Optical and Digital Technique for Watermark Detection

Aidan Mooney and John G. Keating

Department of Computer Science, NUI Maynooth, Maynooth, Co. Kildare, Ireland.

ABSTRACT

A digital watermark is a visible, or preferably invisible, identification code that is permanently embedded in some digital data to prove owner authentication and provide protection of that document. In this paper we utilize a watermark generation technique based on the use of chaotic functions and the motivation for using these functions is presented. The technique used for watermark embedding is also described, together with a watermark detection scheme based on an optical Matched Filter correlator. We provide results of optical simulations of the watermark detection scheme and show that correlation-based detection is an excellent method for detecting chaotically-generated watermarks embedded in the Fourier domain using multiplicative embedding. We also show that it is possible to detect chaotically-generated watermarks in images that have been subjected to noise.

Keywords: Watermarking, Chaotic Functions, Multiplicative Embedding, Matched Filtering, Noise Analysis

1. INTRODUCTION

Digital Watermarking is a rapidly developing technology which may be used to provide a certain degree of protection to a digital document from a malicious attack. Digital watermarks provide a means of placing additional information within digital media so that if copies are made, rightful ownership may be determined[1]. Although encryption of a document provides a certain degree of protection from attack, encryption techniques can only be used to protect digital data during the transmission from the sender to the receiver. After the receiver has decrypted the data, however, the original data is no longer protected[2]. It is here that watermarking may be used to embed a piece of identifying information into the document that can be used to prove ownership at a later date, and thus provide protection of the document's origin. The original owner can prove ownership of attacker copies by proving the copy contains their original watermark.

Numerous watermark generation techniques have been proposed ranging from watermarks generated from pseudorandom sequences of numbers[3] to using personal logos, *e.g.* a company logo. With regard to the use of a personal logo, the entire watermark image needs to be stored in order that watermark detection may be performed on a document. It would be much more economical, if rather than having to store the entire watermark image, a user just needed to store a single value that could be used to recreate the same watermark every time. This is the idea used in chaotically generated watermarks which have been proposed by Pitas *et al.*[4–6]

In Section 2 of this paper we describe a technique used to generate chaotic watermarks based on the logistic difference equation and Peano Scanning. Section 3 outlines the watermark embedding technique, and in Section 4 the proposed optical watermark detection scheme, based on an optical correlator, is presented. In Section 5, simulation results are presented for watermark generation, watermark embedding and watermark detection processes. In Section 6 we present simulation results for the detection scheme in the case where noise is present on the communication channel.

Further author information:
E-mail: amooney@cs.may.ie, john.keating@may.ie

2. WATERMARK GENERATION

The watermarks used in this paper are generated using a chaotic function (or mapping) which is a function that is sensitive to some initial conditions, is unpredictable, indecomposable and yet contains regularity[7]. The motivation for using a chaotic function to generate a watermark lies in the fact that a single variable, s, seeding a chaotic function, will always result in the same output when certain constraints or initial conditions are placed on the mapping. It is much more economical to store or transmit the seed rather than the entire watermark. The chaotic watermark is derived from a chaotic sequence fully described by the map $\{y_j : y_j = f(y_{j-1}, s)\}$ and an initial condition y_0[8]. The function used for watermark generation in this paper is the logistic difference equation:

$$y_{n+1} = a y_n (1 - y_n) \tag{1}$$

although several other functions have also been used, for example, Renyi maps, Markov maps and Bernoulli maps[9].

The logistic difference equation was originally proposed for the description of the dynamics of a population of organisms that appear in discrete generations, such as insects. The value y_{n+1} is dependant on its current density y_n. For low values of s, y_n eventually converges to a single number as n goes to infinity. When s equals 3.0, y_n no longer converges – it oscillates between two values. This characteristic change in behaviour is called a bifurcation. Increasing the value of s even further causes y_n to oscillate between not two, but four values. As one continues to increase s, y_n goes through bifurcations of period 2^n and eventually becomes chaotic. When the value of s equals 3.57, y_n neither converges or oscillates - its value becomes completely random. For values of s larger than 3.57, the behaviour is largely chaotic[10]. Changing the value of s by only 0.001 will result in a totally different behaviour over time, if s is within the chaotic region.

