Digital image watermarking spread-space spread-spectrum technique based on Double Random Phase Encoding

Shi Liu[a], Bryan M. Hennelly[b] and John T. Sheridan[a,b]

[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 Computer Science,
National University of Ireland Maynooth, Ireland

ABSTRACT

In this paper a digital invisible image watermarking technique is proposed based on the numerical simulation of optical Double Random Phase Encoding (DRPE). This technique utilizes the capability of the DRPE to spread the energy of the input information in both the space and the spatial frequency domains using two diffusers. The watermark is in the form of a digital barcode image which 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 a low pass filter. The results presented indicate the feasibility and robustness of the proposed method and it is demonstrated that even when using very few quantization levels, i.e. 2-levels, the watermark can still be extracted with very small errors.

Keywords: Optical Encryption, Double Random Phase Encoding, Discrete Fourier Transform, Digital Watermarking, Spread Spectrum.

1. INTRODUCTION

With the rapid development of modern communication techniques, information security and intellectual property protection are of increasing concern. To provide copyright protection for digital, audio and video data, two complementary techniques are being developed: *encryption* and *watermarking*.[1] Encryption techniques can be used to protect digital data during the transmission from the sender to the receiver. Optical encryption techniques are of interest due to their considerable advantages, such as the inherent capability for parallel processing, and the possibility of hiding information in many different dimensions offering multiple degrees of freedom.[2] In 1995, Refregier and Javidi[3] proposed a Double Random Phase Encoding (DRPE) method to optically encode an amplitude image into a stationary white noise pattern. Their method involves multiplication of the image by random phase screens both in the input (space) and Fourier (spatial frequency) planes. Following this work, several other methods have appeared in the literature including digital optical stream cipher,[4] optical XOR image encryption,[5] and information encryption techniques involving phase-shifting interferometry,[6] fractional Fourier transformation,[7–10] and polarization encoding.[11] The results indicated that a high level of security can be achieved by applying such techniques.

Watermarking is an effective way to provide copyright protection and data tracking security, for many types of information including fingerprinting, broadcast monitoring, data authentication, indexing, and medical safety.[12] Watermarking can be traced back to the steganography technique, which is the science of writing hidden messages in such a way that the presence of the messages cannot be detected.[13] The information hidden by watermarking

Further author information: (Send correspondence to John T. Sheridan)
John T. Sheridan: E-mail: John.Sheridan@ucd.ie

Optics and Photonics for Information Processing VI, edited by Abdul A. S. Awwal, Khan M. Iftekharuddin,
Proc. of SPIE Vol. 8498, 84980R · © 2012 SPIE · CCC code: 0277-786/12/$18 · doi: 10.1117/12.2007660

systems may be associated to its owner or the digital object to be protected and the embedded watermark should not easily be removed. 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 in secret.[14] Watermarking is either "visible" or "invisible". 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 and thus to make an assertion about the ownership of the object.[15] In order to be effective, a watermark should have several important characteristic: (i) unobtrusiveness (perceptually invisible or its presence should not interfere with the host being protected); (ii) robustness (difficult to remove and immune from common signal processing, common geometric distortions, and subterfuge attacks), (iii) universality (applicable to all three media, i.e. image, audio and video data), and (iv) unambiguousness (retrievable).[16]

A new numerical invisible image watermarking technique using Double Random Phase Encoding (DRPE) is proposed in this paper. The watermark information (we choose a barcode image in this paper) is numerically encrypted using a simulation of the optical DRPE process which transforms the barcode into a random noise like image that has its energy spread both in the space and the spatial frequency domains. This encrypted image is then further processed so that it can be easily added to a digital host image, while remaining hidden and being imperceptible. To detect the barcode the watermarked image is input to a numerical inverse DRPE process. The barcode is decrypted and can be separated from the host image which has its energy spread both in the space and spatial frequency domains by the inverse DRPE, using a low pass filter. The general algorithm is described in Section 2.

2. GENERATING AND EMBEDDING THE WATERMARK

2.1 Initial Preparation of the Barcode

A barcode is an optical machine-readable representation that contains data about the object to which it attaches. Originally barcodes represented data by varying the widths and spacings of parallel lines, and were therefore linear or one-dimensional (1D) representations. Barcodes such as the Universal Product Code (UPC), have become ubiquitously elements of modern life. Almost every item that is commercially sold is done so with a UPC barcode. Barcodes are also widely used in health care and hospital settings, for applications ranging from patient identification to the management of medication.

