A Comparative Study of Chaotic and White Noise Signals in Digital Watermarking

Aidan Mooney [a], John G. Keating [a], Ioannis Pitas [b]

[a] *Department of Computer Science, NUI Maynooth, Co. Kildare, Ireland*

[b] *Department of Informatics, Aristole University of Thessaloniki, P. O. Box 451, Thessaloniki 540 06, Greece*

Abstract

Digital Watermarking is an ever increasing and important discipline, especially in the modern electronically-driven world. Watermarking aims to embed a piece of information into digital documents which their owner can use to prove that the document is theirs, at a later stage. In this paper, performance analysis of watermarking schemes is performed on white noise sequences and chaotic sequences for the purpose of watermark generation. Pseudorandom sequences are compared with chaotic sequences generated from the chaotic skew tent map. In particular, analysis is performed on highpass signals generated from both these watermark generation schemes, along with analysis on lowpass watermarks and white noise watermarks. This analysis focuses on the watermarked images after they have been subjected to common image distortion attacks. It is shown that signals generated from highpass chaotic signals have superior performance than highpass noise signals, in the presence of such attacks. It is also shown that watermarks generated from lowpass chaotic signals have superior performance over the other signal types analysed.

1 Introduction

In recent years the design of robust techniques for the protection of multimedia documents has become an important necessity. Steganography and cryptography aimed at providing a certain degree of security while more recently digital watermarking has been proposed. For a review of the early watermarking schemes and the main requirements of a watermarking scheme, the reader may consult [1].

Email addresses: `amooney@cs.nuim.ie` (Aidan Mooney), `john.keating@nuim.ie` (John G. Keating), `pitas@zeus.csd.auth.gr` (Ioannis Pitas).

Digital Watermarking has been proposed in recent years as a robust technique for copyright protection and content verification of multimedia data. The majority of watermarking schemes proposed to date use watermarks generated from pseudorandom number sequences [2–4]. Pseudorandom sequences have an advantage in that they can be easily generated and recreated as a single seed will reproduce the same sequence of numbers each time the generating function is iterated. Chaotic functions have to a lesser extent been used to generate watermark sequences [5–7]. Similarly to the pseudorandom number sequence, a single seed (along with an initial value) will always reproduce the same sequence of numbers, when the chaotic function being used is iterated. The performance of these chaotic watermark sequences are compared with the more conventional pseudorandom watermark sequences.

2 Generation of Watermark Signals

The majority of watermark generation schemes proposed to date use a pseudorandom number generator to create a watermark sequence which is embedded in the cover work. These sequences can be accurately modelled as independent, identically distributed (IID) random variables obeying a uniform distribution [8]. In this case we will deal with zero-mean, pseudorandom sequences distributed in the interval $[-1, 1]$, that have white noise-like properties, that is, a signal with a flat frequency spectrum with equal power in all bands. Highpass signals created by colouring white noise are generated and used in this study by passing the generated white noise through an appropriate highpass linear filtering system.

A chaotic function is a function which is sensitive to initial conditions, is unpredictable, indecomposable and yet contains regularity [9]. The motivation for using a chaotic function to generate a watermark is that a single variable, α, seeding the chaotic function, will always result in the same output (mapping) when certain constraints or initial conditions are placed on the mapping. The use of chaotic functions for the generation of watermarks has been previously proposed, for example, the Bernoulli Map [10,11], Skew Tent Map [6,12,10] and also Logistic Map [13–15]. The skew tent map and Bernoulli maps are well behaved and understood, unlike the logistic map, where particular care must be taken in the selection of a seed for the function [16].

