Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

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

Performance analysis of chaotic and white watermarks in the presence of common watermark attacks

Aidan Mooney [a,*], John G. Keating [a], Daniel M. Heffernan [b,c]

[a] Department of Computer Science, NUI Maynooth, Co. Kildare, Ireland
[b] Department of Mathematical Physics, NUI Maynooth, Co. Kildare, Ireland
[c] School of Theoretical Physics, Dublin Institute for Advanced Studies, Dublin 4, Ireland

ARTICLE INFO

Article history:
Accepted 21 January 2009

ABSTRACT

Digital watermarking is a technique that aims to embed a piece of information permanently into some digital media, which may be used at a later stage to prove owner authentication and attempt to provide protection to documents. The most common watermark types used to date are pseudorandom number sequences which possess a white spectrum. Chaotic watermark sequences have been receiving increasing interest recently and have been shown to be an alternative to the pseudorandom watermark types. In this paper the performance of pseudorandom watermarks and chaotic watermarks in the presence of common watermark attacks is performed. The chaotic watermarks are generated from the iteration of the skew tent map, the Bernoulli map and the logistic map. The analysis focuses on the watermarked images after they have been subjected to common image distortion attacks. The capacities of each of these images are also calculated. It is shown that signals generated from lowpass chaotic signals have superior performance over the other signal types analysed for the attacks studied.

1. Introduction

In recent years the design of robust techniques for the protection of multimedia documents has become an important necessity. Steganography and cryptography aim at providing a certain degree of security in particular confidentiality. Steganography is the study of techniques for hiding the existence of a secondary message (payload message) in the presence of a primary message (carrier message): the very existence of the message is a secret [1]. Cryptography is a mechanism that provides confidentiality and integrity to communication protocols in the presence of adversaries. Legitimate users are explicitly or implicitly provided with a key to decrypt the contents in order to view it. Unfortunately, not all customers with legitimate credentials are trustworthy and can therefore alter or copy the decrypted content in a way the content owner does not permit. Furthermore, cryptography provides no protection once the content is decrypted [2].

Watermarking has been proposed as a means to complement cryptography by embedding a message within the content. Unlike cryptographic techniques the watermark remains in the content after the user has received the file. Digital watermarking is the enabling technology to prove ownership on copyrighted material, detect originators of illegally made copies and monitor the usage of the copyrighted content [5]. For a review of the early watermarking schemes and the main requirements of a watermarking scheme, the reader may consult Cox et al. [6].

The majority of watermarking schemes proposed to date use watermarks generated from pseudorandom number sequences [7–10]. Pseudorandom sequences, which possess a white spectrum, have an advantage in that they can be easily

[*] Corresponding author.
E-mail addresses: amooney@cs.nuim.ie (A. Mooney), john.keating@nuim.ie (J.G. Keating), dmh@thphys.nuim.ie (D.M. Heffernan).

0960-0779/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2009.01.025

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 [11–14]. 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 used is iterated.

Robustness against geometric distortion is one of the most important issues to be solved to increase the robustness of digital image watermarking systems. Such attacks are very simple to implement, so they can defeat most existing watermarking algorithms without causing serious perceptual distortion [5]. In all watermarking systems there is a tradeoff between the robustness, perceptibility and the capacity of the system. If one property is determined, the other two parameters are inverse-proportional.

The capacity of a system refers to the number of bits of a watermark that may be encoded within a work. For an image, the capacity refers to the number of bits encoded within the image. A watermark that embeds *N* bits is referred to as an *N-bit watermark*. Such a system can be used to embed any one of 2^n different messages [3]. Image watermarking capacity is a complex problem and is influenced by the image content. Every image will have a different watermark capacity, with more complex images having the ability to hold more information compared to a flat image, for example, a pure white colour image [4].

In this paper the capacity of the test images used is calculated along with the number of edges present within the image. The resilience of watermarks generated from pseudorandom functions along with watermarks generated from chaotic functions is also analysed in the presence of some common watermark attacks. The functions used to generate the chaotic functions studied in this paper are the skew tent map, the Bernoulli map and the logistic map. These functions are presented in Section 2 along with the main properties of the sequences which are generated from their iteration.

2. Chaotic functions

Chaos can be loosely defined as stating whether or not it is possible to make accurate long-term predictions about the behaviour of a physical system. Chaos is the prevalence of sensitive dependence on initial conditions whatever the initial condition is [15].

A dynamical system *F* is chaotic if [16]:

1. Periodic points for *F* are dense.
2. *F* is transitive.
3. *F* depends sensitively on initial conditions.

A chaotic map is derived from a chaotic sequence fully described by the map $\{y_n : y_n = f(y_{n-1}, a)\}$, where a is a function seed and y_0 is the initial condition. A chaotic discrete-time signal y_n can be generated from a chaotic system with a single state variable by applying the recursion:

$$y_n = f(y_{n-1}) = f^n(y_0), \tag{1}$$

where *f*( ) is a nonlinear transformation that maps scalars to scalars and y_0 is the system's initial condition. A chaotic sequence may be easily reproduced given the same initial conditions and value y_0. A slight change in the initial conditions of a chaotic function will lead to significant changes in the resultant outcome. This effect is known as the "Butterfly Effect" and also as "the sensitive dependence on initial conditions" [17].