If the logistic difference equation is seeded with $3.57 \leq s \leq 4.0$, chaotic behaviour is witnessed and it is this feature that is used to generate watermarks in this paper. A constraint is set on the values produced by the equation, whereby all values of $y_j < 0.5$ are represented in the watermark with a "zero" and values of $y_j \geq 0.5$ represented by a "one" in the watermark. Using this constraint, a 1-D sequence (of zero's and one's) is generated representing a watermark. This 1-D sequence is secure against fraudulent image altering in that it is virtually impossible to obtain the value of the pair (s, y_j). This technique is also cryptographically more secure than a pseudo-random one, because it is not invertible and the original watermark cannot be reproduced without knowledge of the appropriate key[11].

This generated 1-D sequence needs to be converted to a 2-D image of the same size as the image to be watermarked (cover image) in order for embedding to occur. To further improve the security of the watermark, a scanning technique known as Peano Scanning is used to determine the positioning of pixels within the watermark. The Peano Scanning technique is preferable to the more conventional Raster Scanning technique in that its scanning order is not predictable and can produce many variations of scanning within the same image. The Peano scan is an application of the Peano curve to the scanning of images, and it is typically used for analyzing, clustering or compressing images[12]. Any sequence of images that is a power of two may be scanned using this technique. The Peano scan always moves to a neighbouring pixel, but the pattern may appear in different orientations depending on the starting pixel within the scanning routine[13,14]. Fig. 1(a) shows a sample Peano scan of an image block of size 8×8, which can be scaled upwards for images of size $[2^k, 2^k]$. A sample of one such generated watermark, of size 256×256, is shown in Fig. 1(b) where an initial value of $s = 3.672$ was used and followed by Peano scan ordering.

3. WATERMARK EMBEDDING

Watermark embedding involves the "placing" of the watermark within some cover image in either a perceptible (visible) or imperceptible (invisible) manner. Perceptible watermarks, by their nature, are very intrusive to the media and act to deter theft of the media. Imperceptible watermarks have an advantage over perceptible ones, in that their location may be unknown to any potential attackers. However, the less perceptible a watermark is, the more vulnerable it may be to manipulation. Imperceptible watermarks only have the effect of discouraging

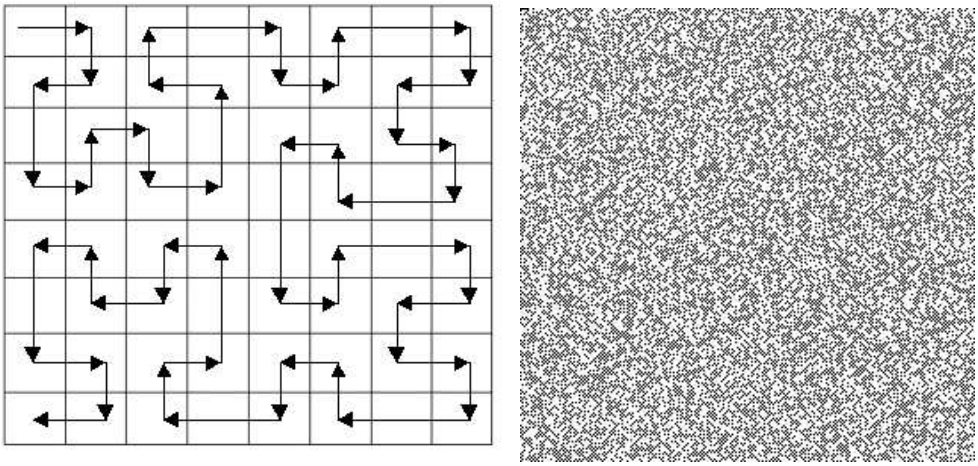

Figure 1. (a): Peano Scanning order used for an image of size 8×8 (b): A sample watermark of size 256×256.