However our use of the barcodes here is not only because they are widely used for identification, but also because: (i) they typically only have two levels, i.e. 0 (black) and 1 (white), making them easier to embed and detect particularly for the method of watermarking extraction proposed in this paper, and (ii) they are inherently one dimensional images which also facilitates our watermark extraction procedure as described in Section 3. In this paper we choose a barcode size $M_x \times N_y$, where the pixel size of the host image we intend to watermark is given by $N_x \times N_y$. For the purpose of the simulations presented in this paper, $N_x = N_y = 1024$, and M_x is the width in pixels in the n_x direction where $M_x = W_{Ix}$ and M_x less than or equal to N_x. The barcode is zeropadded to form an image of size $N_x \times N_y$ matching the size of the host image. In Fig. 1(a) we present a sample barcode image with $M_x = 256$ and $N_y = 1024$. For the preparation of detection results in Section 4, we investigate this barcode image by integrating all its values along the n_y direction to form a 1D signal shown in Fig. 1(c), and we show the pixel range in n_x where $508 \leq n_x \leq 517$ for the comparison in later sections. In Fig. 1(d) we present the DFT of this barcode image, and in Fig. 1(e) we give the distribution of the logarithm of this barcode image's energy in the spatial frequency domain (for the centre horizontal strip $m_y = 513$) by applying a DFT. In fact, all of the energy is concentrated at the low spatial frequencies in m_x and located in the row of $m_y = 513$. We employ a low-pass filter in Section 6 to extract the watermark based on this characteristic.

2.2 Applying the numerical implementation of DRPE

In this paper we apply the method for the numerical simulation of DRPE described in,[17] which discusses the capacity of DRPE to spread a signal's energy in both the space and spatial frequency domains. The standard optical DRPE system is illustrated in Fig. 2(a), and the discrete counterpart of the optical DRPE system is shown in Fig. 2(b). Two diffusers, $D1(n_x, n_y)$ and $D2(m_x, m_y)$, are generated in order to satisfy the sampling considerations discussed in.[17] In our simulation we choose the optimal "bandwidth ratio": 0.8 in n_x-axis and 0.2

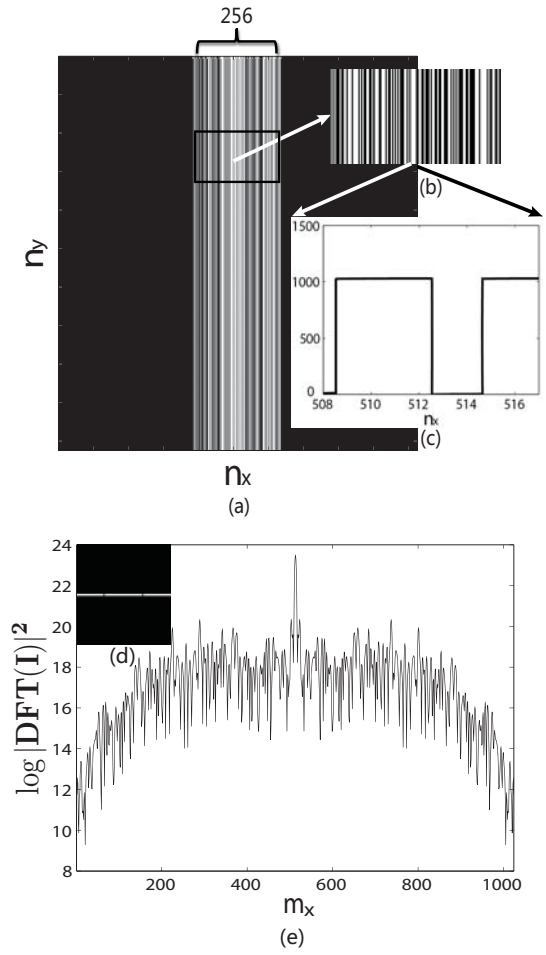


Figure 1. (a) The barcode image, $I(n_x, n_y)$, where $M_x = 256$ and $N_x = N_y = 1024$; (b) Magnified barcode image in a particular region; (c) The 1D signal over n_y direction where $508 \leq n_x \leq 517$ and $n_x \in [1, N_x]$; (d) The distribution of the DFT of the barcode image; and (e) The distribution of the logarithm of this barcode image's energy, $\log |DFT(I)|^2$, where $m_y = 513rd$ in the spatial frequency domain.

in n_y-axis for $D1(n_x, n_y)$; 0.2 in n_x-axis and 0.8 in n_y-axis for $D2(m_x, m_y)$. These two narrowband diffusers are shown in Fig. 3 with their corresponding phases. As a result of bandwidth ratios we choose for the two diffusers, their phases are elongated in horizontal and vertical directions respectively and shown in Fig. 3(c) and Fig. 3(d). We then encrypt the barcode image, $I(n_x, n_y)$, using these two suitable diffusers $D1(n_x, n_y)$ and $D2(m_x, m_y)$. $E(n_x, n_y)$ denotes the encrypted barcode image.