To determine if a function is chaotic one may calculate its Lyapunov exponents. Consider two points in phase-space: y_0 and $y_0 + \Delta y_0$ (see Fig. 1), each of which may generate an orbit in that space using a chaotic equation. The separation between these two points can be considered as a function of time in that after a certain period of time, the state y_0 will be in the state $y_0 + \Delta y(y_0, t)$, since the separation is dependent on the initial state as well as the time. If a system is chaotic it undergoes a series of exponential separations and foldings. For chaotic points, the function $\Delta y(y_0, t)$ will behave erratically [18].

In the following sections the chaotic functions which are analysed in this paper are presented. These functions are the skew tent map, the Bernoulli map and the logistic map all of which are well-studied chaotic functions.

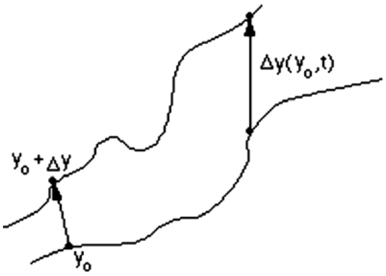

Fig. 1. Rate of separation of two close points which can be used to calculate the Lyapunov exponent.

2.1. Skew tent map

The skew tent map is a piecewise linear Markov map, where a Markov process has the properties, given that its current state is known, the probability of any future event of the process is not altered by additional knowledge concerning its past behaviour. The skew tent map can be expressed as:

$$s : [0,1] \to [0,1]. \tag{2}$$

$$s(x) = \begin{cases} \frac{1}{a} x, & 0\ 6\ x\ 6\ a, \quad a \in [0,1], \\ \frac{1}{a-1} x + \frac{1}{1-a}, & a < x\ 6\ 1. \end{cases}$$

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

$$t[k] = s(t[k-1]) = s^k(t[0]),$$

where $t[0]$ is the initial state of the mapping. Tefas et al. [19] showed that by varying the parameter a, sequences with desirable properties may be generated, in particular either highpass ($a < 0.5$), or lowpass ($a > 0.5$) sequences could be generated. When $a = 0.5$, the symmetric tent map is produced and sequences generated in this case possess a white spectrum.

2.2. Bernoulli shift map

The Bernoulli shift map is a simple chaotic map which contains many chaotic characteristics. The periodic orbits of the mapping are dense, the dynamical system is transitive and the system is sensitive to initial conditions [16].

n-way Bernoulli shifts $B_n(p)$ are chaotic maps defined in the interval $[0,1]$ using the following expression:

$$x_{n+1} = Bx_n (\text{mod } 1). \tag{3}$$

When the value of $B = 2$ (i.e. $x_{n+1} = 2x_n(\text{mod } 1)$) the mapping is referred to as a binary shift Bernoulli Map and is given by:

$$B(x) = \begin{cases} 2x & \text{if} \quad 0\ 6\ x < \frac{1}{2}, \\ 2x - 1 & \text{if} \quad \frac{1}{2}\ 6\ x < 1. \end{cases} \tag{4}$$

If the value of x_0 is rational then the orbit is periodic, and if the value is irrational there is no periodicity, however, chaotic orbits are obtained. Since there are irrational numbers close to every rational number the map exhibits sensitive dependence on initial conditions. For small values of n, Bernoulli map sequences are characterised by lowpass spectrums, while as n increases they tend towards white spectrums [20].

2.3. Logistic map

The logistic mapping is a chaotic map defined by the following expression:

$$y_{n+1} = ay_n(1 - y_n), \tag{5}$$

where a is the 'function seed' and y_n is the current value of the mapping in time with an initial value y_0 [21]. The properties of the logistic map have been thoroughly studied and are well classified. The value y_{n+1} is dependant on its current value y_n. For

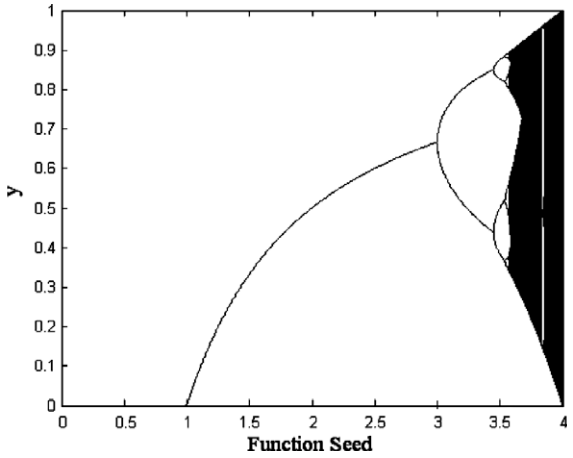

Fig. 2. The bifurcation diagram of the logistic difference equation.

low values of a, y_n eventually converges to a single number as $n \to \infty$ after initial transience has died out. For $1 < a < 3$, there are only two periodic orbits of period one and no chaos. When $a = 3$ the orbits become unstable and this leads to the creation of two new fixed points which lie on a period two orbit [18]. This characteristic change in behaviour is called a bifurcation, and can be seen in the bifurcation diagram shown in Fig. 2. Increasing the value of a (>3.0) causes y_n to go through further bifurcations of period 2^n, and, when the value of $a \approx 3.55699$ (the accumulation point, a_{a}), y_n becomes random. For values of $a > 3.5699$, the behaviour is largely chaotic [21].

