Noisy Optical Detection of Chaos-Based Watermarks

Aidan Mooney and John G. Keating

Department of Computer Science, N.U.I. Maynooth, Maynooth,
Co. Kildare, Ireland.

ABSTRACT

In this paper we investigate the limits on optical detection of noisy watermarks that use a chaotic function, the logistic difference equation, in the watermark generation scheme. By varying the function seed, different chaotic sequences exhibiting lowpass and highpass characteristics, can be obtained for the same function, offering an added security advantage over watermarks generated using pseudorandom sequences. Watermark Detection is the process of determining whether an image is watermarked with a certain watermark. In this paper, we model and investigate an optical correlator suitable for watermark detection for certain classes of high-pass or low-pass watermarks. Once in the public domain a watermarked image may be subjected to noise and other attacks, deliberate and unintentional. Additionally, an optical correlator system will also be subject to shot noise. The effects of shot noise on optically transmitted watermarks are modeled in this paper and we examine how the watermark detection scheme performs in such situations. We quantify the degree of noise that may be present in the watermark detection scheme in order to obtain reliable detection or rejection of a watermark using an optical-correlator.

Keywords: Digital Watermarking, Optical Correlation, Chaotic Functions

1. INTRODUCTION

Digital Watermarking provides a means of inserting additional information into digital documents. This extra information may be used to provide a certain degree of protection of the document from malicious attack. This information is usually a piece of identifying information which may be used at a later date to prove ownership. The original document owner can prove ownership of attacker copies by proving that the copy contains their original watermark.

Numerous watermark generation techniques have been proposed to date, ranging from the use of personal logos to the use of pseudorandom sequences of numbers[1]. The use of chaotic functions for the generation of watermarks has also been proposed by Pitas *et al.*[2–4]. The functions used included ones which produced Markov Maps and Bernoulli Maps. These types of watermark generation schemes require two values, the initial value and the function seed, in order to recreate the same watermark at a later stage. An advantage of these watermarks is their robustness to lowpass attacks. Typically these watermarks are distributed over the full cover image using an additive or multiplicative technique.

To date some optical watermarking approaches have been proposed. Sun *et al.* presented an optical extraction technique which used some optical and visual means like a photocopier while no digitization was required.[5] Trustcopy have also introduced an optical watermarking technique but it uses paper and printers for verification of the watermark. Herrigel *et al.* present an optical/digital watermark identification system in which a reference number is extracted from the watermarked document using a lighting unit and optical part and compared with the original watermark.[6] None of these techniques use optical techniques in the detection of the watermark but just for the extraction of the embedded watermarks. These extracted watermarks are used in a visual or digital verification technique.

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

2. GENERATION OF THE WATERMARK

In this paper, we utilise watermarks that are generated using a chaotic function. A chaotic function is a function which is sensitive to 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, a, seeding the chaotic function, will always result in the same output (mapping) when certain constraints or initial conditions are placed on the mapping. As mentioned previously, such watermarks have robustness properties that may be analysed analytically. A chaotic map is derived from a chaotic sequence fully described by the map $\{y_j : y_j = f(j_{j-1}, a)\}$ and an initial condition y_0. The function used in this paper for the generation of sequences which are transformed into watermarks is the logistic difference equation:

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

where a is the function 'seed' and y_n is the current value of the mapping in time.[8] The logistic difference equation was originally proposed to describe the dynamics of a population of insects in discrete generations. The value y_{n+1} is dependant on its current density y_n. For low values of a, y_n eventually converges to a single number as n goes to infinity. When a equals 3.0, y_n no longer converges – it oscillates between two values. This characteristic change in behaviour is called a bifurcation, as shown in Fig. 1(a). Increasing the value of a even further causes y_n to oscillate between not two, but four values. As a increases, y_n goes through bifurcations of period 2^n and eventually becomes chaotic. When the value of $a \approx 3.57$, y_n neither converges or oscillates - its value becomes completely random. For values of a larger than 3.57, the behaviour is largely chaotic[8].