Figure 2. (a): The original gray scale image of size 256×256. (b): Original Image corrupted with noise of intensity 50%

theft if the attacker is aware of the technology and the possibility that a watermark may be present in the image of interest[1].

For our experiments the original image, I, used is the "Lena" gray scale image of size 256×256 pixels shown in Fig. 2(a). In general, the embedding of an imperceptible watermark, may occur either in the spatial domain or in some transform domain, for example, the Fourier Domain[15], the Discrete Cosine Domain[16] or the Discrete Wavelet Domain[17]. In this paper, however, we deal with the embedding of an imperceptible watermark in the Fourier domain.

Fig. 3 shows the block diagram of the watermark embedding technique described in this paper. The original image, I, is transformed to the Fourier domain via the Fourier Transform to give the image J. The watermark, W, is also transformed to the Fourier domain to give the image X. Once we have the Fourier domain representations of both the original image and the watermark the watermark is inserted using the "multiplicative embedding technique"[18]

$$y_i = j_i + \gamma j_i x_i \tag{2}$$

where y_i is the i^{th} pixel of the watermarked image Y, j_i is the i^{th} pixel of the image J, x_i is the i^{th} pixel of the image X and γ is known as the embedding factor and controls the watermark strength[18]. γ controls the

trade-off between watermark visibility and watermark robustness within the image. The lower the value of γ the less noticeable a watermark is within an image and therefore does not noticeably alter the perceived quality of the image[19]. The image Y is now the Fourier domain representation of the watermarked image Z. This image is then transformed back to the spatial domain via the inverse Fourier Transform to give the watermarked image which may then be made available to whoever the owner wishes. This technique differs from Pitas *et al's.*[4–6] work as it embeds the watermark in the Fourier domain as opposed to embedding in the spatial domain, and as such requires a new detection technique, which is discussed in the next section.

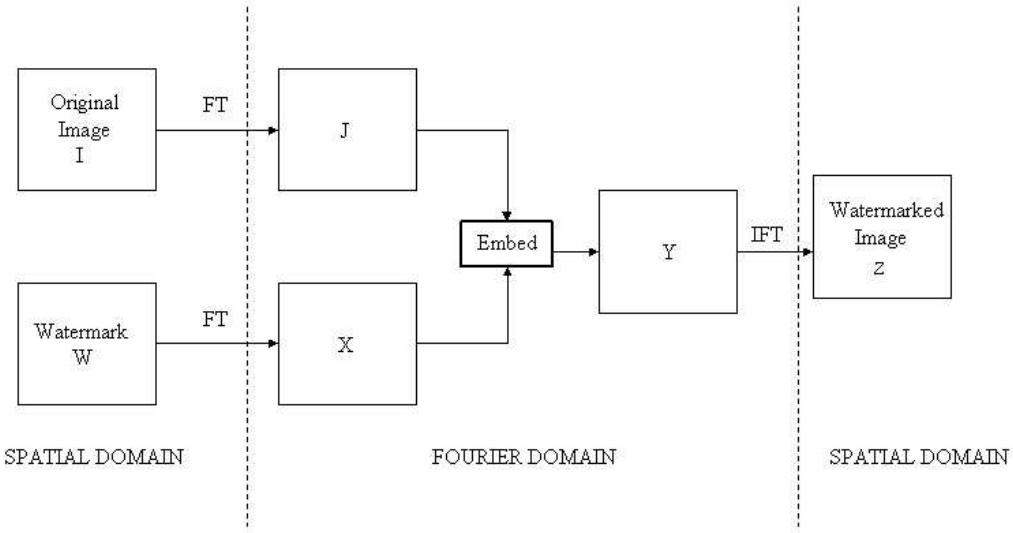

Figure 3. Block Diagram of watermark embedding procedure.