In the chaotic regime, the chaotic intervals move together by inverse bifurcation as a is increased from a_∞ to 4 until the iterates become distributed over the whole interval [0,1] at $a = 4$. There are, however, values in the chaotic regime where periodic behaviour is exhibited by the map. When using the logistic map to produce chaotic sequences care must be taken in the selection of the function seed. A thorough analysis of the logistic map for the purpose of watermark generation has been presented previously by the authors [13].

3. Watermark generation

The selection of the watermark to use in a particular scenario can be the most important decision a user has to make. Digital watermarks have been generated in numerous ways, including the use of personal logos [22], the use of text (as used in Adobe's PhotoShop and Corel's Paint Shop Pro), the use of pseudorandom sequences of numbers [9,23] and the use of chaotic functions [24–26].

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 [7–9]. A single seed will reproduce the same sequence of numbers each time. These watermark sequences are normally embedded in an imperceptible manner within the cover image. These sequences can be accurately modelled as independent, identically distributed (I.I.D.) random variables obeying a uniform distribution [27]. These kinds of sequences possess white noise-like properties or attributes, that is, a signal with a flat frequency spectrum with equal power in any band.

Chaotic watermarks refer to those which are generated by the recursive iteration of some chaotic function. Watermark generation based on the use of chaotic functions has been suggested, with the skew tent map [11,19,24], Bernoulli shift maps [28–30], Henon map [31] and n-way tailed sequences [28] being used. The logistic map has also been utilised by Xiang et al. [32], Mooney et al. [25,33–35], Zhang and Tian [31] and also by Dawei et al. [26].

A single seed and an initial value will always generate the same sequence of numbers. This combination of seed and initial value make it very difficult for an attacker to re-generate the watermark. Chaotic watermarks attain similar properties with white ones with the additional feature of controllable spectral/correlation properties, a fact that renders them ideal for a variety of applications [20], including watermarking.

With both pseudorandom watermarks and chaotic watermarks a sequence of real numbers is generated by iterating the function in question. This sequence of numbers is usually converted to one of two numbers to give a binary valued watermark. For example, if the user generated a sequence of numbers, x_n, whose values ranged between 0 and 1 the following rule may be used to generate a binary-valued watermark values w_n:

$$w_n = \begin{cases} -1 & x_n \leqslant 0.5, \\ 1 & x_n > 0.5. \end{cases} \tag{6}$$

In this paper a number of different watermark types will be generated:

- Pseudorandom watermarks – white noise signals (WN).
- Highpass pseudorandom watermarks – from the colouring of white noise signals (HPN).
- Highpass chaotic watermark – skew tent map with a value for a = 0.1 (HPC).
- Lowpass chaotic watermark – skew tent map with a value for a = 0.8 (LPC).
- Bernoulli map watermarks – $x = 3$ (BN3).
- Bernoulli map watermarks – $x = 9$ (BN9).
- Logistic map watermarks – $a = 3.7$ (Log3.7).
- Logistic map watermarks – $a = 3.85$ (Log3.8).

The resilience of these watermark types is studied in the presence of common watermarking attacks and the results presented. These attacks are discussed in Section 5.

4. Watermark embedding and watermark detection

4.1. Watermark embedding

In this study watermark embedding is performed within the Discrete Wavelet Domain using a technique proposed by Barni et al. [9]. This is a popular technique in watermarking and has proven successful under certain watermark attacks [5,10,36]. The image to be watermarked is first decomposed through the Discrete Wavelet Transform (DWT) in four levels:

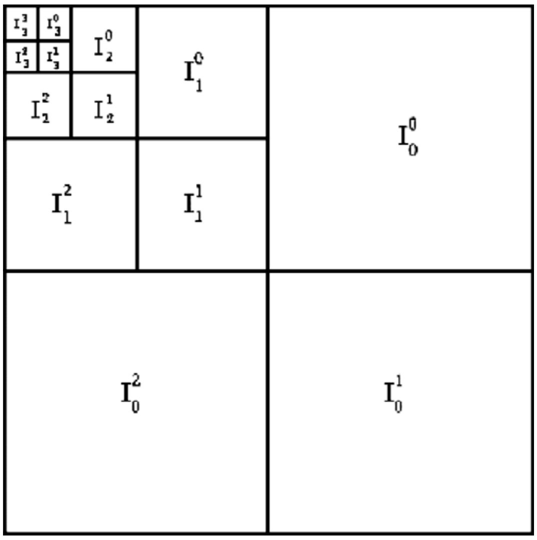

Fig. 3. Four-level wavelet decomposition scheme.