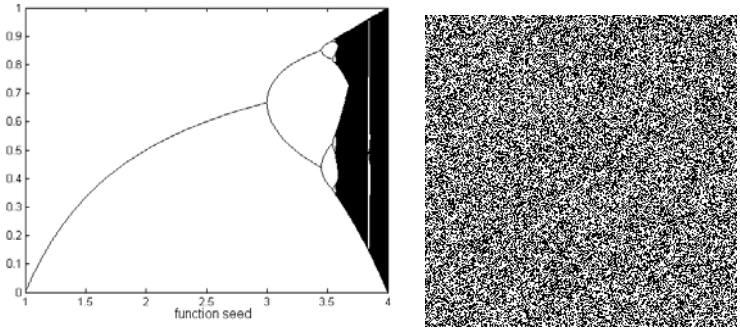

Figure 1. (a) Bifurcation Diagram for the Logistic Map (b) Watermark generated by iterating the Logistic Map with an initial value of 0.001 and a value of $a = 4$.

When the logistic equation is seeded with a value $3.57 \leq a \leq 4.0$ (the chaotic region), and the map iterated, chaotic behaviour is witnessed and it is this feature of the logistic equation that we utilise to generate watermarks. The trajectory's produced for maps of this equation will differ greatly even for small differences in the seed value for the equation, provided the seed is within the chaotic region.

The 1D sequence generated by iterating this map is a sequence of real numbers between 0 and 1. These values are converted to one of two values: if the number is less than 0.5 then it is converted to a 0, otherwise it is a 1. This sequence needs to be converted into a 2D sequence which one may use as a watermark. In this paper, we generate watermarks which are the same size as the image which will contain the watermark. A scanning technique, known as Peano Scanning, is used to determine the order which the pixels of the sequence get embedded into the watermark being generated. Peano Scanning is preferable to the more conventional Raster Scanning technique in that its scanning is not predictable and can produce many variations of scanning within the same image. The only drawback with using Peano Scanning is that it will only operate on images whose height and width are multiples of 2. The Peano scanning order always moves to a neighbouring pixel, but the pattern may appear in different orientations depending on the starting pixel with the scanning routine[9, 10]. An example of a watermark generated in this technique is shown in Fig. 1(b). In this case the function was seeded with a value $a = 4$ and an initial starting value of $y_0 = 0.001$.

As the watermarks produced using chaotic function are reproducible and chaotic only the initial starting value and seed are needed to generate a sequence of numbers. This ensures that the sequence may only be reproduced if someone has the initial starting value and also the function seed. Due to the fact that the logistic map is not invertible means there is added security over pseudorandom sequences. The primary advantage, however, is that is is possible to investigate the lowpass properties of the resulting watermark. To date, Markov maps and Skew Tent maps amongst others have been analysed, and presented in the literature. In the following section we provide results of a similar treatment for the logistic map.

2.1. Lowpass and Highpass Properties of Logistic Map Watermarks

Pitas *et al.* advocate the use of the power spectrum to determine if a particular generated watermark sequence is lowpass or highpass in characteristics.[2] The power spectrum of a function is defined as the modulus-squared of the discrete Fourier Transform of some finite sampled section of it.

$$P(u,v) = |FT[I(u,v)]|^2 \tag{2}$$

where $P(u,v)$ is the power of a pixel (u,v), FT stands for Fourier Transform and $I(x,y)$ is the image pixel whose power spectrum one is calculating. For the logistic equation this power spectrum is:

$$P(y_n) = |FT[y_n]|^2 \tag{3}$$

The sequences generated by Pitas *et al.* in this case use the Markov Map.[2] By calculating the Power Spectrum for different seed values (α) of this map one can see that the Power Spectrum decreases, in general, as the value of α increases. Pitas *et al.* say that as the value of the seed increases we get more lowpass watermarks. This can be seen when a watermark is generated with a value for the seed, α, of 0.1 and compared with a watermark generated with a seed value of 0.9, both incorporating Peano scanning order. It is observed that the pixels change more smoothly in the case where $\alpha = 0.9$ than in the case where $\alpha = 0.1$ indicating more lowpass characteristics within the watermark.