In this study the skew tent map was selected, as it is a well-behaved chaotic function which has been extensively studied [5,17], but any other well-behaved chaotic function may be used. The skew tent map is a piecewise linear Markov map which may be expressed as [17]:

$$\tau(x) = \begin{cases} (\frac{1}{\alpha})x \quad , & 0 \leq x \leq \alpha \quad , \alpha \in [0,1] \\ \tau(x) = (\frac{1}{\alpha-1})x + (\frac{1}{1-\alpha}) & , \alpha < x \leq 1 \end{cases} \qquad (1)$$

where

$$\tau : [0,1] \rightarrow [0,1]$$

A trajectory $t[k]$ of the dynamical system is obtained by iterating this map i.e.

$$t[k] = \tau(t[k-1]) = \tau^k(t[0])$$

The sequences starting point $t[0]$ (map's initial condition) is considered to be the watermark key. The generated sequences $t[k]$ may be transformed to 2-D sequences (watermark image) using a Peano scanning technique. Peano scanning is preferable to the more conventional Raster scanning technique in that it preserves local image neighbourhoods and can produce many variations of scanning within the same image [7,18,19]. Sample 2-D watermarks generated using the skew tent map are shown in Fig. 1, where the skew tent map was seeded with $t[0] = 0.001$ and with $\alpha = 0.1$ (Fig. 1a) and with $t[0] = 0.001$ and with $\alpha = 0.9$ (Fig. 1b). The difference in the density variations in the watermark pixels in both cases can be observed. Tefas *et al.* [17] showed that by varying the parameter α, sequences with desirable properties may be generated, in particular either highpass ($\alpha < 0.5$), or lowpass ($\alpha > 0.5$) ones. When $\alpha = 0.5$, the symmetric tent map is produced and sequences generated in this case possess a white spectrum.

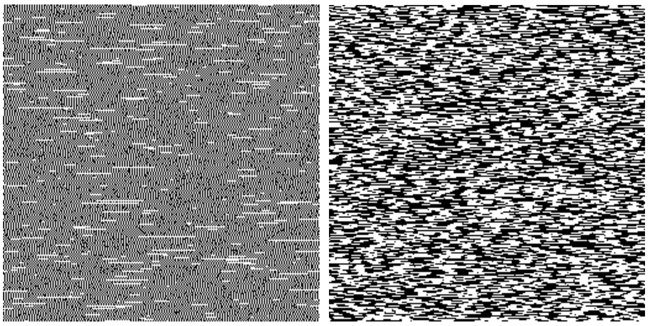

Fig. 1. Sample of 2-D skew tent map signals generated when a) $t[0] = 0.001$ and $\alpha = 0.1$, b) $t[0] = 0.001$ and $\alpha = 0.9$.

The chaotic signals used in this paper were generated by the recursive iteration of the skew tent map, seeded with $t[0] = 0.001$ and having $\alpha = 0.1$ for highpass chaotic signals, and $t[0] = 0.001$ and having $\alpha = 0.8$ for lowpass chaotic signals. The generated watermark signals were embedded in the cover image as described in Section 3.

In applications where no severe distortions are expected, eg. in captioning/indexing applications, highpass spectrum skew tent watermarks can be used since they guarantee superior performance [17]. Watermark signals generated by the iterating of a chaotic function have an advantage over signals generated by colouring white noise in that these signals are much easier to create and recreate. Rather than having to seed a white noise generator and then apply a filter to the resultant signal to generate coloured noise, a single seed can determine the properties of the generated sequence from the chaotic function. This study also serves to show that there are more advantages than this for using chaotic signals over the commonplace white noise signals, in watermark generation. In particular the advantages in using highpass chaotic signals over highpass coloured noise signals is presented.

3 Watermark Embedding and Watermark Detection

In this study watermark embedding is performed in the Wavelet Domain using a technique proposed by Barni *et al* [4]. This is a popular technique in watermarking and has proven successful under certain watermark attacks [20–22]. The image to be watermarked is first decomposed through the Discrete Wavelet Transform (DWT) in four levels: I_l^θ is the subband at resolution level $l = 0, 1, 2, 3$ with orientation $\theta \in 0, 1, 2, 3$ (see Fig. 2a). The watermark is embedded in the three detail bands at level 0, as these bands offer a satisfactory level of robustness and also provides a low level of visibility in the resulting watermarked image [4]. The watermarked image $\tilde{I}$ is the result of the embedding of the watermark into the subbands by modifying them according to:

$$\tilde{I}_0^\theta(i, j) = I_0^\theta(i, j) + \gamma w^\theta(i, j) x^\theta(i, j) \qquad (2)$$

where γ is the embedding factor which controls the watermark strength, I is the original image, x is the watermark to be embedded and $w^\theta(i, j)$ is a weighting factor. For the watermark to be embedded in the cover image the maximum, but still imperceptible, level of the weighing function $w^\theta(i, j)$ needs to be determined based on how the eye perceives changes in an image. Barni *et al.* [4] propose the following considerations:

- The eye is less sensitive to noise in the high resolution bands and in those bands having orientation of 45^o (i.e., $\theta = 1$ bands shown in Fig. 2).
- The eye is less sensitive to noise in those areas of the image where brightness is high or low.