4. WATERMARK DETECTION

We have designed a chaotic watermark detection scheme suitable for optical implementation. The motivation for the use of an optical detection technique is that optical processing is faster than a similar digital technique due to the inherent parallelism of the system[20]. The optical correlator was invented in 1964 by Anthony VanderLugt and its basis structure is shown in Fig. 4. The optical correlation technique discussed is based on the Matched Filtering technique[21,22] which is known to be an effective technique for watermark detection.

Optical Correlation is a computational technique in which an incoming signal is compared to a previously calculated reference, known as a filter. In this technique the spectrum of a target object is caused to interfere with a reference beam in the Fourier plane and the resulting interference pattern recorded and used as a filter, F. This filter is then reinserted into the Fourier plane to act as a matched spatial filter. An input signal, s, is placed in the input plane and is illuminated, and optically Fourier transformed to S. This signal is then optically mixed with the filter F in the Fourier plane. The new signal is again optically Fourier transformed to produce the correlation signal between the input image and the filter[23].

Fig. 5 shows the optical configuration of a Matched Filtering technique. In the output plane the presence of the signal can be detected by measuring the intensity of the light. If the input image is not centered on the origin, the bright point in the output plane simply shifts by a amount equal to the amount it is off origin[24]. The image being searched for, in this case the watermark, is used to generate the filter using the Fourier Transform. This filter is placed in the Fourier Domain of the optical configuration. The input image, which in this case is the possibly watermarked image, is placed in the input plane and displayed on an Spatial Light Modulator (SLM). This SLM is illuminated and the resulting signal Fourier transformed by lens $L2$, which then interferes with the filter present in the Fourier plane. Lens $L3$ performs an inverse Fourier transform on the input presented to it. The output, in the spatial domain, is the correlation signal produced between the input image and the

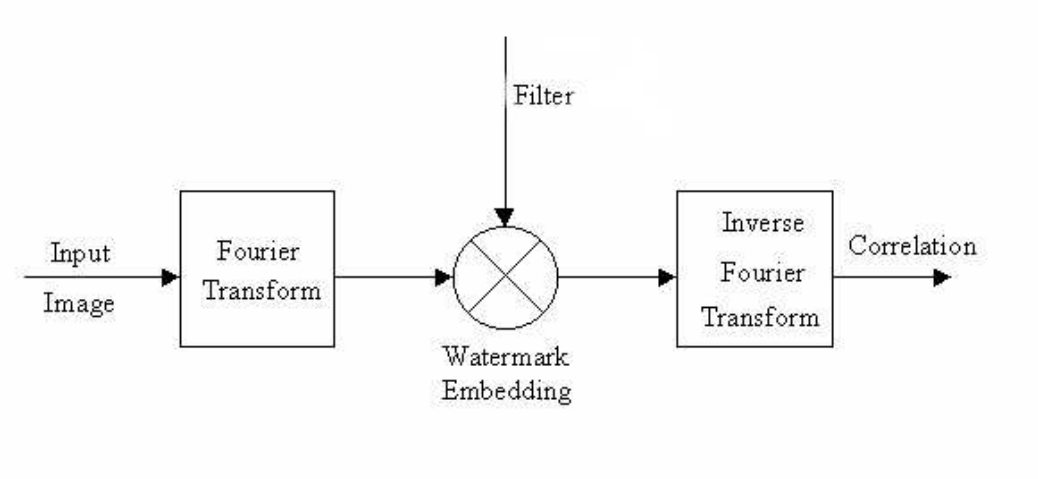

Figure 4. Overview of the Optical Correlation Procedure.