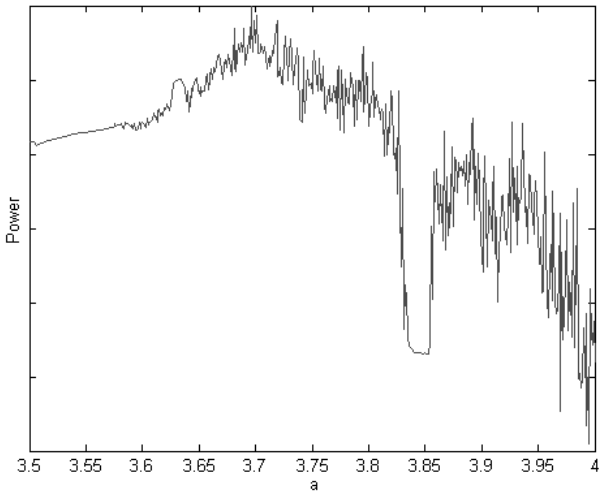

Figure 2. Power Spectrum Density of the chaotic region of the logistic map.

We have performed similar analysis for the logistic equation. The power spectrums were calculated for different values of the seed, a. It was observed that when $a = 3.7$ the power spectrum obtained is higher than in the case where $a = 3.99$. This indicates that the sequence produced when $a = 3.7$ is more highpass than the sequence produced when $a = 3.9$. Fig. 2 shows the power spectrum values obtained for the entire range of

values for a in the range $3.57 \leq a \leq 4$. It can be seen that, in general, as the value of a increase the power spectrum obtained decreases. This indicates that, in general, the sequences produced for higher values of a are more lowpass in character than those produced for lower values of a. There are a few exceptions to this case, the main occurring when $a \approx 3.83$. Around this value the logistic map is in a stable state, a period tripling state. The watermarks produced in this case are not suitable for watermarking, as there is no randomness in the pixels. By examining the watermark generated in this case, one can see a pattern repeating within the watermark. This is due to the fact that within this region chaotic behaviour is not witnessed, but instead a stable predicable state is observed. This does not occur for 'well-behaved' chaotic maps like the Markov map. We would recommend that when one wishes to generate a watermark using the logistic map that one does not seed the function with a value near to a bifurcation point.

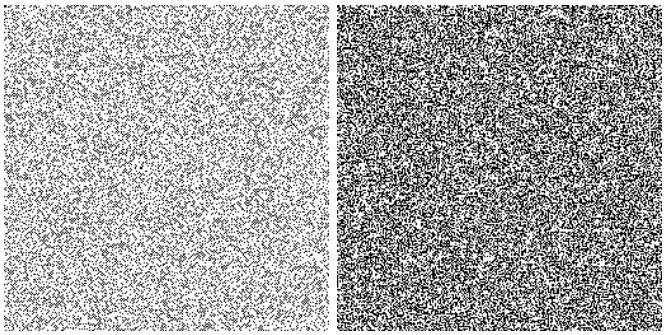

Figure 3. (a): Watermark produced in the case where $a = 3.7$ (b): Watermark produced in the case where $a = 3.99$.

Fig. 3 shows the watermarks produced for the two cases, where $a = 3.7$ and $a = 3.99$. They demonstrate that the watermark produced when $a = 3.7$ has much more density variation in it then the watermark produced in the case where the watermark is generated when $a = 3.99$. This is what one expects from looking at their corresponding power spectrums which suggest that in the case of $a = 3.99$ the watermark produced are much more lowpass than those produced when $a = 3.7$.