I_l^{h} is the subband at resolution level $l = 0, 1, 2, 3$ with orientation $\mathrm{h} \in 0, 1, 2, 3$ (see Fig. 3). 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 [9]. The watermarked image Ψ is the result of the embedding of the watermark into the subbands by modifying them according to:

$$\Psi_0^{\mathrm{h}}(i,j) = I_0^{\mathrm{h}}(i,j) + \mathrm{c}w^{\mathrm{h}}(i,j)x^{\mathrm{h}}(i,j), \tag{7}$$

where c is the embedding factor which controls the watermark strength, I is the original image, x is the watermark to be embedded and $w^{\mathrm{h}}(i,j)$ is a weighting factor. For the watermark to be embedded in the cover image the maximum, but still imperceptible, level of the weighing function $w^{\mathrm{h}}(i,j)$ needs to be determined based on how the eye perceives changes in an image. Barni et al. [9] propose the following considerations:

- The eye is less sensitive to noise in the high resolution bands and in those bands having orientation of 45° (i.e. $\mathrm{h} = 1$ bands shown in Fig. 3).
- 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.

With this scheme 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.

4.2. Image capacity

According to Cox et al. [37] the watermark should be embedded in the DC and the low frequency AC components in the DCT domain due to their large perceptual capacity. Similar strategies can be applied to the DWT by embedding in the I_3^3 (Low-Low) band after a four-level decomposition for example. Low frequency components have larger perceptual capacity compared to high frequency components because they have large magnitudes and can be used to embed stronger watermarks without introducing visible artifacts [38]. Embedding the watermark in the lower level subbands increases the images visual fidelity or makes it perceptually invisible, however, it reduces its robustness. Embedding watermarks in the higher level subbands of a DWT increases the robustness of the watermark. However, the images visual fidelity may be lost which can be measured by the peak signal to noise ratio (PSNR).

Shannon's well-known channel capacity bound,

$$C = \frac{1}{2}\log 2\left(1 + \frac{P}{N}\right) \quad (\text{bits/sample}) \tag{8}$$

is a theoretic capacity bound of an analog-value time-discrete communication channel in a static transmission environment, i.e. where the (codeword) signal power constraint, P, and the noise power constraint, N, are constants [39]. The capacities of the test images shown in Fig. 4 were calculated (using Eq. (8)) to determine the maximum number of bits that could be embedded without affecting the perceptibility of the cover image. The capacity of each image for each of the watermark type is given in Table 1.

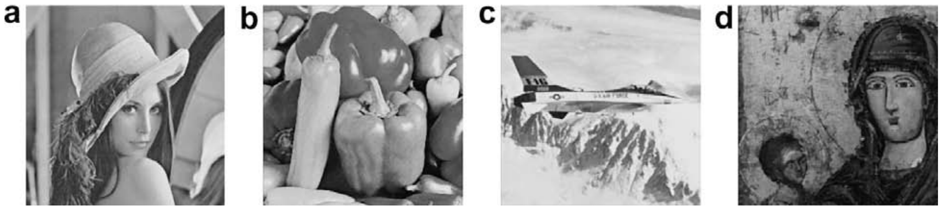

Fig. 4. Original images (from top left to bottom right). (a) “Lena”, (b) “Peppers”, (c) “Airplane”, and (d) “Madonna”.

Table 1
Image capacities (in kilobytes) for the four cover images shown in Fig. 4 for the different watermark types.

Watermark	Lena	Peppers	Airplane	Madonna
LM37	5.48	5.81	6.08	5.39
LM385	5.29	5.85	5.88	5.18
HPC	5.28	5.84	5.87	5.18
LPC	5.28	5.84	5.87	5.18
HPN	5.25	5.78	5.72	5.18
WN	5.28	5.84	5.87	5.18
BN3	5.27	5.84	5.87	5.18
BN9	5.28	5.84	5.87	5.18

The number of edges present within the test images was also calculated using the Canny edge detection technique [40]. Table 2 shows the number of edges present within the four test images using this method. It can be seen from Table 1 that, in general, the images with the most information content in terms of edge information, are able to accommodate more watermark bits without affecting the perceptibility of the image, i.e. they have better capacity. For example, in the case of watermarks generated from the logistic map when $a = 3.7$ it can be seen that the image “Airplane” have the highest capacity levels of the four images, with the image “Madonna” having the lowest capacity.

4.3. Watermark detection

Watermark detection is also performed in the Wavelet Domain and is accomplished without referring to the original cover image [9]. The correlation between the DWT coefficients of the possibly watermarked image and the watermark sequence is computed using:

$$\mathrm{q} = \frac{1}{3MN}\sum_{\mathrm{h}=0}^{2}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} I'^{\mathrm{h}}_{0}(i,j)x^{\mathrm{h}}(i,j), \tag{9}$$

where $M \times N$ is the image size, I' is the possibly watermarked image and x is the watermark sequence. The computed correlation value q is then compared to a chosen threshold to determine the presence or absence of a watermark. For watermarking applications we cannot 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);

Table 2
Number of edges present within the test images.