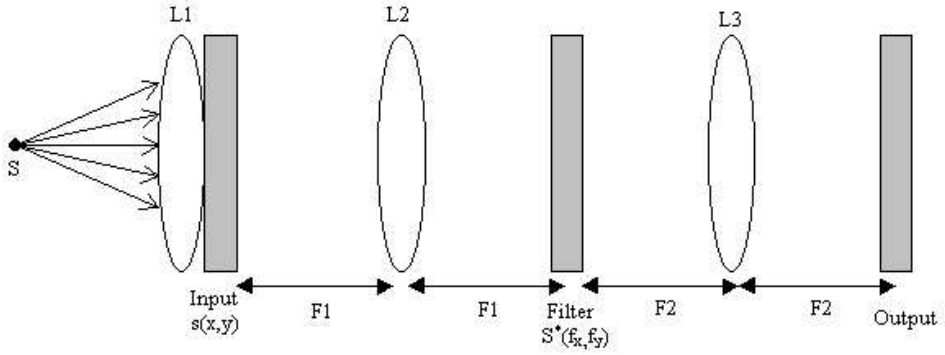

Figure 5. The optical configuration of the Matched Spatial Filter.

watermark. The proposed detection scheme presented was modelled and the simulation results are presented in Section 5.

5. SIMULATION RESULTS

Simulations of our watermark embedding and Matched Filtering detection techniques have been carried out using Matlab. The proposed techniques have been investigated using the 256×256 "Lena" cover image shown in Fig. 2(a) and the 256×256 watermark shown in Fig. 1(b). Watermark embedding takes place as is described in Section 3. The resulting watermarked image is calculated and embedded in the original image as previously described. There is little if any perceptual difference between the original image and this watermarked image, which is a fundamental requirement of a watermarking system[25].

For the detection system, the possibly watermarked image together with the watermark whose presence one wishes to determine in the image are used as inputs to the detector. The watermark is used as a filter and this filter is generated as previously discussed. The detection technique returns an output image which is the correlation between the possibly watermarked image and the watermark. The presence of the watermark in the possibly watermarked image may be determined by correlating these two images. If the watermark being searched for, is present in the watermarked image one would expect a single correlation peak when a correlation is performed on the two images. If the watermark is not present or if a different watermark is present one would not expect to get a single correlation peak but a more uniform distribution of correlation peaks in the output.

Fig. 6(a) gives the output of the detection technique when a watermarked image, and the watermark of interest, are presented as inputs to the detector. This result is for the case where the image shown in Fig. 2(a) is watermarked with the image shown in Fig. 1(b). In this case a single sharp correlation peak is observed in the correlation plane which is in keeping with what one expects in such a case. This indicates that the image presented to the correlator at the input plane has been watermarked with the reference used to generate the filter used in the detection technique.

Fig. 6(b) shows the output of the detection technique for an image containing the watermark of interest (one obtains the sharp correlation peak) and the case when a different watermark is used in the filter. In the case of the latter, there is no single sharp correlation peak but a broader distribution of peaks which is what one expects in such a case. This indicates that the watermarked image has not been watermarked with the particular watermark. A similar result is found when an image which has no watermark present in it is correlated with any watermark.