3. WATERMARK EMBEDDING

Watermark embedding is the process of 'placing' a defining piece of data within a cover document. This embedding can occur in 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 is unknown to 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 theft if the attacker is aware of watermarking technology and the possibility that a watermark may be present in the image.[11] For the analysis in this paper, the watermark generated with the logistic equation is embedded into the well-known "Lena" image of size 256×256, shown in Fig. 4(a).

The generated watermark is embedded in a multiplicative manner in the spatial domain, expressed as:

$$m_n = j_n + \gamma j_n x_n \tag{4}$$

where m_n is the n^{th} pixel of the watermarked image M, j_n is the n^{th} pixel of the cover image J, x_n is the n^{th} pixel of the watermark X and γ is known as the embedding factor and controls the watermark strength. The multiplicative watermark embedding rule relies on "Weber's Law", which indicates that the change in a stimulus that will be just noticeable is a constant ratio of the original stimulus,[12] and may be expressed as:

$$\frac{\Delta I}{I} = k \tag{5}$$

Figure 4. (a) Cover image - Lena (b) Cover image with noise - SNR = 21.15dB.

where I represents the initial intensity of a pixel, ΔI the change in the intensity of the pixel and k signifies that the proportion on the left hand side remains constant despite the value of I changing. In Eqn. 4, 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[13].

4. OPTICAL WATERMARK DETECTION

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[14]. The optical correlation technique discussed is based on the Matched Filtering technique[15, 16] which has been shown 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. A large output from the correlation operation indicates a high degree of similarity between the signal and the 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 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[17].

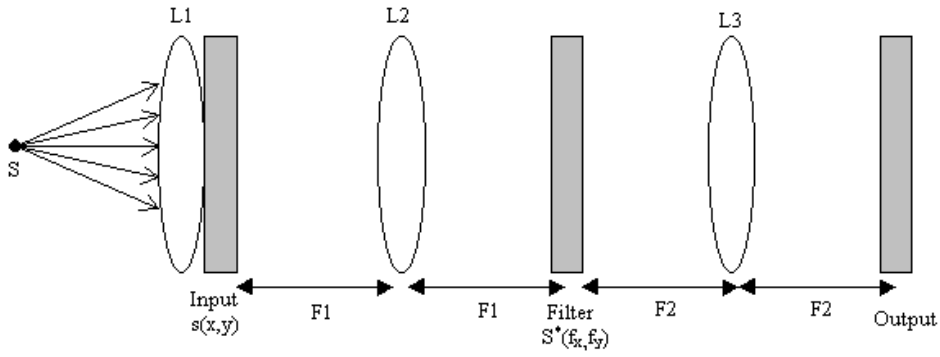

Figure 5. The optical configuration of the MSF.

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[18]. The 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 watermark. The proposed optical detection scheme presented was modelled and the simulation results are presented.

Simulations of the watermark embedding technique and the optical watermark detection techniques have been carried out using MATLAB. Watermark generation was performed as described in Section 2 with $3.57 \leq a \leq 4$ (i.e. the chaotic region).Watermark embedding follows the technique presented in Section 3. The resulting watermarked image is calculated and it is observed that there is little perceptual difference between the original image and the watermarked image, which is a fundamental requirement of a watermarking system.[19]

For the optical detection system, the possibly watermarked image together with the watermark whose presence(or absence) in the image one wishes to determine are used as inputs to the detector. The watermark is used as the filter for the matched filter detector. The optical 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. In the case of the optical correlator modelled here a sharp correlation peak in the output indicated that the image does indeed contain the watermark which was used as the filter. A similar detection technique is used in[20] for an image encryption technique.

Fig. 6(a) gives the output of the optical detection technique when a watermarked image is presented to the detector along with the embedded watermark. In this case a single sharp correlation peak is observed at the centre of 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 watermark used to generate the filter used in the detection process. Fig. 6(b) gives the output of the optical detection technique when a watermarked image is presented to the detector along with an embedded watermark which is different to the watermark used to generate the filter. In this case, there is no single sharp correlation peak visible at the centre of the correlation plane. This indicates that the image presented has not been watermarked with the watermark which is used to generate the filter used. A similar result is obtained when an image which has no watermark embedded in it is correlated with any watermark.