2.3 Making the Encrypted Image Real Valued

Since the digital images studied here are real valued only, the encrypted barcode image is made real by adding it to it's own conjugate:

$$E_R(n_x, n_y) = E(n_x, n_y) + E^*(n_x, n_y), \tag{1}$$

where $E_R(n_x, n_y)$ is the real valued encrypted image and $*$ again denotes the conjugate operation. Since $DRPE_N$ is a linear system, if we input the real valued signal $E_R(n_x, n_y)$ to the inverse $DRPE_N^{-1}$ system we decompose the output into two separate terms. Eq. (2) below describes the details of the decryption process.

$$\begin{aligned} \tilde{I}(n_x, n_y) &= DRPE_N^{-1}\{E_R(n_x, n_y), D1(n_x, n_y), D2(m_x, m_y)\} \\ &= I(n_x, n_y) + \mathcal{DFT}^{-1}\Big\{\mathcal{DFT}^{-1}\{E^*(n_x, n_y)\} \times D2^*(m_x, m_y)\Big\} \times D1^*(n_x, n_y). \end{aligned} \tag{2}$$

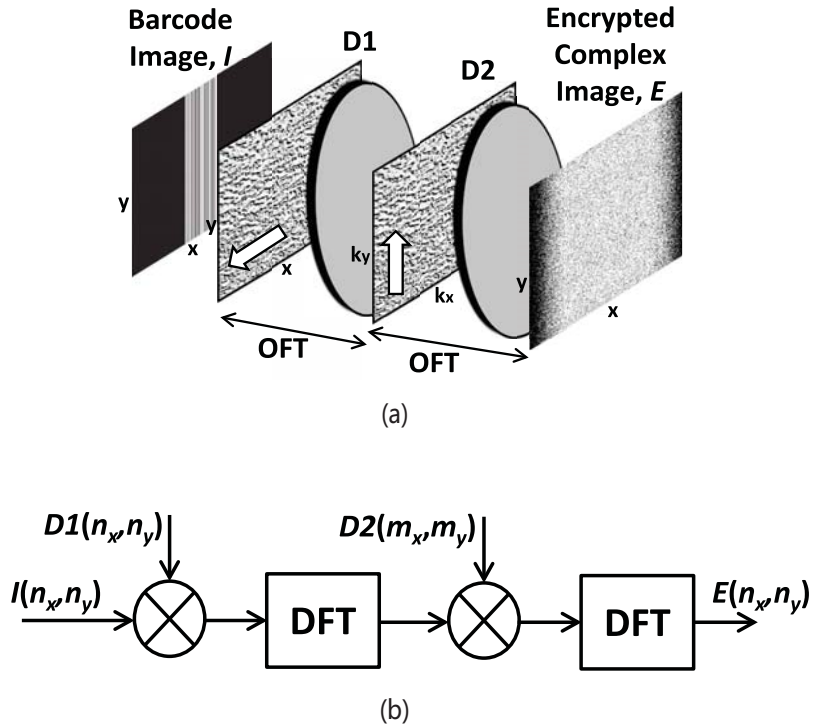


Figure 2. The illustration of the DRPE: (a) The standard optical DRPE system; (b) The discrete counterpart of the optical DRPE system.

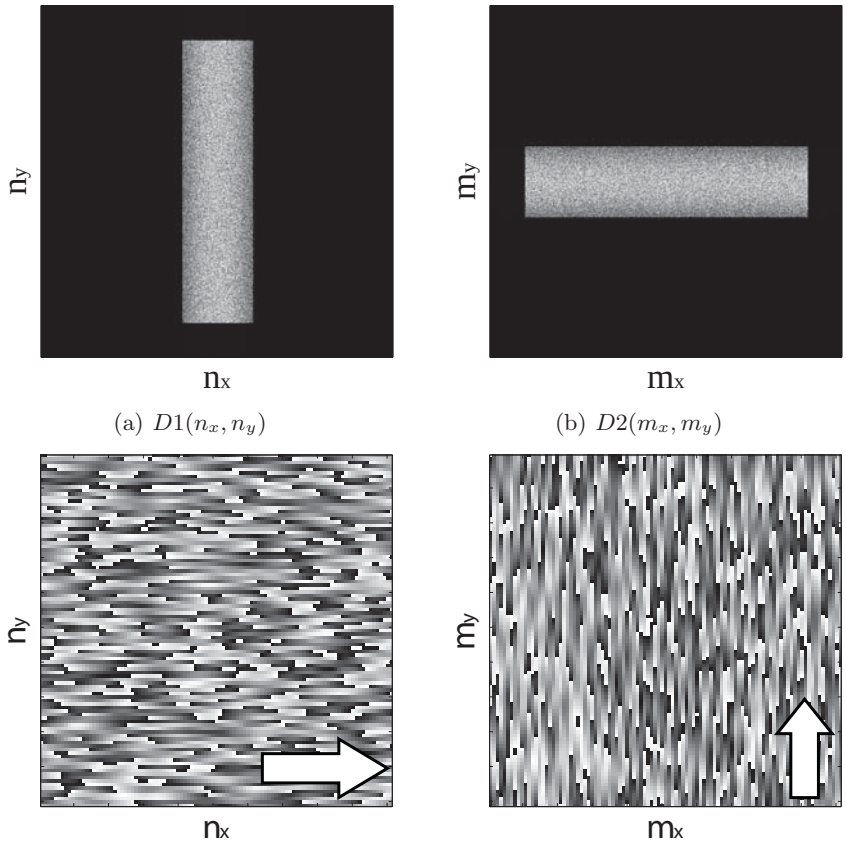
As can be seen, two images are decrypted: (i) the original barcode image $I(n_x, n_y)$ and (ii) the decryption of $E^*(n_x, n_y)$. Table 1 describes the widths and bandwidths for the two terms, $E(n_x, n_y)$ and $E^*(n_x, n_y)$, as they pass through the decryption system. The energy of $E^*(n_x, n_y)$ term will be even further spread both in the space and spatial frequency domains. This term appears as a speckle like noise that overlays the correctly decrypted barcode image, as shown in Fig. 4(a). In Fig. 4(c) we also describe this noise by integrating over n_y where $513 \leq n_x \leq 517$ and $n_x \in [1, N_x]$. In order to remove the noise, we apply a low pass filter (discussed in detail in Section 6) to the real valued decrypted barcode image, $\tilde{I}(n_x, n_y)$. Fig. 4(d) shows a result of the low-pass filtering giving a 1D barcode signal in the same range of pixels, and we can see that the speckle noise is reduced significantly.