Image	Edges within Image
Madonna	1526
Lena	2396
Peppers	2560
Airplane	2870

The value of the threshold is given by [9,26]:

$$T_\rho = 3.97\sqrt{2\sigma^2_{\rho_B}}, \quad (10)$$

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

If the value of $\rho > T_\rho$ then we can say that the image is watermarked with the watermark we are checking for. Otherwise we can say that the image is not watermarked with the presented image.

5. Attacks

The described watermark embedding and detection schemes have been applied to four cover images ("Lena", "Peppers", "Airplane" and "Madonna" shown in Fig. 4). These images were subjected to four-level wavelet decomposition and subsequently watermarked.

In order to compare the performance of the particular watermark types, the watermarked images were subjected to attacks. The attacks performed on these watermarked images were JPEG compression, additive noise (referred to as noise addition here), image cropping (see Fig. 5(a)) and image rotation (which leads to the cropping of the corners of the images and is referred to as corner cropping in this paper).

JPEG is a lossy compression technique designed to exploit known limitations of the Human Visual System (HVS), notably the fact that small changes in the image will go unnoticed when viewed by the human eye. Noise addition refers to the addition of a noise signal to a cover image. Any unwanted signal within an image is considered to be noise. The signal-to-noise ratio (SNR) is a widely used metric which represents a measure of image quality in the presence of noise; the higher the value of the SNR the lower the level of noise in an image [41]. In this study, the noise type which was added to the images was Poisson noise [34].

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 3 shows the results of attacking the watermarked images with JPEG compression. It can be seen that the watermarks generated when $a = 3.85$ for the logistic map outperform the other watermark types with the lowpass chaotic watermark performing best for one of the other images. Watermarks generated when $a = 3.85$ have been shown to be lowpass in nature [33]. It is therefore expected that lowpass watermarks would perform best for this attack, given that lowpass water-

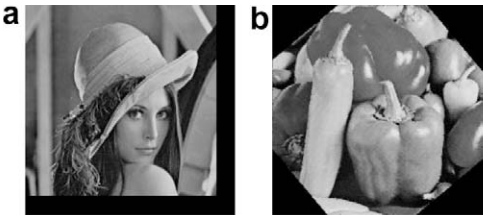

Fig. 5. (a) Lena image cropped by 9% and, (b) Peppers image rotated by 50°.

Table 3
Results of the robustness of the test images to JPEG compression for different watermark types.

Type	Lena	Peppers	Airplane	Madonna
HPN	7:1	9:1	5:1	5:1
HPC	15:1	13:1	7:1	6:1
LPC	9:1	14:1	8:1	9:1
WN	11:1	9:1	6:1	8:1
BN3	8:1	9:1	7:1	8:1
BN9	4:1	4:1	2:1	3:1
Log3.7	7:1	4:1	3:1	4:1
Log3.85	9:1	13:1	9:1	13:1

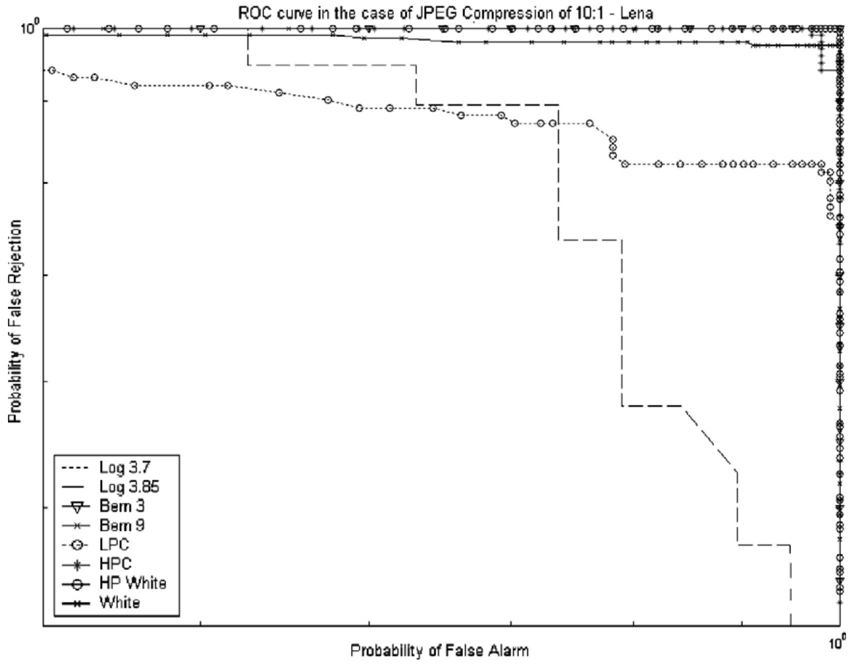

Fig. 6. ROC curve for watermarking schemes based on highpass chaotic signals, lowpass chaotic signals, white noise signals, highpass white noise signals, signals generated from the logistic map and signals generated from the Bernoulli map, after a JPEG compression ratio of 10:1 – "Lena".

marks have increased robustness to image distortions that have lowpass characteristics (filtering, nonlinear filtering such as median filtering, lossy compression, etc.) [42].