- The eye is less sensitive to noise in highly textured areas of the image.

The effective application of the weighing function in the embedding scheme can be seen in Fig. 2b where the difference between the original image (the well-known ‘Lena’ image) and the corresponding watermarked image is shown amplified by a factor of 10. It can be observed that the watermark is predominantly hidden in the highly textured areas of the image, making it very difficult for an attacker to remove the watermark without severely distorting the image.

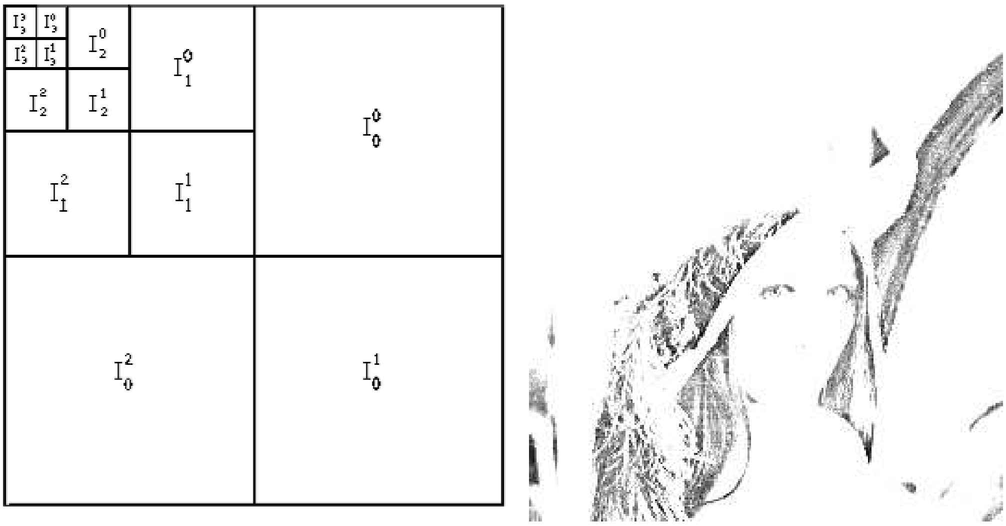

Fig. 2. a) Four level Wavelet Decomposition Scheme [4], b) Difference between original ‘Lena’ image and watermarked image amplified ten times.

Watermark Detection is also performed in the Wavelet Domain and is accomplished without referring to the original cover image [4]. The correlation between the DWT coefficients of the possibly watermarked image and the watermark sequence is computed using:

$$\rho = \frac{1}{3MN} \sum_{\theta=0}^{2} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \tilde{I}_0^{\theta}(i,j) x^{\theta}(i,j) \tag{3}$$

where $M \times N$ is the image size, $\tilde{I}$ is the possibly watermarked image and x is the watermark sequence. The computed correlation value ρ is then compared to a chosen threshold to determine the presence or absence of a watermark. For watermarking applications we can not be sure if a watermark is present in the image, therefore, the Neyman-Pearson criterion is normally used to determine the threshold: instead of minimizing the overall error probability, the probability of missing the watermark is minimized, to a given probability of false alarm, P_f. When presented with an image I' and a watermark signal

w, there are three possibilities:

Case A: image I' is not watermarked (w is not present);
Case B: image I' is watermarked but not with w (w is not detected);
Case C: image I' is watermarked with w (w is detected);

The value of the threshold is given by [4,15]:

$$T_\rho = 3.97\sqrt{2\sigma^2_{\rho_B}} \tag{4}$$

where $\sigma^2_{\rho_B}$ is the variance in relation to a missed detection, i.e. the variance of ρ in Case B.