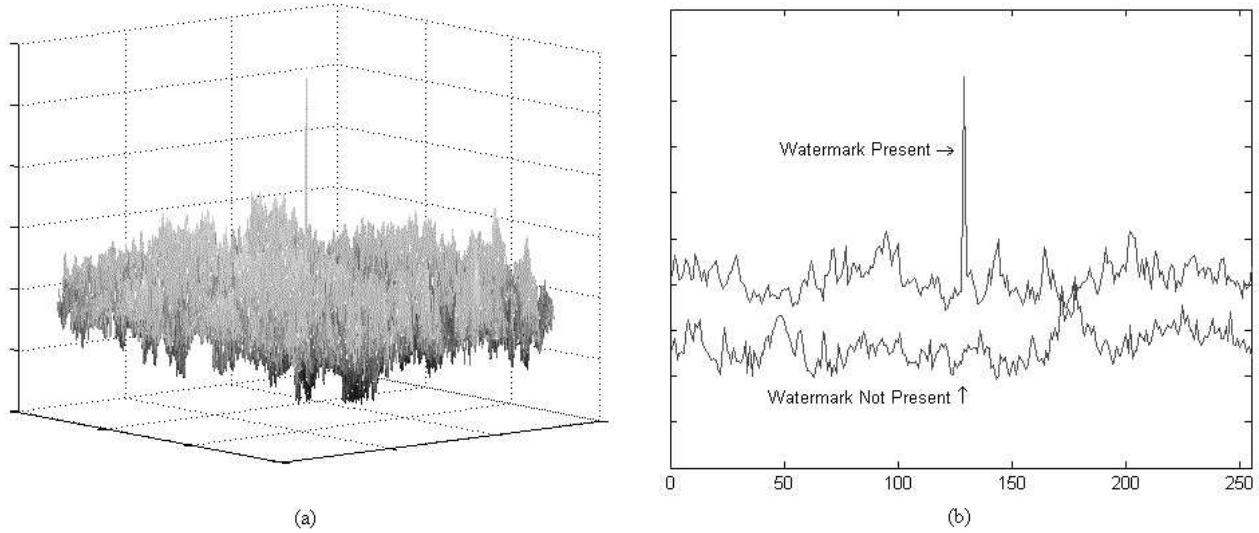

Figure 6. (a): Correlator Output when a particular watermark is present (b): Correlator Output when a particular watermark is present and when there is no watermark present in the input image.

From our simulations of the correlation-based detector, we have observed that it is possible to determine whether an image is watermarked with a particular watermark, or otherwise, just by observing the pattern returned from the detector in the output plane. If the observed output of the detector simulation results in a single correlation peak we can say that the watermarked image has been watermarked with the watermark presented in the input plane. However, if the observed output contains a broader distribution of correlation peaks one can say that the image presented at the input plane has not been watermarked with the watermark presented to the filter. By observing this pattern we can say with a certain degree of confidence (although this confidence level has yet to be estimated) that the image is either watermarked with the watermark which is presented to the detection correlator or is not watermarked with the watermark.

6. NOISE ANALYSIS

Images processed by an optical system are often degraded by some random errors – this degradation is usually called noise and may occur during image capture, transmission or processing[26]. Noise may also be present as random background signals in transmission or communication signals. This shot noise is caused by the random fluctuations in the motion of charge carriers[27], and may be modelled by a Poisson distribution. We are interested in the performance of the detection scheme when a watermarked image is corrupted with noise, and have therefore, conducted experiments on watermarked images with various levels of noise intensity, *e.g.* the watermarked image Fig. 2(a) corrupted with a 50% noise intensity is shown in Fig. 2(b). Fig. 7(a) shows the

detector output in the case where the watermarked image was subjected to noise with an intensity level of 5%, and was then presented together with the watermark as inputs to the detector. It can be seen that there is a distinct correlation peak for this cases which suggests that the proposed scheme is resistant to noise at that intensity.