Table 1. Quantifying the decrypted terms of the watermarked image.

Terms	Width	Bandwidth
$DRPE_N^{-1}\{E\}$	W_{Ix}	B_{Ix}
$DRPE_N^{-1}\{E^*\}$	$W_{Ix} + 2B_{D2x}$	$B_{Ix} + 2B_{D1x}$
$DRPE_N^{-1}\{Q_l\}$	$W_{Qlx} + B_{D2x}$	$B_{Qlx} + B_{D1x}$
$DRPE_N^{-1}\{H\}$	$W_{Hx} + B_{D2x}$	$B_{Hx} + B_{D1x}$

2.4 Quantization

Typically, the watermark should be hidden with the user unaware that the image is watermarked. Importantly, the host image quality should not be reduced after embedding the watermark, which means the image should be indistinguishable to that before the watermark was embedded. If we need the watermark to be invisible,



(a) $D1(n_x, n_y)$ (b) $D2(m_x, m_y)$

(c) Phase of $D1(n_x, n_y)$ (d) Phase of $D2(m_x, m_y)$

Figure 3. The two narrowband diffusers and their phase values: (a) $D1(n_x, n_y)$, (b) $D2(m_x, m_y)$, (c) Phase of $D1(n_x, n_y)$ and (d) Phase of $D2(m_x, m_y)$.

the energy in the watermark must be much less than the energy in the host image and evenly spread across it. Therefore, quantizing the real valued encrypted image to a lower numbers of grayscale levels is necessary before it is embedded into the host image.

The weakest possible watermark we could add would be a two lowest grayscale levels watermark. The energy of such a watermark would therefore be relatively week compared with the 256-level host image. We exam three possible quantization levels, i.e., 2-level, 4-level, and 8-level watermarking in our simulation. When we decrypt this quantized watermark, the additive quantization noise $Q_l(n_x, n_y)$ will add into the real valued encrypted image $E_R(n_x, n_y)$, and $Q_l(n_x, n_y)$ can be given by, $\min\big(E_R(n_x, n_y)\big) * l + 0.5$, due to the normalization and shifting procedures. Therefore the watermark can be described as follows:

$$\begin{aligned} E_{Q_l}(n_x, n_y) &= E_R(n_x, n_y) + Q_l(n_x, n_y) \\ &= E(n_x, n_y) + E^*(n_x, n_y) + Q_l(n_x, n_y). \end{aligned} \tag{3}$$

2.5 Creating the Watermarked Image

A watermark-embedding procedure is imperceptible if observers cannot distinguish the original data from the data with the inserted watermark. Eq. (4) indicates that the quantized watermark being added into the host image.

$$\bar{H}(n_x, n_y) = E_{Q_l}(n_x, n_y) + H(n_x, n_y), \tag{4}$$

where, $\bar{H}(n_x, n_y)$ is the watermarked image, $E_{Q_l}(n_x, n_y)$ is the watermark we generated, and $H(n_x, n_y)$ is the host image. In our simulation, we choose a grayscale host image with 256 gray levels.[18] When adding into the