4 Experimental Approach

The described watermark embedding and detection schemes have been applied to four cover images ("Lena", "Peppers", "Airplane" and "Madonna" shown in Fig. 3). These images were subjected to a four-level wavelet decomposition and subsequently watermarked. The watermarks used were those generated from white noise signals, highpass noise signals, lowpass chaotic signals and highpass chaotic signals.

The presence or absence of a watermark signal within a particular possibly watermarked (PWM) cover image is determined by supplying the watermark detector with the PWM and the watermark. The presence or absence of this watermark within the image is determined based on the correlation and threshold values presented in Section 3. If the correlation value is greater than the threshold, the detector determines that the watermark is present in the image, otherwise, it determines that the watermark is not present.

Fig. 4a shows detection results when the detector was supplied with two hundred highpass watermark signals generated by colouring white noise signals. The watermarked image present at the detector had been watermarked with a watermark seeded with a value of 132. It can be seen that the highest value of the correlation response (and the only one greater than the threshold) occurs when the watermark presented at the detector was seeded with a value of 132 and, hence, one can say that the watermark under test is present in the image.

Fig. 4b shows the case where the detector was supplied with two hundred watermark signals generated by iterating the skew tent map function, with values of α from 0 to 1. The presented image was watermarked with a watermark seeded with a value of 0.8. It can be seen that the watermark supplied with

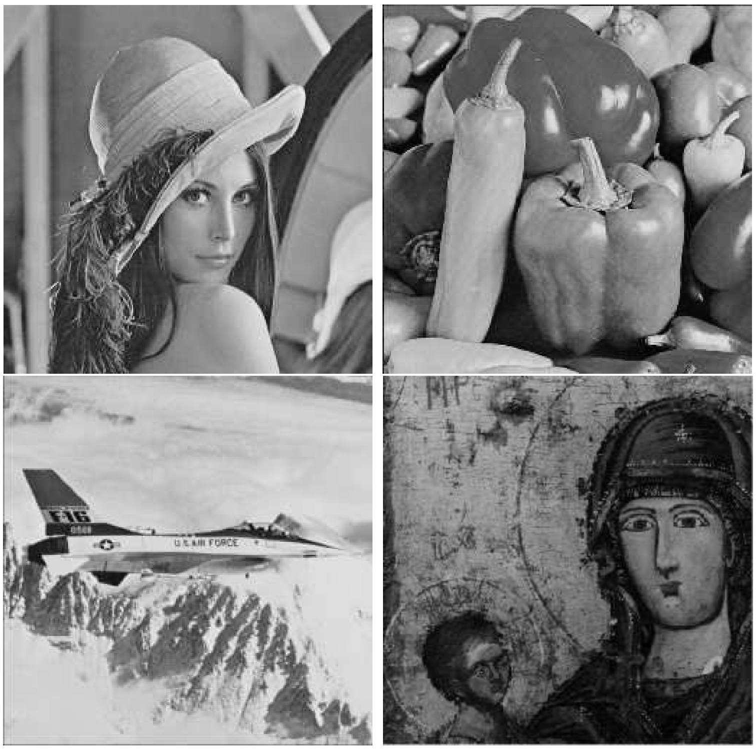

Fig. 3. Original images (from top left to bottom right) a) “Lena”, b) “Peppers”, c) “Airplane”, and d) “Madonna”.

the seed 0.8 was correctly detected in the presented image as it was the only value to have a correlation over the calculated threshold.

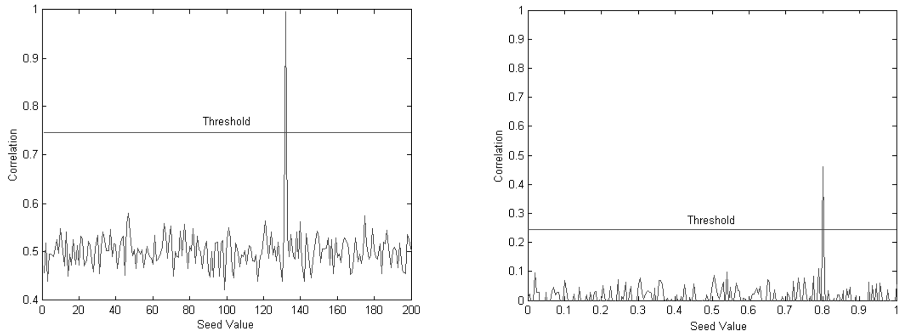

Fig. 4. Correlation Response from Watermark Detector supplied with a) two hundred watermarks generated from colouring white noise signals and, b) two hundred watermarks generated from skew tent maps.

