16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP

ROBUST WATERMARKING OF DIGITAL IMAGES BASED ON CHAOTIC MAPPING AND DCT

E. Chrysochos, V. Fotopoulos, and A. N. Skodras
Digital Systems & Media Computing Laboratory,
School of Science and Technology, Hellenic Open University,
13-15 Tsamadou st., GR-26222, Patras, Greece
phone: + (30) 2610367535, fax: + (30) 2610367520, email: {e.chrysochos, vfotop1, skodras}@eap.gr
web: dsmc.eap.gr

ABSTRACT

In this paper, a new robust watermarking scheme is presented. The algorithm is based on a chaotic function and a correlation method for detection, operating in the frequency domain. The proposed scheme is blind and comparing to other chaos related watermarking methods, experimental results exhibit satisfactory robustness against a wide variety of attacks such as filtering, noise addition, geometric manipulations and JPEG compression with very low quality factors. The scheme also outperforms traditional frequency domain embedding both in terms of robustness and quality.

1. INTRODUCTION

In recent years digital media have spread worldwide. As the media industry grows, the need for media distribution grows along. The digital distribution through Internet is a common practice among media community, but certain problems have risen along with it [1]. The main problem media industry faces today is copyright control, since it suffers from huge economic losses due to illegal copy and distribution of digital copyrighted material. Thus authentication and copyright protection have become necessary practices [2] and there is an increasing interest in the area of digital watermarking [3]. Digital watermarking stands for embedding a signature signal, called 'watermark', into a digital cover, in order to prove ownership, check authenticity or integrity of the cover, and it may relate to audio, images, video or even text.

Image watermarking schemes are usually categorized according to three factors [4]: a) The domain in which the information (watermark) is embedded (e.g. spatial, DCT, DWT, other), b) the type of the watermark embedded (e.g. random sequence, binary logo), and c) the target application for which the watermarking scheme is intended for (e.g. copyright protection, broadcast monitoring, tamper detection).

We refer to *robust* watermarking when the watermark is still detectable after various removal procedures (accidental or malicious) called *attacks*, whereas we refer to *fragile* watermarking, when the slightest alteration of the image, is detectable or noticeable in the content of the watermark. Robust watermarking is usually used for copyright control, whereas fragile watermarking is usually used for integrity check and authentication.

One rather intriguing category of digital watermarking is based on chaos theory and chaotic functions. In image processing the chaotic functions used are two-dimensional, and are known as chaotic maps. There are many such functions but the most famous for images is the *Arnold's cat* map.

Voyatzis and Pitas [5] first presented a chaotic watermarking scheme in spatial domain, which used toral automorphism. A two-dimensional chaotic function was applied on a watermark logo in order to mix and spread its content spatially. Afterwards the chaotic logo was embedded in the host image, achieving less detectability and more robustness against attacks.

Zhao et al [6] presented a watermarking algorithm in wavelet domain which uses a chaotic map, called "logistic map". The image is divided in non overlapping 8x8 blocks and some of them are selected to create a sub image. The selection of the blocks is based on the chaotic logistic map. The sub image is then transformed in the DWT domain where a watermark sequence, created also by the logistic map, is embedded.

Yeh and Lee in [7] proposed a block-based, fragile watermarking technique in spatial domain. An authentication signature, along with a relation signature, intended for recovery purposes, is embedded in the two least significant bits of each pixel, for every block. In this case, toral automorphism is applied in order to create block relations. Therefore recovery and authentication data (recovery and authentication signature respectively), of each block is spread to other blocks by using a chaotic map as a spreading function.

Wu and Shih [8] proposed an algorithm based on a chaotic map and a reference register, for improving watermarking capacity, by breaking local spatial similarity and generating more significant coefficients in the transformed domain. In the present communication we apply chaotic mapping to images in order to create a noise-like version, before applying the DCT transform to it as a whole. A random sequence is afterwards embedded in the DCT transform coefficients. For detection, the improved correlation-based method of [11] is used in order to decide if a test image is watermarked or not.