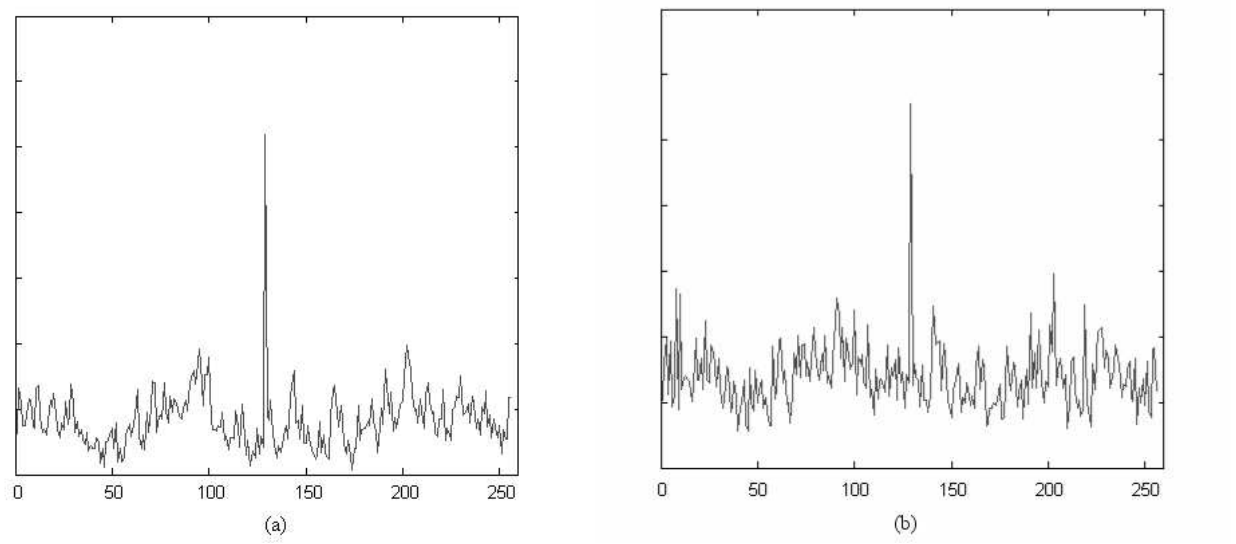

Figure 7. (a): Correlator output in the case where the watermarked image has been corrupted by noise with an intensity level of 5% and the watermark is embedded (b): Correlator output in the case where the watermarked image has been corrupted by noise with an intensity level of 20% and the watermark is embedded.

The detection procedure was also repeated in the case where there was no watermark embedded into an image that was noise corrupted. This unwatermarked image together with the watermark shown in Fig. 2(a) were presented as inputs to the detector and we found that no single distinct peak in the output was observed. This correctly indicated that the image had not been watermarked with the watermark presented to the detector. This is also the correlator output obtained when a watermark and a watermarked image, which has been watermark by a different watermark, are presented to the detector. This is not a problem, however, as the purpose of the detector is to determine if a specific watermark exists in the test image.

The above results are for the case where the noise intensity added to the original image was of a low degree. We have also determined that increased noise intensity ($\leq$50%) does not impact on the ability of the detection system to correctly determine watermark presence. Fig. 7(b) shows the correlation output in the case where the watermarked image was subjected to a noise intensity of 20%. It can be seen in the cases where noise intensities of 5% and 20% corrupt a watermarked image, that a distinct correlation peak is still present in the output, indicating that the detection scheme is robust when images are subjected to noise of these intensities.

7. CONCLUSION

We have demonstrated a watermark detection scheme based around an optical correlator using matched filtering. The use of an optical technique is favoured over a similar digital technique, due to the fact that optical processing is faster due to the inherent parallelism of the system. The detector discussed is used to verify the existence or absence of a watermark within a possibly watermarked image. When a watermark is present in an image and these images are presented to the detector a sharp correlation peak is observed in the output plane. If, however, the watermark was not present there is no single correlation peak present in the output plane. This technique has been shown to be an effective technique for watermark detection and is shown to be robust to noise in the watermarked image arising from the optical system or otherwise.