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 optical detection 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 it is immediately evident that the image is either watermarked with the watermark which is presented to the detection correlator or is not watermarked.

5. SYSTEM 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.[21] 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,[22] and may be modelled by a Poisson distribution. The Poisson distribution for mean λ of a random variable x is given by:

$$p(x) = \frac{\lambda^x e^{-\lambda}}{x!} \tag{6}$$

where x is an integer and has the property that its variance σ^2 equals its mean λ. As Poisson noise is discrete for each pixel value the mean changes for each pixel and thus the variance of each pixel is different.

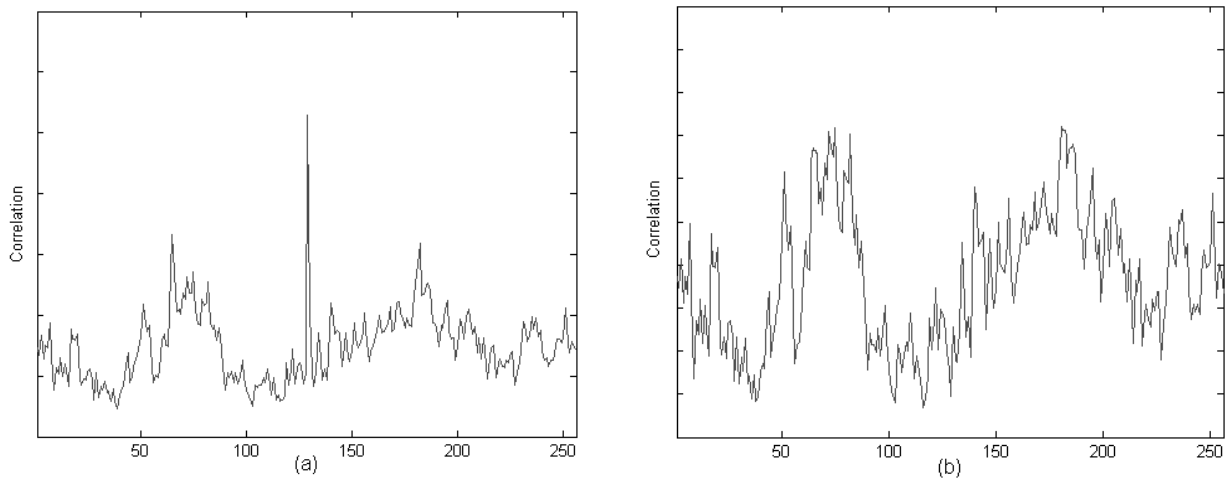

Figure 6. (a): Correlator output when a watermark generated with $a = 3.7$ is embedded in cover image (b): Correlator output when a watermark generated with $a \neq 3.7$ is embedded in cover image.

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. These experiments were performed on both relative lowpass and highpass watermarks produced by the logistic equation. Fig. 7 shows the case where a watermark is generated with the function seed $a = 3.7$. This watermark is then embedded in the cover image, Lena, and is then subjected to noise of varying intensities. The signal-to-noise ratio (SNR) is a widely used computation which represents a measure of image quality, and may be usually expressed as:

$$SNR = 20 \log_{10} \frac{\sum_{(n,m)} I(n,m)^2}{\sum_{(n,m)} (I(n,m) - I'(n,m))^2} \quad \text{dB} \tag{7}$$

where $I(n, m)$ is the original image and $I'(n, m)$ is the noisy image. The higher the value of the SNR the less noise is present in an image. The scaling factor used in this paper for the SNR is 20. In some cases this value is 10 but from the literature in watermarking it appears that 20 is the standard in this field.