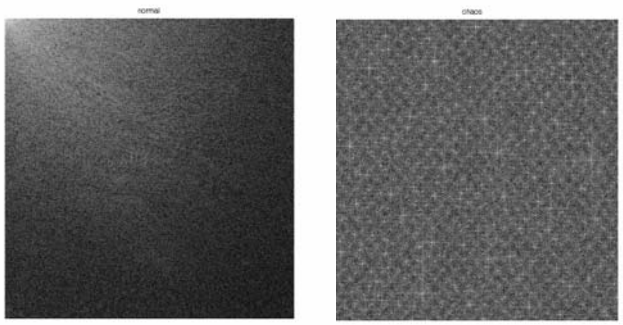
The rest of this paper is organized as follows. In section 2 the chaotic function and its properties are described, and the proposed watermarking scheme is demonstrated. In section 3 experimental results are presented, while conclusions are drawn in section 4.

2. PROPOSED IMAGE WATERMARKING SCHEME

2.1 Chaotic function

Chaotic systems are deterministic (predictable, if enough information is provided) systems that are governed by non-linear dynamics. These systems show deterministic behaviour which is very sensitive to its initial conditions, in a way that the results are uncorrelated and seem random.

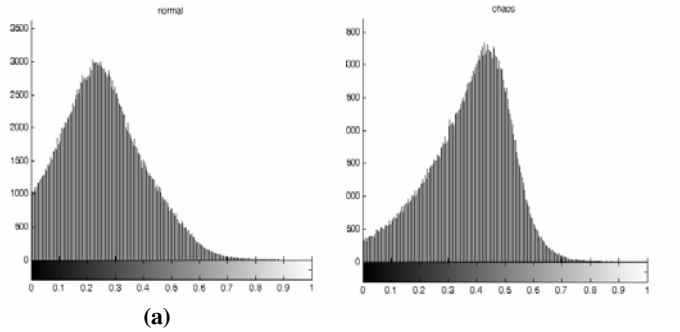
One category of chaotic systems is chaotic maps. A chaotic map, which can be considered as a two dimension chaotic function, is a tool that relocates the pixels of an image and breaks spatial continuity. If we transform the resulting chaotic image in the frequency domain, the number of coefficients of significant value is highly increased in comparison with the respective transformed image as has been shown in [8]. In figure 1 the power spectrum of DCT coefficients for Lena, with and without the use of chaos is presented. The coefficients are in logarithmic scale and have been normalized with regard to the DC coefficient.



(a) **(b)**

Figure 1 – Power spectrum of DCT coefficients for normal (a) and chaotic (b) Lena image

In figure 2 the histograms of the respective DCT coefficients are presented. As can be seen in figures 1 and 2, the transformed chaotic image is richer in frequency content, a desirable property in watermarking, as there are more suitable candidate coefficients for manipulation and information embedding.



(a)

Figure 2 – Histogram of DCT coefficients for normal (a) and chaotic (b) Lena image

Voyatzis and Pitas in [5] presented a watermarking scheme based on a two dimensional chaotic function, called "toral automorphism". This cyclic chaotic function, each time applied on a square image, rearranges its pixels. After it is applied T times, where T is the period of the function, the pixels return to their initial location. If (x, y) are the initial coordinates of a pixel, the outcome coordinates of the chaotic function (x', y') are given by (1)

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \ell & \ell+1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \qquad (1)$$

Where N denotes the width of the image and ℓ is an integer parameter, which affects the period T of the chaotic function.

2.2 Features of the proposed scheme

The proposed watermarking scheme has the following features:

- Blind; in order to detect the watermark no original is needed.
- Robust against filtering attacks like low pass filtering, Gaussian noise and median.
- Robust against noise attacks like dust, salt and pepper, speckles and scratches.
- Robust against some mild geometrical attacks like cropping, aspect ratio changes, resizing and rotation, provided synchronization is achieved.
- Multicast; a certain watermark can be embedded several times to increase robustness.
- Applicability to color images.
- No visual degradation of the image.

The basic principle of this scheme is based on the correlation method, applied not in spatial domain, but in frequency domain jointly with a chaotic function. A chaotic map (1) is applied on the host image and the derived chaotic image is transformed in frequency domain with DCT. The energy of the transformed image is scattered throughout all of the DCT coefficients and the resulting DCT matrix has more significant (therefore appropriate for embedding) coefficients. A random sequence is generated according to a seed, which is used as a *key* for the embedding and extraction rocedure.