The watermarks generated either from the chaotic function or from colouring white noise were then subjected to attacks. In the case of the chaotic sequences both a highpass signal (generated when $t[0] = 0.001$ and $\alpha = 0.1$) and a lowpass signal (generated when $t[0] = 0.001$ and $\alpha = 0.8$) were analysed. In the case of the white noise signals, a normal white noise signal along with a highpass signal generated by colouring the white noise signal were analysed. White noise signals are commonly used in watermark generation and are created as pseudorandom number sequences [4,23,24].

5 Results and Discussion

In order to compare the performance of the particular watermark types used the watermarked images were subjected to attacks. The attacks performed on these watermarked images were JPEG compression, noise addition (signal processing attack) and image dropping (geometric attack) [25]. The results of these attacks can be seen in Table 1. Each of the watermarked images were subjected to a range of JPEG compressions ranging from compression ratios of $2:1$ to $20:1$, using Paint Shop Pro. The ability or inability of the watermark detector to detect the embedded watermark was recorded and the maximum level of compression at which the detector correctly identified the watermark was also recorded.

Noise addition refers to the addition of a noise signal to a cover image. The signal-to-noise ratio (SNR) is a widely used computation which represents a measure of image quality in the presence of noise, and may be computed by:

$$\mathrm{SNR} = 20\log_{10}\frac{\sum_{(n,m)} I(n,m)^2}{\sum_{(n,m)}(I(n,m)-I'(n,m))^2} \quad [\mathrm{dB}] \tag{5}$$

where $I(n,m)$ is the original image and $I'(n,m)$ is the noisy image. The higher the value of the SNR the lower the level of noise in an image. The SNR is measured in decibels [dB]. Each of the watermarked images were subjected to a range of noise levels, with the noise value present within the image increasing until the watermark could no longer be detected. The maximum value of the noise present (SNR) in the image, at which the watermark could be detected, was computed and recorded. In this study, the noise type which was added to the images was Poisson noise [13].

Image cropping refers to the process of removing (blacking out) a certain number of pixels of an image. In this paper image cropping is used to remove pixels in an image from the bottom right corner of the image inwards. The aim of this attack is to remove or crop enough of the image so that the watermark is removed as well, in other words, that enough of the watermark is removed so that watermark detection fails. The results obtained for image cropping will vary, depending on the corner one wishes to crop from. For example, if one looks at the “Madonna” cover image, one can see that most of the detail in the picture is located in the bottom right of the image. Therefore, if one performed an image cropping from the top left corner, superior values for watermark detection would occur with higher levels of image cropping.

Table 1 contains the breakdown limits of the three attacks performed on the watermarked images, i.e. the severity of each attack that destroys the watermark. In the case of JPEG Compression it was found that highpass chaotic signals performed better than highpass noise signals. For example, in the case of "Lena", correct watermark detection occurred up to a compression ratio of 15 : 1 for highpass chaotic signals as opposed to 7 : 1 for the highpass noise signals. This result can also be observed for each of the cover images used, where the highpass chaotic signals performed better than highpass noise signals when subjected to JPEG compression. Lowpass signals were found to have increased robustness to JPEG compression. This is what is expected as lowpass watermarks have increased robustness with respect to image distortions that have lowpass characteristics (filtering, nonlinear filtering such as median filtering, lossy compression etc.) [26].

In the case of noise addition, it was observed that, in general, highpass chaotic signals performed better than highpass coloured noise signals. For example, in the case of "Peppers" correct detection of the watermark occurred with a noisy watermarked image with a SNR up to 20.01dB created by using highpass chaotic watermarks in comparison to 21.24dB for highpass coloured noise signals. In the case of the other two signals used, superior performance was achieved by the lowpass chaotic signals over the white noise signals. In general, this result was shown for each of the cover images used in this study.