In the case of no noise there is a sharp correlation peak (Fig. 6) in the output from the optical detector. It can be seen that in the case of noise corruption which results in a SNR of 39.21dB (Fig. 7(a)) that there is still a sharp correlation peak in the output. This suggests that watermarks generated with this seed are robust to noise manipulations of this level. Fig. 7(b) shows the output when the same watermarked image was subjected to noise which resulted in a SNR of 20.55dB. This noisy image is shown in Fig.4(b). There is no sharp centre peak in the output indicating the inability of the optical detection scheme to detect the presence of the watermark in the image after this corruption. It was found that for the case of watermarks generated with a function seed of $a = 3.57$ that the optical detection technique correctly detected the presence of the watermark up to a SNR level of 21.15dB.

From the power spectrum of the logistic equation (Fig. 2) it can be seen that the watermarks created when $a = 3.99$ are much more lowpass than those produced when $a = 3.7$. We expected, therefore, that these watermarks would be much more resistant to the introduction of noise in the system. Fig. 8(a) shows the case where the watermark created with $a = 3.99$ was embedded in the cover image, and then subjected to noise which resulted in a SNR level of 21.15dB. The resulting image was then correlated with the watermark and it can be seen that there is a sharp centre peak in the correlation output. This suggests that the optical detector is able to detect the existence of the watermark after this level of noise corruption. Fig. 8(b) shows the case where the same watermarked image is subjected to noise which results in a SNR value of 14.96dB, and then correlated with

the embedded watermark. It can be seen that there is a sharp centre peak present in the output suggesting that watermarks created with this seed are resistant to noise addition of this intensity level. This is true for noisy images producing a SNR as low as 13.14dB which have watermarks embedded in them seeded with $a = 3.99$.

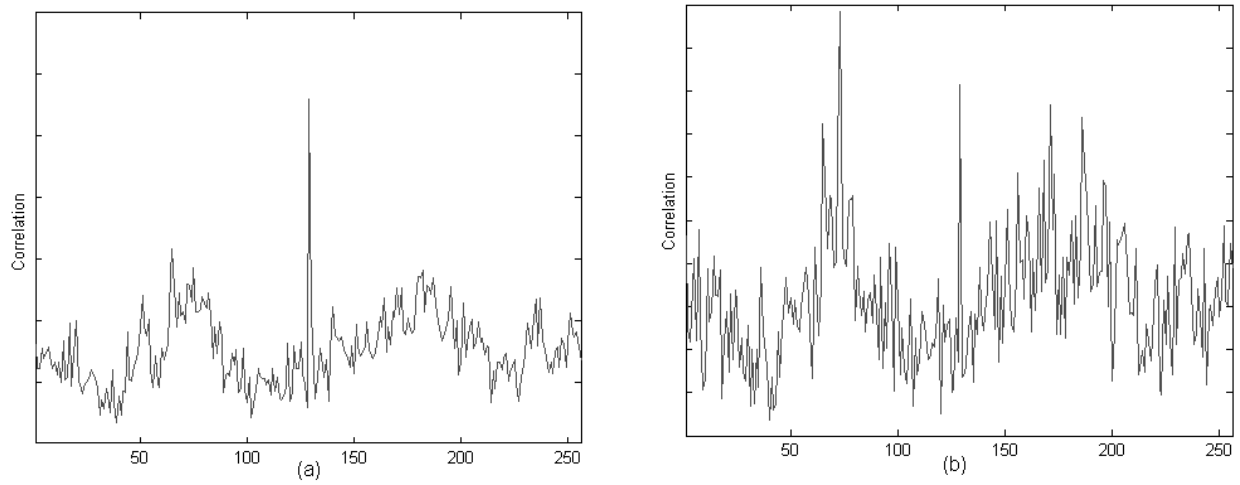

Figure 7. (a) Correlation response with SNR = 39.21dB, a = 3.7 (b) Correlation response with SNR = 21.15dB, a = 3.7.