2.3 Embedding procedure

In order to embed the information in the host image certain parameters must be specified [9]: an integer from which the random sequence derives (*key*), the starting coefficient (*start)*, the total number of DCT coefficients to be affected (*N*), and the strength of the embedding procedure (*a*).

The steps of the embedding algorithm for a grayscale image are depicted in figure 3 and are the following:

a. A random sequence (*w*) is generated according to *key*. The sequence consists of *N* random numbers which are normally distributed with zero mean and unit variance.
b. The period T of the chaotic function (1) for the particular image is calculated.

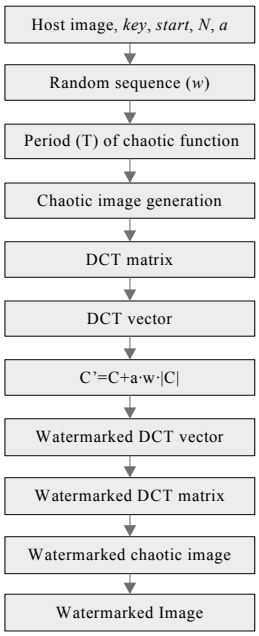


Figure 3 – Embedding procedure

c. The chaotic function (1) is applied $\lfloor T/3 \rfloor$ times to the host image creating the chaotic image. The chaotic image seems more like noise, as shown in figure 4.
d. The DCT coefficients of the chaotic image, as a whole, are calculated formulating the respective DCT matrix.
e. A vector is produced by zigzag scanning the DCT matrix.
f. Each DCT coefficient from *start* to *start*+*N*-1 is altered according to the following rule:

$$C' = C + \alpha \cdot w \cdot |C|$$

where α denotes the strength of the embedding procedure, C' denotes the altered coefficient, C denotes the initial coefficient, and *w* denotes the respective element of the random sequence.
g. The altered coefficients form the watermarked DCT matrix by inverse zigzag scanning.
h. The watermarked chaotic image is generated by applying inverse DCT function on the watermarked DCT matrix.
i. The chaotic function (1) is applied $T - \lfloor T/3 \rfloor$ times to the watermarked chaotic image, producing the final watermarked image.

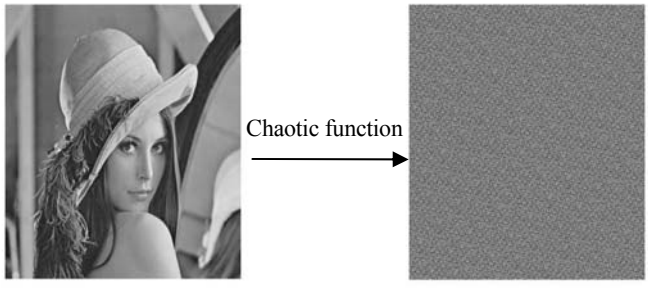


Figure 4 - Host Image (Lena 512x512) and its chaotic representation after applying equation (1) $\lfloor T/3 \rfloor$ times

The watermarking algorithm described, could also be applied to color pictures. The only difference is that instead of gray scale intensity values, some or all of the other color components are used [10]. Therefore the watermark could be embedded more than once, achieving higher robustness.

2.4 Watermark extraction

In order to detect whether an image is watermarked or not, the parameters *start*, *N* and *key*, as well as the improved correlation-based detection method, presented in [11], are used. In [11], except for the right *key*, in order to increase robustness against attacks, a symmetrical precinct (*keyspace*), around the *key* value is used. A typical size for this precinct is ±10. The steps, of the detecting algorithm in a grayscale image are the following:

a. The period (T) of the chaotic function (1) for the specified image is calculated.
b. The chaotic image is generated by applying the chaotic function (1) $\lfloor T/3 \rfloor$ times to the initial image.
c. The DCT coefficients of the chaotic image are calculated formulating the respective DCT matrix
d. A vector is produced by zigzag scanning the DCT matrix.
e. According to *key* a random sequence (*w*) is generated.
f. The correlation between the random sequence and the respective coefficients of the DCT vector is calculated.
g. After calculating the correlation for all the keys in *keyspace*, the detector's output is defined as the ratio of the first maximum to the second maximum of the correlation values in the precinct.
h. If the output is higher than a predefined threshold (*k*), the image is considered to be watermarked; otherwise the image is considered not watermarked.