Fig. 6 shows a sample ROC curve generated in the case of a JPEG compression ratio of 10:1, as applied to the "Lena" image, for the eight watermark types. It may be observed in this case that the watermark signals generated from the logistic map with a seed of 3.85 perform the best for this level of attack. The lowpass chaotic watermarks generated from the skew tent map have the next best performance of the watermark types under investigation. This is what is to be expected as these watermark types have the best performance for this attack. All the other watermark types under investigation are shown to have similar robustness levels for this level of attack. This is in keeping with what is presented in Table 3.

Table 4 shows the robustness of the four watermarked test images to the addition of noise. It can be seen that the lowpass watermarks generated from the skew tent map perform best for this attack.

Fig. 7 shows an ROC curve generated in the case where noise was added to the test image "Peppers" which resulted in an SNR of approximately 23 dB. The superior performance of the logistic map watermark, generated when $a = 3.85$, may be observed over the other watermark signal types. Again, this corresponds with the findings outlined in Table 4. In this curve it is observed that the lowpass watermarks generated from the skew tent map have the next best performance with all the other watermark types having similar performance for this level of attack. This is in line with the results presented in Table 4.

Table 4
Results of the robustness of the test images to noise addition (dB) for different watermark types.

Type	Lena	Peppers	Airplane	Madonna
HPN	22.70	21.24	24.25	23.98
HPC	22.30	20.91	23.23	24.36
LPC	21.15	20.44	22.20	20.94
WN	20.72	28.83	22.71	21.82
BN3	21.80	22.63	24.14	20.99
BN9	23.88	23.02	25.16	23.86
Log3.7	22.03	24.63	23.78	32.50
Log3.85	23.60	19.78	23.76	26.59

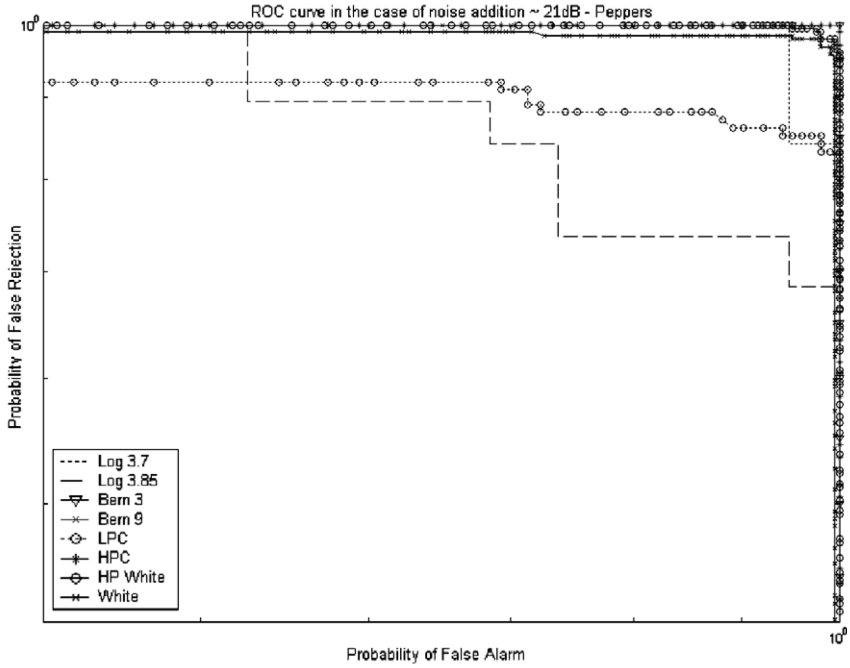

Fig. 7. ROC curve for watermarking schemes based on highpass chaotic signals, lowpass chaotic signals, white noise signals, highpass white noise signals, signals generated from the logistic map and signals generated from the Bernoulli map, after the addition of noise resulting in an SNR of ≈23 dB – “Peppers”.

Fig. 8 shows an ROC curve in the case where the test image “Lena” was cropped by 30% of its width and 30% of its height. It can be seen that all eight watermark types had demonstrated a similar robustness to this level of cropping attack. This is anticipated from analysing the results of Table 5. It can be seen that all of the watermark signals types used were all robust to this level of attack for the “Lena” cover image.