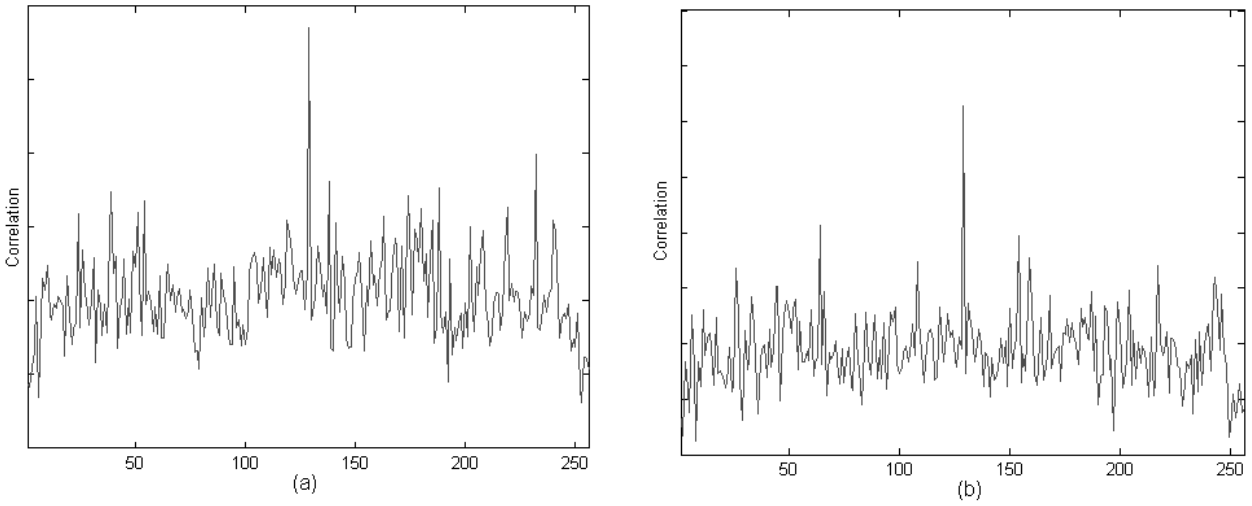

Figure 8. (a) Correlation response with SNR = 21.15dB, a = 3.99 (b) Correlation response with SNR = 14.96dB, a = 3.99 .

The maximum level of noise corruption which the detector can detect the embedded watermark was found for numerous seed values for the logistic map. The results of this analysis are shown in Fig. 9. In general, the expected result was found for watermarks generated in the chaotic range of the logistic function, i.e. lower pass watermarks perform much better in the presence of noise - they are more robust. Results from the stable period tripling state of the logistic function ($\approx 3.83 \leq a \leq \approx 3.85$) are not presented, as this area of the map is unsuitable for watermark generation, due to the non chaotic behaviour of the map in this area.

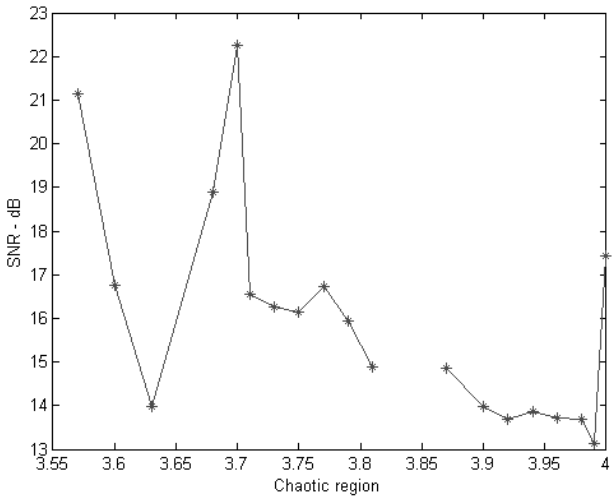

Figure 9. Value of SNR for which the optical detector can detect the embedded watermark (generated with a seed in the chaotic region).