REFERENCES

1. N. F. Johnson, "An introduction to watermark recovery from images," *Proceedings of SANS Intrusion Detection and Response Conference* , 1999.
2. G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state of the art overview," *IEEE Signal Processing* **17**, pp. 20–46, 2000.
3. I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio, and video," *IEEE International Conference on Image Processing (ICIP'96)* **III**, pp. 243–246, 1996.
4. A. Nikolaidis and I. Pitas, "Comparison of different chaotic maps with application to image watermarking," *IEEE International Symposium on Circuits and Systems, Geneva* , 2002.
5. N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing,Elsevier* **66**, pp. 385–403, 1998.
6. S. Tsekeridou, V.Solachidis, N.Nikolaidis, A.Nikolaidis, A. Tefas, and I.Pitas, "Bernoulli shift generated watermarks: Theoretic investigation," *IEEE Int. Conf. on Acoustics, Speech and Signal Processing* , 2001.
7. R. L. Devaney, *A first course in Chaotic Dynamical Systems - Theory and Experiment*, Perseus Books, Cambridge, Massachusetts, 1992.
8. A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Markov chaotic sequences for correlation based watermarking schemes," *International Conference on Nonlinear Dynamics (NLD'01), Thessaloniki, Greece* , 2001.
9. A. Nikolaidis and I. Pitas, "Comparison of different chaotic maps with application to image watermarking," *IEEE Symposium on Circuits and Systems* , 2000.
10. M. Marek and I. Schreiber, *Chaotic Behaviour of Deterministic Dissipative*, Cambridge University Press, Cambridge, 1991.
11. A. Nikolaidis and I. Pitas, "Region-based image watermarking," *IEEE Transactions on Image Processing* **10**, 2001.
12. A. C. Ansari, I. Gertner, and Y. Y. Zeevi, "Combined wavelets-dct image compression," *SPIE Proc. Signal Processing, Sensor Fusion and Target Recognition* **1699**, pp. 308 – 317, 1992.
13. K. Yang and M. Mills, "Fractal based image coding scheme using peano scan," *ISCAS '88* **1470**, pp. 2301–2304, 1988.
14. R. Stevens, A. F. Lehar, and F. Preston, "Manipulation and presentation of multidimensional image data using the peano scan," *IEEE Trans. Patterm Pattern Anal. Machine Intell* , 1983.
15. V. Licks and R. Jordan, "On digital image watermarking robust to geometric transformations," *IEEE International Conference on Image Processing* , 2000.
16. A. . Piva, M. Barni, F. Bartolini, and V. Cappellini, "Dct-based watermark recovery without resorting to the uncorrupted original image," *International Conference on Image Processing (ICIP '97)* , 1997.
17. P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," *SPIE Symposium, Electronic Imaging, Conference on Security and Watermarking of Multimedia Contents* .
18. M. Barni, C. I. Podilchuk, F. Bartolini, and E. J. Delp, "Watermark embedding: Hiding a signal within a cover image," *IEEE Communications* **39**, 2001.
19. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, London, 2002.
20. J. Rosen, "Three-dimensional optical fourier transform and correlation," *Optics Letters* **22**, 1997.
21. M. Shen, X. Zhang, L. Sun, P. J. Beadle, and F. H. Y. Chan, "A method for digital image watermarking using ica," *4th International Symposium on Independent Component Analysis and Blind Signal Separation* , 2003.
22. A. Sequeira and D. Kundur, "Communication and information theory in watermarking: A survey," *Multimedia Systems and Applications IV, A. G. Tescher, B. Vasudev, and V. M. Bove, eds., Proc. SPIE* **4518**, pp. 216 – 227, 2001.
23. P. Birch, S. Tan, R. Young, T. Koukoulas, F. Claret-Tournier, D. Budgett, and C. Chatwin, "Experimental implementation of a wiener filter in a hybrid digital/optical correlator," *Optics Letters* **26**, pp. 494 – 496, 2001.
24. J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill Publishing, Singapore, 1996.

25. I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," *Workshop on Information Hiding, Newton Institute, University of Cambridge* , 1996.
26. M. Sonka, V. Hlavac, and R. Boyle, *Image Processing, Analysis, and Machine Vision-Second Edition*, PWS Publishing, San Francisco, 1999.
27. F. R. Connor, *Noise-Introductory Topics in Electronics and Telecommunication-Second Edition*, Edward Arnold Publishing, London, 1982.