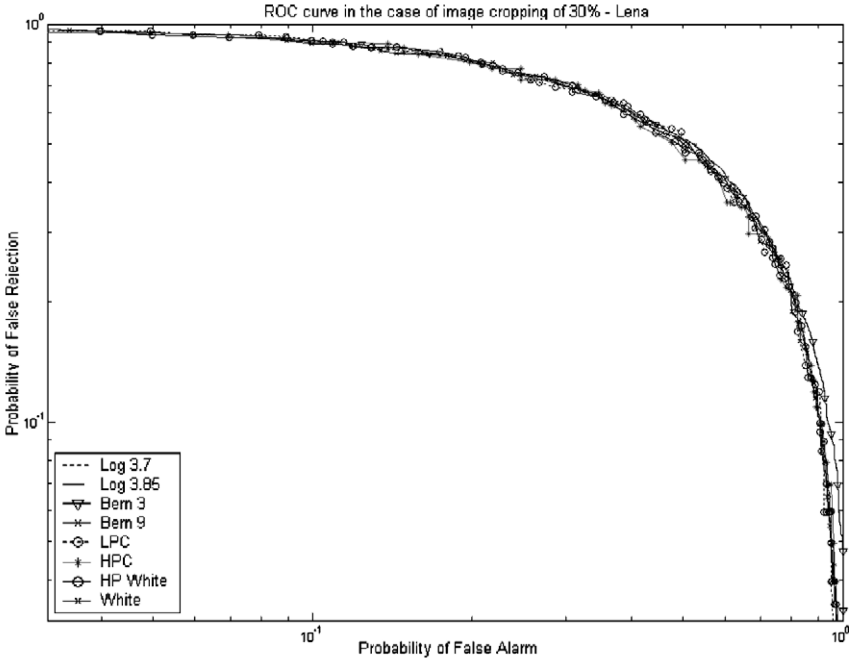

Fig. 8. ROC curve for watermarking schemes based on highpass chaotic signals, lowpass chaotic signals, white noise signals, highpass white noise signals, signals generated from the logistic map and signals generated from the Bernoulli map, after image cropping of 30% – “Lena”.

Table 5
Results of the robustness of the test images to image cropping for different watermark types.

Type	Lena (%)	Peppers (%)	Airplane (%)	Madonna (%)
HPN	36	31	14	28
HPC	49	42	16	29
LPC	28	36	24	23
WN	36	34	23	28
BN3	40	35	22	26
BN9	43	38	24	28
Log3.7	31	30	23	34
Log3.85	36	31	23	22

6. Conclusion

In this paper a comparison has been performed between watermarks generated from chaotic functions and pseudorandom number sequences and the results were presented. In particular, a comparison was carried out between highpass skew map chaotic watermarks, lowpass skew map chaotic watermarks, white noise watermarks (pseudorandom number watermarks), highpass coloured white noise watermarks, watermarks generated from the Bernoulli map and watermarks generated from the logistic map. Chaotic watermarks offer superior performance over the pseudorandom based watermarks with lowpass chaotic signals having the best overall performance for the attacks discussed. The capacities of the test images were also calculated and it was demonstrated that the images that possessed the most information content contained within edges had the highest capacities of the images tested.

It can be seen from the results presented that lowpass chaotic signals generated from the skew tent map and from the logistic map perform with the highest robustness for the different watermark types subjected to attack. In addition to the lowpass chaotic watermarks, the highpass chaotic watermarks generated also account for a large proportion of the best performing image/watermark pair, showing the benefits of using chaotic watermark signals. Chaotic signals offer a suitable 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 over the more widely used pseudorandom sequences in watermarking applications when subjected to common watermark attacks.

References

[1] Arnold M, Schmucker M. Techniques and applications of digital watermarking and content protection. Artech House; 2003.
[2] Cox IJ, Doërr G, Furon T. Watermarking is not cryptography. In: Proceedings of the fifth international workshop on digital watermarking; 2006.
[3] Cox IJ, Miller ML, Bloom JA. Digital watermarking. London: Morgan Kaufman; 2002.
[4] Fan Z, Hongbin Z. Capacity and reliability of digital watermarking. In: Proceedings of the international conference on the business of electronic product reliability and liability; 2004. p. 162–5.
[5] Du J, Woo C-S, Pham B. Recovery of watermark using differential affine motion estimation. In: Proceedings of third AISW, vol. 44; 2005. p. 81–8.
[6] Cox IJ, Miller ML, McKellips AL. Identification and protection of multimedia information. Proc IEEE 1999;87 [special issue].
[7] ÓRuanaidh JJK, Pereira S. A secure robust digital image watermark, electronic imaging: processing, printing and publishing in colour; 1998.
[8] Venkatesan R, Jakubowski M. Image watermarking with better resilience. In: Proceedings ICIP 2000; 2000.
[9] Barni M, Bartolini F, Piva A. Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans Image Process 2001;10:783–91.
[10] Lee CH, Lee HK. Geometric attack resistant watermarking in wavelet transform domain. Opt Exp 2005;13:1307–21.
[11] Tefas A, Nikolaidis A, Nikolaidis N, Solachidis V, Tsekeridou S, Pitas I. Markov chaotic sequences for correlation based watermarking schemes. Chaos, Solitons & Fractals 2003;17:567–73.
[12] Mooney A. The generation and detection of chaos based watermarks, Ph.D. Thesis, Department of Computer Science, National University of Ireland Maynooth; 2005.
[13] Mooney A, Keating JG, Heffernan DM. A detailed study of the generation of optically detectable watermarks using the logistic map. Chaos, Solitons & Fractals 2006;30:1088–97.
[14] Mooney A, Keating JG, Pitas I. A comparative study of chaotic and white noise signals in digital watermarking. Chaos, Solitons & Fractals 2008;35:913–21.
[15] Ruelle D. Deterministic chaos: the science and the fiction. Proceed Roy Soc Lond A 1990:241–8.
[16] Devaney RL. A first course in chaotic dynamical systems – theory and experiment. Cambridge (MA): Perseus Books; 1992.
[17] Lorentz E. Predictability: does the flap of a butterfly's wings in Brazil set off a Tornado in Texas? New York Academy of Sciences; 1963.
[18] Ott E. Chaos in dynamical systems. Cambridge: Cambridge University Press; 1993.
[19] Tefas A, Nikolaidis A, Nikolaidis N, Solachidis V, Tsekeridou S, Pitas I. Performance analysis of watermarking schemes based on skew tent chaotic sequences. In: Proceedings of the NSIP'01, vol. 51; 2001. p. 1979–94.
[20] Tsekeridou S, Solachidis V, Nikolaidis N, Nikolaidis A, Tefas A, Pitas I. Statistical analysis of a watermarking system based on Bernoulli chaotic sequences. Signal Process 2000;81:1273–93.
[21] Marek M, Schreiber I. Chaotic behaviour of deterministic dissipative. Cambridge: Cambridge University Press; 1991.
[22] Mohanty SP, Ramakrishnan KR, Kankanhalli M. A dual watermarking technique for images. In: Proceedings of the seventh ACM international conference on multimedia; 1999. p. 49–51.
[23] Cox IJ, Kilian J, Leighton T, Shamoon T. Secure spread spectrum watermarking for images, audio and video. In: Proceedings international conference on image processing, ICIP'96; 1996. p. 243–6.
[24] Tefas A, Nikolaidis A, Nikolaidis N, Solachidis V, Tsekeridou S, Pitas I. Statistical analysis of markov chaotic sequences for watermarking applications. Proceed IEEE Int Sympos Circuits Syst 2001;2:57–60.
[25] Mooney A, Keating JG. Optical and digital technique for watermark detection. Proceed SPIE Opt Inform Syst 2003;5202:97–105.
[26] Dawei Z, Guanrong C, Wenbo L. A chaos-based robust wavelet-domain watermarking algorithm. Chaos, Solitons & Fractals 2004;22:45–54.