6. CONCLUSION

We have investgated a watermark generation technique which uses chaotic functions, which are cryptographically secure because of the invertibility of such functions. We have examined the power spectrum of the chaotic region of the logistic function and thus were able to determine if the generated watermarks were lowpass or highpass ones. These generated watermarks were embedded in an image in a multiplicative manner using the Peano scanning algorithm. A watermark detection scheme based around an optical correlator using matched filtering has also been investigated. 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. It was also demonstrated that for lowpass watermarks produced by this chaotic function they are much more robust to noise addition in the watermark detection process, which one expects.

REFERENCES

1. I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio, and video," *Proceedings of International Conference on Image Processing (ICIP'96)* **III**, pp. 243–246, 1996.
2. A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I.Pitas, "Markov chaotic sequences for correlation based watermarking schemes," *Proceedings of Chaos, Solitons and Fractals* **17**, pp. 567–573, 2003.
3. A. Nikolaidis and I. Pitas, "Comparison of different chaotic maps with application to image watermarking," *Proceedings of IEEE International Symposium on Circuits and Systems, Geneva* , pp. 509–512, 2002.
4. S. Tsekeridou, V.Solachidis, N.Nikolaidis, A.Nikolaidis, A. Tefas, and I.Pitas, "Bernoulli shift generated watermarks: Theoretic investigation," *Proceedings of IEEE Int. Conf. on Acoustics, Speech and Signal Processing* , pp. 1989–1992, 2001.
5. Q. B. Sun, P. R. Feng, and R. Deng, "An optical watermarking solution for authenticating printed documents," *Proceedings of International. Conference on Information Technology: Coding and Computing* , pp. 65–70, 2001.
6. A. Herrigel, S. Voloshynovskiy, and Z. Hrytskiv, "An optical/digital identification/verification system based on digital watermarking technology," *Proceedings of SPIE International Workshop on Optoelectronic and Hybrid Optical/Digital Systems for Image/Signal Processing* , 1999.
7. R. L. Devaney, *A first course in Chaotic Dynamical Systems - Theory and Experiment*, Perseus Books, Cambridge, Massachusetts, 1992.
8. M. Marek and I. Schreiber, *Chaotic Behaviour of Deterministic Dissipative*, Cambridge University Press, Cambridge, 1991.
9. K. Yang and M. Mills, "Fractal based image coding scheme using peano scan," *Proceedings of ISCAS '88* **1470**, pp. 2301–2304, 1988.
10. R. Stevens, A. F. Lehar, and F. Preston, "Manipulation and presentation of multidimensional image data using the peano scan," *Proceedings of IEEE Trans. Patterm Pattern Anal. Machine Intell* , pp. 520–526, 1983.
11. N. F. Johnson, "An introduction to watermark recovery from images," *Proceedings of SANS Intrusion Detection and Response Conference* , 1999.
12. *Encyclopaedia Brittanica Online*, http://www.britannica.com/.
13. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, London, 2002.
14. J. Rosen, "Three-dimensional optical fourier transform and correlation," *Optics Letters* **22**, pp. 964–966, 1997.
15. 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* , pp. 209–214, 2003.
16. A. Sequeira and D. Kundur, "Communication and information theory in watermarking: A survey," *Proceedings of Multimedia Systems and Applications IV, A. G. Tescher, B. Vasudev, and V. M. Bove, eds., Proc. SPIE* **4518**, pp. 216 – 227, 2001.
17. 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.
18. J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill Publishing, Singapore, 1996.
19. 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* , pp. 175–190, 1996.
20. A. Sinha and K. Singh, "A technique for image encryption using digital signature," *Optics Communications, Elsevier Science* **218**, pp. 229 – 234, 2003.
21. M. Sonka, V. Hlavac, and R. Boyle, *Image Processing, Analysis, and Machine Vision-Second Edition*, PWS Publishing, San Francisco, 1999.
22. F. R. Connor, *Noise-Introductory Topics in Electronics and Telecommunication-Second Edition*, Edward Arnold Publishing, London, 1982.