In general, highpass chaotic signals were also found to be more robust to image cropping than highpass coloured noise signals. For example, in the case of "Lena", correct detection was found for the image cropped up to 49% of its width (W) and 49% of its height (H) when watermarked with a highpass chaotic signal. In the case of a highpass noise correct signal detection was only observed up to a level of 36% W and 36% H. Similar results were observed for each of the cover images used in this study.

In every watermarking system there is a tradeoff between the probability of false alarm and the probability of false rejection. As the threshold increases, the false alarm probability decreases and the false rejection probability increases. It is only by analyzing both of these measures at the same time that the system performance can be determined. The plot of the probability of false alarm (normally along the x-axis) versus the probability of false rejection is called the receiver operating characteristic (ROC) curve of the corresponding watermarking system [27]. This plot conveys all the necessary system performance information. Fig. 5 shows an example of a ROC curve generated in the case of a JPEG compression ratio of 10 : 1 for the "Lena" image. The superior performance of the lowpass chaotic watermarks can be observed for this case, corresponding with the results shown in Table 1. It may also be observed that highpass noise watermark signals, generated from the colouring of white noise, have the worst performance of the four signal types.

Fig. 6 shows a ROC curve in the case of image cropping for the "Peppers" image. In this case the image image and height was cropped by 20%. The highpass white

Table 1
Results of the attacks on the four cover images shown in Fig. 3, where the watermark signals used were Highpass Noise (HPN) signals, Highpass Chaotic signals (HPC), Lowpass Chaotic signals (LPC) and White Noise signals (WN). The underlined results denote the best overall performance for the HPN, HPC, LPC and WN signals. Results with ** denote the best performance from the HPN and HPC signals.

	JPEG Compression	Noise Addition (SNR)	Image Cropping
HPN			
-Lena	7 : 1	22.70dB	36% W, 36% H
-Peppers	9 : 1	21.24dB	31% W, 31% H
-Airplane	5 : 1	24.25dB	14% W, 14% H
-Madonna	5 : 1	23.98dB**	28% W, 28% H
HPC			
-Lena	$\underline{\text{15 : 1}}^{**}$	22.30dB**	$\underline{\text{49\% W, 49\% H}}^{**}$
-Peppers	13 : 1**	$\underline{\text{20.01dB}}^{**}$	$\underline{\text{42\% W, 42\% H}}^{**}$
-Airplane	7 : 1**	23.23dB**	16% W, 16% H**
-Madonna	6 : 1**	24.36dB	$\underline{\text{29\% W, 29\% H}}^{**}$
LPC			
-Lena	9 : 1	21.15dB	28% W, 28% H
-Peppers	$\underline{\text{14 : 1}}$	24.44dB	36% W, 36% H
-Airplane	$\underline{\text{8 : 1}}$	$\underline{\text{22.20dB}}$	$\underline{\text{24\% W, 24\% H}}$
-Madonna	$\underline{\text{9 : 1}}$	$\underline{\text{20.94dB}}$	23% W, 23% H
WN			
-Lena	11 : 1	$\underline{\text{20.72dB}}$	36% W, 36% H
-Peppers	9 : 1	28.83dB	34% W, 34% H
-Airplane	6 : 1	22.71dB	23% W, 23% H
-Madonna	8 : 1	21.82dB	29% W, 29% H

watermarks have the worst performance under this attack where the other three watermarks have similar performance at this level of the attack.Fig. 7 shows a ROC curve for the case where noise, presented in Section 5, resulting in an SNR of 21.9dB, has been added to the "Lena" image. The noise added resulted in an SNR of 21.9dB. It can be seen that the watermarks created from lowpass chaotic sequences have superior performance over the other three watermark types. In summary, we