[27] Tefas A, Nikolaidis A, Nikolaidis N, Solachidis V, Tsekeridou S, Pitas I. Performance analysis of correlation-based watermarking schemes employing markov chaotic sequences. IEEE Trans Signal Process 2003;51:1979–94.
[28] Nikolaidis N, Tsekeridou S, Nikolaidis A, Tefas A, Solachidis V, Pitas I. Applications of chaotic signal processing techniques to multimedia watermarking. In: Proceedings of the IEEE workshop on nonlinear dynamics in electronic systems; 2000. p. 1–7.
[29] Tsekeridou S, Solachidis V, Nikolaidis N, Nikolaidis A, Tefas A, Pitas I. Bernoulli shift generated watermarks: theoretic investigation. In: Proceedings of IEEE international conference on acoustics, speech and signal processing; 2001. p. 1989–92.
[30] Tsekeridou S, Solachidis V, Nikolaidis N, Nikolaidis A, Tefas A, Pitas I. Theoretic investigation of the use of watermark signals derived from bernoulli chaotic sequences, SCIA2001; 2001.
[31] Zhang J, Tian L. A new watermarking method based on chaotic maps. In: Proceedings of IEEE, multimedia and expo conference, vol. 2; 2004. p. 939–42.
[32] Xiang H, Wang L, Lin H, Shi J. Digital watermarking systems with chaotic sequences. Proceed Security Watermarking Multimedia Contents 1999:449–57.
[33] Mooney A, Keating JG. The impact of the theoretical properties of the logistic function on the generation of optically detectable watermarks. In: Proceedings SPIE, technology for optical countermeasures, optics/photonics in defence and security, vol. 5615; 2004. p. 120–9.
[34] Mooney A, Keating JG. Noisy optical detection of chaos-based watermarks. In: Proceedings SPIE, photonics north, vol. 5579; 2004. p. 341–0.
[35] Mooney A, Keating JG. Generation and detection of watermarks derived from chaotic functions. In: Proceedings SPIE, imaging and vision, opto-Ireland, vol. 5823; 2005. p. 58–69.
[36] Si H, Li CT. Encyclopedia of virtual communities and technologies – copyright protection in virtual communities through digital watermarking. Idea Group Publishing; 2005.
[37] Cox IJ, Killian J, Leighton T. Secure spread spectrum watermarking for multimedia. In: Proceedings of the IEEE international conference on image processing, ICIP'97, vol. 6; 1997. p. 1673–87.
[38] Daren H, Jiufen L, Jiwu H, Hongmei L. A DWT-based image watermarking algorithm. IEEE Int Conf Multimedia and Expo 2001:429–32.
[39] Shannon CE. A mathematical theory of communication. Bell Syst Tech J 1948;27:373–423.
[40] Canny J. A computational approach to edge detection. IEEE Trans Pattern Anal Mach Intell 1986;8:679–98.
[41] Kutter M, Petitcolas FAP. A fair benchmark for image watermarking systems. Proceed SPIE Security Watermarking Multimedia Contents 1999;3657:226–39.
[42] Fridrich J. Combining low-frequency and spread spectrum watermarking. Proceed SPIE Sympos Opt Sci Eng Instrum 1998;3456.