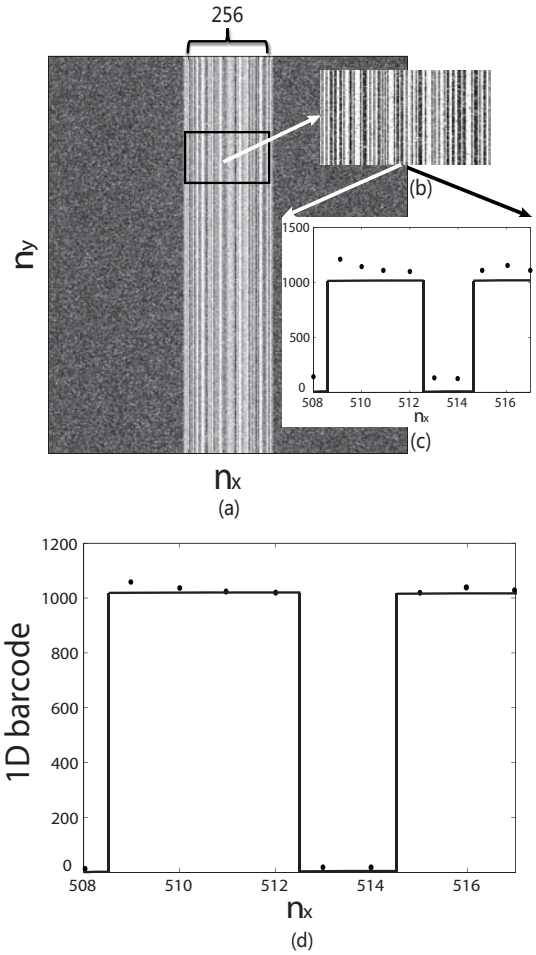


Figure 4. (a) Decrypted real valued encrypted barcode image with speckle noise, where $M_x = 256$ and $N_x = N_y = 1024$; (b) Magnified barcode image in a particular region; (c) The 1D signal (in dots) over n_y direction where $508 \leq n_x \leq 517$ and $n_x \in [1, N_x]$; (d) Decrypted 1D barcode (in dots) signal in the same n_x pixel range after the low-pass filter.

host image, the gray levels of the watermarked image are kept between 0 and 255 if we add over the maximum level 255, i.e., forcing all gray levels exceeding 255 to be 255 exactly. The watermark is undetectable after embedding. No significant changes in the host image can be visually observed for any of the quantization levels watermarks examined here.

3. DETECTION OF THE WATERMARK

The procedure for detecting the barcode in the 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, and (iii) removing the margins outside the barcode's width, W_{Ix}, and obtaining the $M_x \times N_y$ barcode image. The first two parts have the optical implementation shown in Fig. 5(a). The discrete counterpart is given in Fig. 5(b).

First, the watermarked image is decrypted through the inverse $DRPE_N^{-1}$ scheme. The decryption process

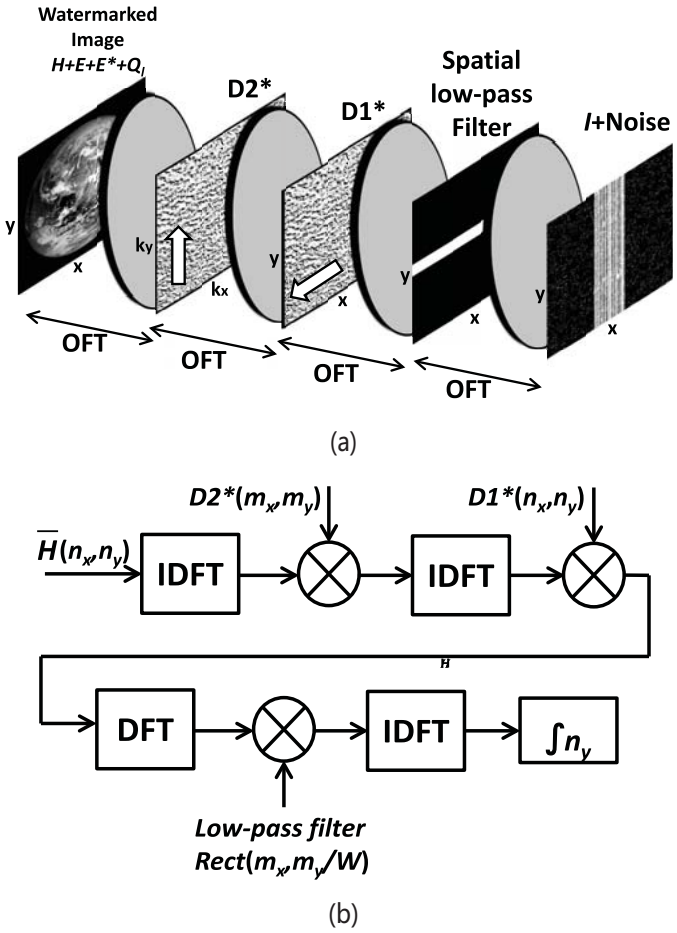


Figure 5. The illustration of detecting the watermark image: (a) Optical inverse DRPE system with a spatial low-pass filter; (b) The numerical simulation of this extraction procedure.