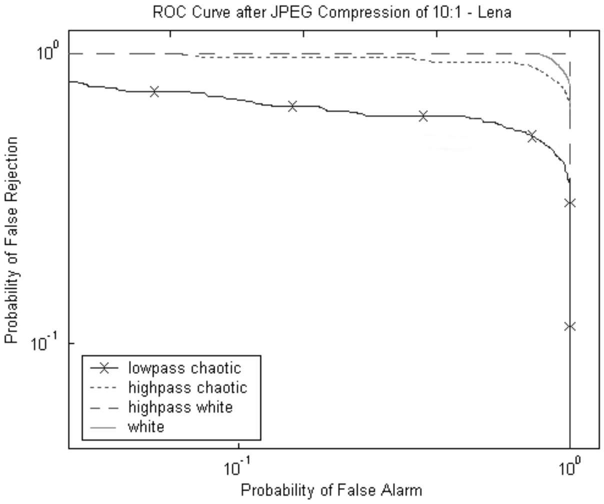

Fig. 5. ROC curve for watermarking schemes based on highpass chaotic, lowpass chaotic, white noise and highpass white noise signals, after JPEG compression ratio of 10 : 1, using "Lena" image.

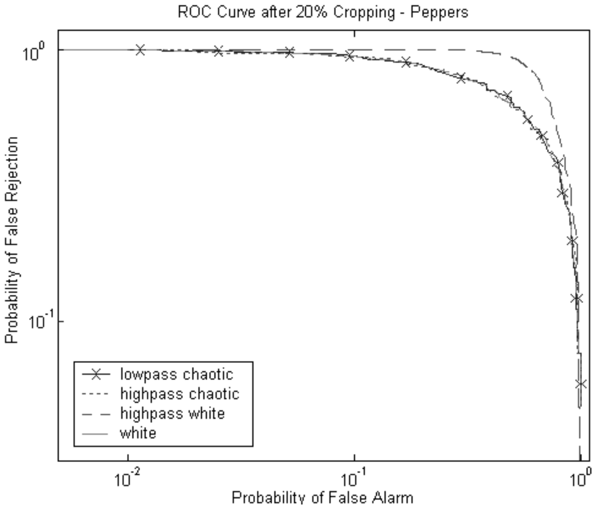

Fig. 6. ROC curve for watermarking schemes based on highpass chaotic, lowpass chaotic, white noise and highpass white noise signals, after image cropping of 20%, using "Peppers" image.

recommend the use of lowpass chaotic watermarks for use in watermark generation and we have shown them to provide improved robustness to common watermarking attacks over white noise watermarks. The latter have the worst performance of the studied watermark types in the presence of the attacks studied.

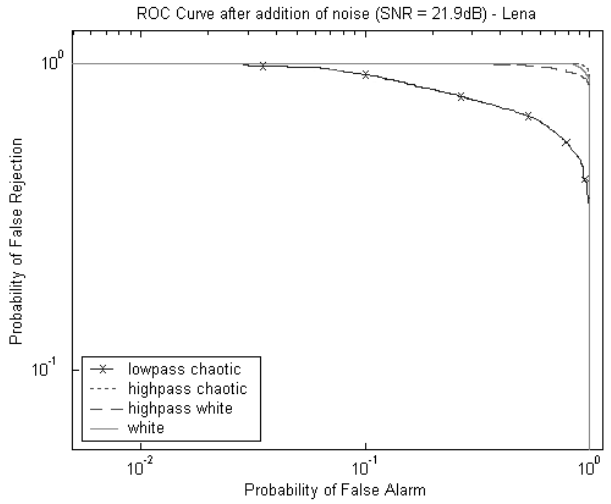

Fig. 7. ROC curve for watermarking schemes based on highpass chaotic, lowpass chaotic, white noise and highpass white noise signals, after Noise addition resulting in an SNR = 21.9dB, using “Lena” image.

6 Conclusion

In this paper watermarks signals generated as white noise, coloured highpass noise, lowpass chaotic signals and highpass chaotic signals were generated and embedded into four cover images. The presence of a watermark was determined in these possibly watermarked images after they were subjected to different common watermarking attacks. The robustness of each signal to these attacks was determined and it was observed that the highpass chaotic watermarks perform steadily better than the highpass noise signals in the presence of the attacks discussed. It was also observed that lowpass chaotic signals have the best overall performance for the attacks discussed, with these signals performing best in six out of twelve experiments. Highpass chaotic signals perform next best with best results in five out of the twelve experiments. It can be observed that chaotic signals perform better than the corresponding noise signals in the presence of the attacks presented. Chaotic signals offer an alternative to the more frequently used white noise signals, as they can be easily generated and their properties easily controlled. These chaotic sequences have been shown to have superior robustness than the widely used pseudorandom sequences in watermarking applications.