The extraction procedure is depicted in figure 5.

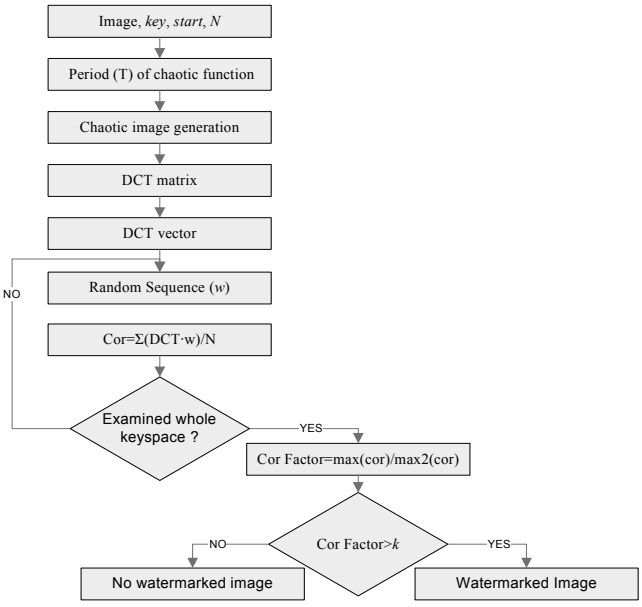


Figure 5 – Extraction Procedure

3. EXPERIMENTAL RESULTS AND COMPARISONS

The robustness of the watermark depends on the strength parameter (*a*), used during embedding (section 2.3). As *a* value increases the robustness of the scheme raises accordingly. Nevertheless this comes with a cost in quality of the watermarked image. As expected, image quality is inversely proportional to robustness. This results from PSNR measurements and objective evaluation of watermarked images.

The correlation method is based on the fact that the sequence (w) generated according to *key*, is normally distributed with zero mean and unit variance. Furthermore DCT coefficients of natural images tend to approximate a Laplacian distribution. Due to this assumption, there is a variation in correlation factor and PSNR results depending on the selected DCT coefficients for the embedding procedure. This is shown in figure 6, where the correlation factor varies depending on the starting coefficient and the number of coefficients affected. A high correlation factor is more robust and therefore, parameters *start* and *N* producing a high correlation factor, are more suitable for achieving robustness against attacks (with the restriction that the resulting quality is acceptable).

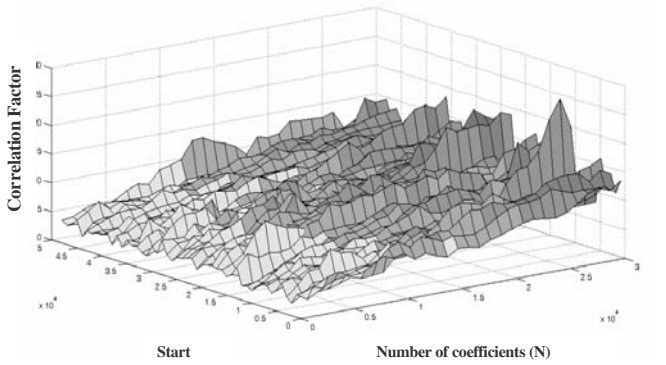


Figure 6 – Correlation factor depending on starting coefficient (*start*) and number of coefficients affected (*N*)

The proposed method, based on chaotic map and improved correlation-based detection method [11], gives better results than the standard method of correlation. In figure 7 we can see two watermarked images, with *a*=0.3, *start*=500 and *N*=10000, watermarked with the chaotic function and the standard method respectively.