can be described as follows:

$$\begin{aligned}\tilde{I}(n_x,n_y) &= DRPE_N^{-1}\{\bar{H}(n_x,n_y), D1(n_x,n_y), D2(m_x,m_y)\}\\ &= I(n_x,n_y) + DRPE_N^{-1}\{E^*(n_x,n_y), D1(n_x,n_y), D2(m_x,m_y)\}\\ &\quad + DRPE_N^{-1}\{Q_l, D1(n_x,n_y), D2(m_x,m_y)\}\\ &\quad + DRPE_N^{-1}\{H, D1(n_x,n_y), D2(m_x,m_y)\}.\end{aligned} \tag{5}$$

As can be seen, the decrypted image is made up of four separate terms. We can investigate the support of each of these terms independently due to the linearity of the system. The evolutions of the widths and bandwidths of the four decrypted terms, as the watermarked image propagates through the decryption system, can be seen in Table 1. Only the first term $DRPE_N^{-1}\{E, D1, D2\}$ contracts to reform the original barcode image $I(n_x, n_y)$. However, the presence of the other three terms produces a strong speckle noise, dominated by the host image term, making it difficult to detect the watermark.

The optical decryption system is followed by a third OFT and the signal then passes through a spatial filter (low pass filtering in the k_y dimension, i.e. $rect(k_y/W)$ where W is the width of the filter), which is followed by a fourth OFT to return to the space domain. Then a 1D detected barcode signal is obtained since only the 513rd row of the decrypted watermarked image in the frequency domain passes through the low pass filter. The centrally localized energy of the barcode remains while the strong speckle noise has been significantly reduced

since it was spread throughout the frequency domain. We evaluate the efficiency of this low pass filter by calculating the SNR of the detected barcode image. SNR is defined as the ratio of signal energy to the noise energy as follow:

$$\mathrm{SNR}_{dB} = 10 \log_{10} \frac{P_{signal}}{P_{noise}}, \tag{6}$$

where SNR is measured in decibels. P_{signal} represents the energy of the original barcode signal and P_{noise} represents the energy of the noise signal dominated by the host image term in the detected barcode image.

In order to detect the presence of the barcode, it is important to note that the watermark should not be too weak. For this reason we have found it is necessary to make the barcode width smaller enough (we choose a width of 16 pixels in our simulation) – thereby compressing the energy of the barcode image as much as possible and making it visible following decryption even in the presence of the strong noise. In the case of $W_{Ix} = 16$ and $l = 2$ in our simulation, the SNR of the extracted barcode image is 101.88 dB.

4. SIMULATION RESULTS

In this section, we present the results of the watermark detection using different quantization levels and different barcode widths. In order to evaluate the detection results, steps 1-2 as follows can be used:

1. We first bin the 1D detected barcode signal into a binary sequence with 0s and 1s using a suitable threshold. All the pixel values greater than the threshold are set to 1 and otherwise are set to 0. We note this binary sequence as the detected 1D barcode.

2. Then we calculate the total different numbers of pixel values, n_{err}, between this detected 1D barcode and the original 1D barcode. Therefore, the detection error percentage, p_{err}, can be obtained by n_{err}/W_{Ix}.

In our simulation, we first examine the case of $W_{Ix} = 256$ and $l = 2$. Fig. 6(a) shows an illustration of the detected barcode image, $\tilde{I}(n_x, n_y)$, and its magnified barcode image in a particular region is given in Fig. 6(b). In Fig. 6(c) we present the 1D barcode signal in dots where $508 \leq n_x \leq 517$. To evaluate this detection result, we apply steps 1-2 above and obtain the detection error percentage that $p_{err} = 26.5625\%$. In Fig. 6(d) we present the detected 1D barcode and the original 1D barcode in dots and solid line respectively in the same n_x pixel range. As can be seen, $n_{err} = 2$ and $p_{err} = 25\%$ in this pixel range in this case. Results for the case of $W_{Ix} = 16$ and $l = 2$ are shown in Fig. 7. For the purpose of comparison, we pick out the 16 pixels where $505 \leq n_x \leq 520$ particularly from the $W_{Ix} = 256$ barcode image case. The detection error percentage was found to be $p_{err} = 0$. We can see that the detected 1D barcode and the original 1D barcode are exactly the same in Fig. 7(d) .

Table 2 gives the simulation results of the detection error percentage (p_{err}) using different barcode widths including $W_{Ix} = 16, W_{Ix} = 32, W_{Ix} = 64, W_{Ix} = 128$, and $W_{Ix} = 256$, and different quantization levels including 2-level, 4-level, and 8-level. We may conclude that the smaller the barcode width is, and the larger quantization level is, the more accurate the detection will be. When $W_{Ix} = 16$, the perfect detection with no errors appears in all different quantization levels, which indicates the feasibility of our proposed method.