References

[1] "Identification and protection of multimedia information," *Special issue on Proceedings of the IEEE* **87**, 1999.

[2] J. J. K. O. Ruanaidh and S. Pereira, "A secure robust digital image watermark," *Electronic Imaging: Processing, Printing and Publishing in Colour* , 1998.

[3] R. Venkatesan and M. Jakubowski, "Image watermarking with better resilience," *Proceeds. ICIP 2000* , 2000.

[4] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Trans. on Image Processing* **10**, pp. 783–791, 2001.

[5] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I.Pitas, "Markov chaotic seqences for correlation based watermarking schemes," *Choas, Solitons and Fractals* **17**, pp. 567–573, 2003.

[6] 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.

[7] A. Mooney and J. G. Keating, "Optical and digital technique for watermark detection," *Proceedings of SPIE, Optical Information Systems* **5202**, pp. 97–105, 2003.

[8] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I.Pitas, "Performance analysis of correlation-based watermarking schemes employing markov chaotic sequences," *IEEE Trans. on Signal Processing* **51**, pp. 1979–1994, 2003.

[9] R. L. Devaney, *A first course in Chaotic Dynamical Systems - Theory and Experiment*, Perseus Books, Cambridge, Massachusetts, 1992.

[10] 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.

[11] S. Tsekeridou, V.Solachidis, N.Nikolaidis, A.Nikolaidis, A. Tefas, and I.Pitas, "Theoretic investigation of the use of watermark signals derived from bernoulli chaotic sequences," *SCIA200* , 2001.

[12] 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.

[13] A. Mooney and J. G. Keating, "Noisy optical detection of chaos-based watermarks," *Proceedings SPIE, Photonics North* **5579**, pp. 341–350, 2004.

[14] A. Mooney and J. G. Keating, "The impact of the theoretical properties of the logistic function on the generation of optically detectable watermarks," *Proceedings SPIE, Technology for Optical Countermeasures, Optics/Photonics in Defence and Security, London* , pp. 120–129, 2004.

[15] Z. Dawei, C. Guanrong, and L. Wenbo, "A chaos-based robust wavelet-domain watermarking algorithm," *Choas, Solitons and Fractals* **22**, pp. 45–54, 2004.

[16] A. Mooney and J. G. Keating, "Generation and detection of watermarks derived from chaotic functions," *Proceedings SPIE, Imaging and Vision, Opto Ireland* , 2005.

[17] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I.Pitas, "Performance analysis of watermarking schemes based on skew tent chaotic sequences," *NSIP'01* , 2001.

[18] K. Yang and M. Mills, "Fractal based image coding scheme using peano scan," *Proceedings of ISCAS '88* **1470**, pp. 2301–2304, 1988.

[19] 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.

[20] J. Du, C.-S. Woo, and B. Pham, "Recovery of watermark using differential affine motion estimation," *Proceedings of Third AISW2005* **44**, pp. 81–88, 2005.

[21] H. Si and C.-T. Li, *Encyclopedia of Virtual Communities and Technologies - Copyright Protection in Virtual Communities through Digital Watermarking*, Idea Group Publishing, 2005.

[22] C.-H. Lee and H.-K. Lee, "Geometric attack resistant watermarking in wavelet trasform domain," *Optics Express* **13**, pp. 1307–1321, 2005.

[23] H. Brunk, "Host-aware spread spectrum watermark embedding techniques," *Proc. SPIE Security and Watermarking of Multimedia Contents* **5020**, pp. 699–707, 2003.

[24] A. Briassouli and M. G. Strintzis, "Locally optimum nonlinearities for dct watermark detection," *IEEE Tran. on Image Processing* **12**, pp. 1604–1617, 2004.

[25] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," *SPIE - Security and Watermarking of Multimedia Contents* , pp. 147–158, 1999.

[26] J. Fridrich, "Combining low-frequency and spread spectrum watermarking," *Proceedings SPIE International Symposium on Optical Science, Engineering and Instrumentation* , pp. 2–12, 1998.

[27] I. J. Cox, M. L. Miller, and J. Bloom, *Digital Watermarking*, Morgan Kaufmann, London, 2002.