 99, vol. 1, Washington, DC, USA, 1999, pp. 885–889.
[28] N. Nishchal, Optical image watermarking using fractional Fourier transform, J. Opt. 38 (2009) 22–28.
[29] Z. Liu, L. Xu, Q. Guo, C. Lin, S. Liu, Image watermarking by using phase retrieval algorithm in Gyrator transform domain, Opt. Commun. 283 (2010) 4923–4927.
[30] Q. Guo, Z. Liu, S. Liucora, Image watermarking algorithm based on fractional Fourier transform and random phase encoding, Opt. Commun. 284 (2011) 3918–3923.
[31] N. Takai, Y. Mifune, Digital watermarking by a holographic technique, Appl. Opt. 41 (2002) 865–873.
[32] L.-Z. Cai, M.-Z. He, Q. Liu, X.-L. Yang, Digital image encryption and watermarking by phase-shifting interferometry, Appl. Opt. 43 (2004) 3078–3084.
[33] X.F. Meng, L.Z. Cai, M.Z. He, G.Y. Dong, X.X. Shen, Cross-talk-free double-image encryption and watermarking with amplitude phase separate modulations, J. Opt. A: Pure Appl. Opt. 7 (2005) 624.
[34] H. Kim, Y. Lee, Optimal watermarking of digital hologram of 3-D object, Opt. Express 13 (2005) 2881–2886.
[35] B.M. Hennelly, J.T. Sheridan, Fractional Fourier transform-based image encryption: phase retrieval algorithm, Opt. Commun. 226 (2003) 61–80.
[36] H. Zhang, L. Cai, X. Meng, X. Xu, X. Yang, X. Shen, G. Dong, Image watermarking based on an iterative phase retrieval algorithm and sinecosine modulation in the discrete-cosine-transform domain, Opt. Commun. 278 (2007) 257–263.
[37] X. Wang, D. Zhao, Double-image self-encoding and hiding based on phase-truncated Fourier transforms and phase retrieval, Opt. Commun. 284 (2011) 4441–4445.
[38] C. Liu, J. Gu, W. Wu, J. Guo, Application of random amplitude-phase optical encryption based on normal speckle pattern interference in digital watermarking, Appl. Mech. Mater. 427 (2013) 2067–2072.
[39] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G. De Natale, A. Neri, A commutative digital image watermarking and encryption method in the tree structured Haar transform domain, Signal Process.: Image Commun. 26 (2011) 1–12.
[40] S. Liu, B.M. Hennelly, J.T. Sheridan, Digital image watermarking spread-space spread-spectrum technique based on double random phase encoding, Opt. Commun. 300 (2013) 162–177.
[41] Lena, ⟨http://sipi.usc.edu/database/⟩, 2011 (website).
[42] E. Lam, J. Goodman, A mathematical analysis of the dct coefficient distributions for images, IEEE Trans. Image Process. 9 (2000) 1661–1666.
[43] G.K. Wallace, The JPEG still picture compression standard, Commun. ACM 34 (1991) 30–44.
[44] L. Zhilin, K.W. Lam, Effects of JPEG compression on the accuracy of photogrammetric point determination, Photogramm. Eng. Remote Sens. 68 (2002) 847–853.
[45] MATLAB, ⟨http://www.mathworks.co.uk/help/matlab/ref/imwrite.html⟩, 2013 (website).
[46] MATLAB, ⟨http://www.mathworks.co.uk/support/sysreq/sv-r2013a/⟩, 2013 (website).
[47] Einstein, ⟨http://simple.wikipedia.org/wiki/Albert_Einstein⟩, 1921 (website).
[48] Cameraman, ⟨http://www.imageprocessingplace.com/root_files_V3/image_databases.htm⟩, 2013 (website).
[49] C.-Y. Lin, S.-F. Chang, Distortion modeling and invariant extraction for digital image print-and-scan process, in: Proceedings of International Symposium on Multimedia, 1999.
[50] HPCM2320, ⟨http://h10010.www1.hp.com/wwpc/us/en/sm/WF10a/18972-18972-3328064-12004-3328083-3597338.html⟩, 1999 (website).
[51] Kyocera, ⟨http://www.kyoceradocumentsolutions.eu/index/products/product/taskalfa520i.html⟩, 1999 (website).
[52] D.H. Ballard, Generalizing the Hough transform to detect arbitrary shapes, Pattern Recognit. 13 (1981) 111–122.
[53] C. Harris, M. Stephens, A combined corner and edge detector, in: Alvey Vision Conference, Manchester, UK, vol. 15, 1988, p. 50.
[54] HP8100DN, ⟨https://h10057.www1.hp.com/ecomcat/hpcatalog/specs/C4216A.htm⟩, 1999 (website).
[55] Canon, ⟨http://www.canon-europe.com/Support/Consumer_Products/products/scanners/CanoScan_series/CanoScan_5200F.aspx⟩, 2002 (website).
[56] A.H. Ang, W.H. Tang, Probability concepts in engineering, Planning 1 (2004) 1–3.
[57] N.L. Johnson, A.W. Kemp, S. Kotz, Univariate Discrete Distributions, John Wiley & Sons, Hoboken, NJ, USA, 2005.
[58] D. Tao, ⟨https://sites.google.com/site/dctresearch/Home/content-based-image-retrieval⟩, 2001 (corel database).
[60] S. Liu, B.M. Hennelly, J.T. Sheridan, Numerical simulation of double random phase encoding, Opt. Eng. 51 (2012) 128201.