Table 2. Simulation results for the detection error percentage (p_{err}) using different barcode widths (W_{Ix}) and different quantization levels (l).

level (l) / **Barcode (W_{Ix})**	2-level (%)	4-level (%)	8-level (%)
16	0	0	0
32	0	0	0
64	3.125	1.5625	0
128	10.1563	9.375	8.5938
256	26.5625	24.2188	19.5313

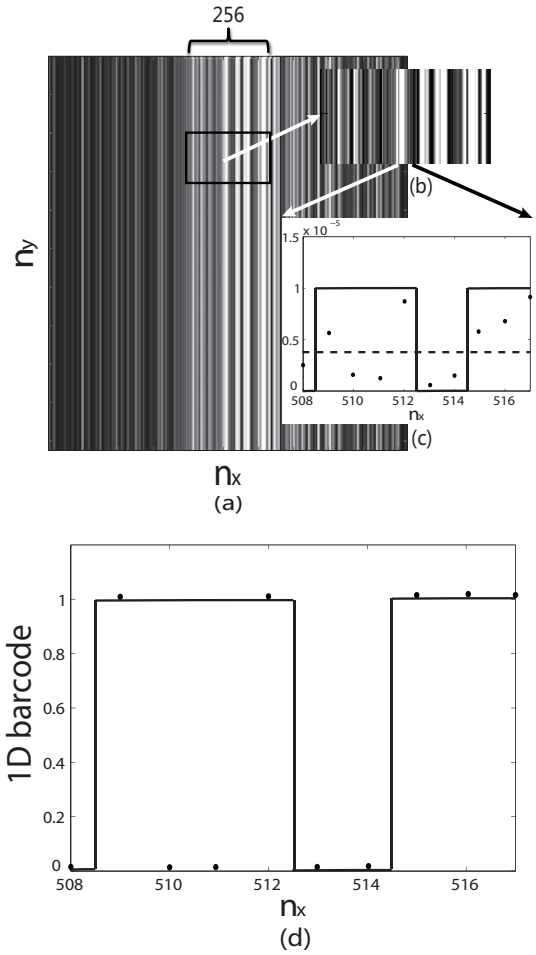


Figure 6. The illustration of the detection results in the case of $W_{Ix} = 256$ and $l = 2$, including: (a) The detected barcode image, $\tilde{I}(n_x, n_y)$; (b) Magnified detected barcode image in a particular region; (c) The 1D signal (in dots) of this detected barcode image over n_y where $508 \leq n_x \leq 517$ and $n_x \in [1, 1024]$, with the threshold in dashed line; and (d) The detected 1D barcode in dots and the original 1D barcode in solid line.

5. CONCLUSION

In summary, we have proposed a digital invisible image watermarking technique using as the basis, the optical encryption method known as Double Random Phase Encoding (DRPE). This method is a spread-space and spread-spectrum technique that utilizes the ability of the DRPE to spread the energy of the input information (barcode) in both the space and the spatial frequency domains using two optimally designed narrowband diffusers. We apply the discrete model of the optical DRPE system that described in.[17] To create a relatively low energy watermark, we quantize the real valued encrypted barcode image into a lower number of levels. After embedding the watermark, the host image appears unchanged indicating that the watermark is well hidden. To detect the original barcode, we apply the inverse DRPE system and a low-pass filter to appropriately extract the energy of the watermark eliminating most of energy of the incorrectly decrypted host image. The simulation results demonstrates the feasibility and robustness of the proposed scheme. It has been shown that even for lower numbers of quantization levels, e.g. the 2-level case, the watermark can still be identified with very few errors. We view our proposed watermarking method to be the combination of the concepts of "spatial watermarking methods" and "spectral watermarking methods" since we spread the energy of the watermark in both domains. Furthermore, we consider the limiting case, i.e. fully-aliasing, which is the complete discrete model with no relation to the continuous optical system. The simulation results and the properties in this case can be viewed

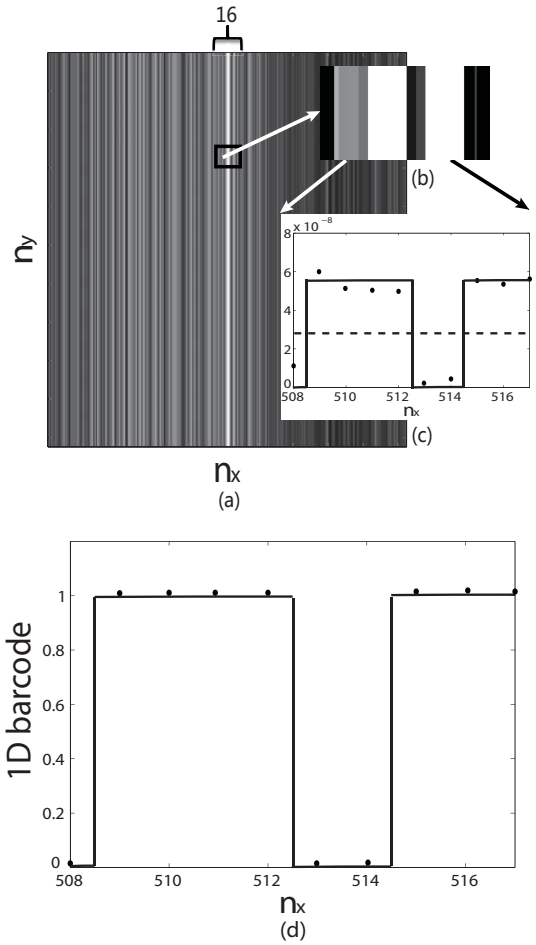


Figure 7. The illustration of the detection results in the case that $W_{Ix} = 16$ and $l = 2$, including: (a) The detected barcode image, $\tilde{I}(n_x, n_y)$; (b) Magnified detected barcode image in a particular region; (c) The 1D signal (in dots) of this detected barcode image over n_y where $508 \leq n_x \leq 517$ and $n_x \in [1, 1024]$, with the threshold in dashed line; and (d) The detected 1D barcode in dots and the original 1D barcode in solid line.

to add to the security and robustness of our method. For the future work, the robustness of our method will be quantitatively tested, which need to be proved the ability that the watermark can survive after common signal processing operations. lossy compression or some geometric distortions. Moreover, the two diffusers, which are noted as the keys for DRPE system, will be tested to quantify the security level of our method.

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. We acknowledge further support from Enterprise Ireland and SFI through the National Development Plan.

REFERENCES

[1] Langelaar, G., Setyawan, I., and Lagendijk, R., "Watermarking digital image and video data. a state-of-the-art overview," *Signal Processing Magazine, IEEE* **17**, 20 –46 (sep 2000).

[2] Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M., and Javidi, B., "Optical techniques for information security," *Proceedings of the IEEE* **97**, 1128 –1148 (june 2009).

[3] Refregier, P. and Javidi, B., "Optical image encryption based on input plane and fourier plane random encoding," *Opt. Lett.* **20**(7), 767–769 (1995).
[4] Madjarova, M., Kakuta, M., Yamaguchi, M., and Ohyama, N., "Optical implementation of the stream cipher based on the irreversible cellular automata algorithm," *Opt. Lett.* **22**, 1624–1626 (Nov 1997).
[5] Han, J., Park, C., Ryu, D., and Kim, E., "Optical image encryption based on XOR operations," *Optical Engineering* **38**, 47–54 (Jan. 1999).
[6] Tajahuerce, E., Matoba, O., Verrall, S. C., and Javidi, B., "Optoelectronic information encryption with phase-shifting interferometry," *Appl. Opt.* **39**, 2313–2320 (May 2000).
[7] Hennelly, B. and Sheridan, J., "Image encryption and the fractional fourier transform," *Optik - International Journal for Light and Electron Optics* **114**(6), 251 – 265 (2003).
[8] Unnikrishnan, G., Joseph, J., and Singh, K., "Optical encryption by double-random phase encoding in the fractional fourier domain," *Opt. Lett.* **25**, 887–889 (Jun 2000).
[9] Liu, S., Yu, L., and Zhu, B., "Optical image encryption by cascaded fractional fourier transforms with random phase filtering," *Optics Communications* **187**(1-3), 57 – 63 (2001).
[10] Zhang, Y., Zheng, C.-H., and Tanno, N., "Optical encryption based on iterative fractional fourier transform," *Optics Communications* **202**(4-6), 277 – 285 (2002).
[11] Gopinathan, U., Naughton, T. J., and Sheridan, J. T., "Polarization encoding and multiplexing of two-dimensional signals: application to image encryption," *Appl. Opt.* **45**, 5693–5700 (Aug 2006).
[12] Podilchuk, C. and Delp, E., "Digital watermarking: algorithms and applications," *Signal Processing Magazine, IEEE* **18**, 33 –46 (jul 2001).
[13] I.J. Cox, M. M. and Bloom., J., [*Digital Watermarking*], Morgan Kaufmann Publishers (2002).
[14] I.J. Cox, M.L. Miller, J. B. J. F. and Kalker., T., [*Digital Watermarking and Steganography, 2nd Ed.*] (2008).
[15] Hsu, C.-T. and Wu, J.-L., "Hidden digital watermarks in images," *Image Processing, IEEE Transactions on* **8**, 58 –68 (jan 1999).
[16] Cox, I., Kilian, J., Leighton, F., and Shamoon, T., "Secure spread spectrum watermarking for multimedia," *Image Processing, IEEE Transactions on* **6**, 1673 –1687 (dec 1997).
[17] S. Liu, B. M. Hennelly, and J. T. Sheridan, "A numerical simulation of Double Random Phase Encoding,", *Submitted to Optical Engineering*, (2012).
[18] NASA, "1024px-antichthon." Website (2006). `http://en.wikipedia.org/wiki/File:1024px-Antichthon.jpg`.