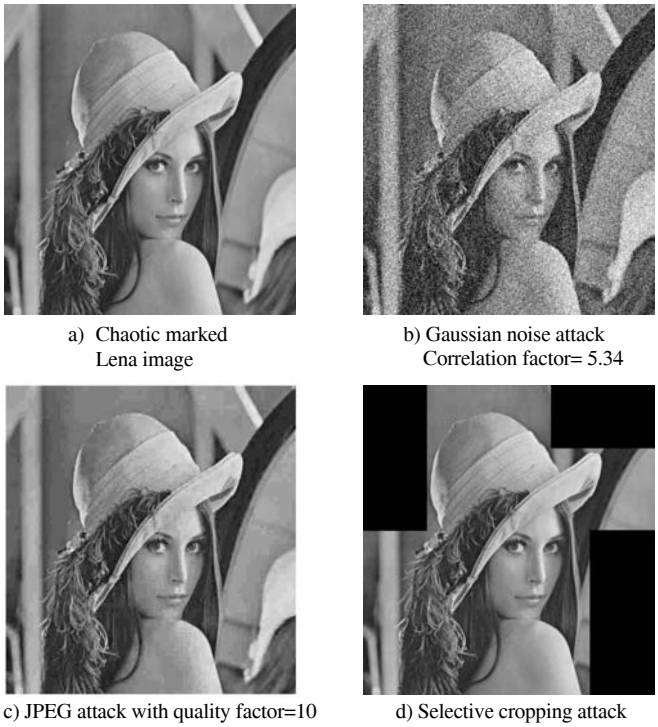
Figure 7 – Chaotic based and standard watermarked Lena image for strength=0.3, start=500 and N=10000

The chaotic implementation produced a watermarked image of PSNR= 45.17dB and correlation factor of 6, while the standard implementation produced a watermarked image of PSNR= 36.61dB and correlation factor of 5.87. The chaotic implementation always outperforms standard correlation method by allowing the selection of parameters that produce similar or higher correlation factors, while the resulting image quality is far superior.

In order to achieve higher robustness (at the expense of image quality) we selected the parameters *a*=0.3, *start*=2 and *N*=40000. The watermarked image, of fair PSNR=36.15dB, shows no obvious degradation, providing a high and robust correlation factor (8.34). In figure 8 we can see some attacks on Lena Image and the respective correlation factors. The threshold for the correlation factor was set to 1.5 which is a perfectly safe value for both Type I and Type II errors.

The proposed chaotic-correlation based scheme shows robustness against filtering attacks like low pass filtering, median filtering and Gaussian blur. The watermark was detectable after JPEG attack, as low as 10% quality, which in 'Lena's case gives a compression ratio of 64:1. The watermark was also not compromised by noise attacks like salt and pepper, dust and speckles, Gaussian and uniform noise. The scheme is also robust to some geometrical attacks like cropping, aspect ratio changes, resizing and rotation, given image synchronization.

Results for images 'Lena', 'peppers', 'baboon' and 'airplane', are presented in table 1.



a) Chaotic marked Lena image

b) Gaussian noise attack Correlation factor= 5.34

c) JPEG attack with quality factor=10 Correlation factor= 1.53

d) Selective cropping attack Correlation factor= 4.05

Figure 8 – Attacks against watermarked Lena image

Table 1 – PSNR and correlation factor results for different images

image	*start*	*N*	*a*	PSNR (dB)	Correlation factor	Correlation factor after JPEG attack with quality=15%
Lena	2	40.000	0.3	36,15	8.34	1.58
peppers	2	40.000	0.3	36,50	10.82	2.29
airplane	2	40.000	0.3	34,25	10.79	1.86
baboon	2	40.000	0.3	33,14	8.76	2.78

The proposed scheme is more robust compared to [7] and [5], as [7] is a fragile implementation and [5] is based on subjective visual observation, which stands up to 6:1 JPEG compression. The method of [6] seems to be more robust against geometrical attacks (due to wavelets features) but no explicit measurements for compression or filtering attacks are mentioned. The method of [8] is outperformed, as it merely withstands JPEG compression down to quality 20 (with PSNR=35.24dB), opposed to JPEG compression with quality factor 10 and PSNR=36.15dB, presented in this work.

4. CONCLUSIONS

A robust watermarking scheme for images is presented, based on correlation method and a chaotic function. The proposed scheme shows robustness against filtering attacks like low pass filtering, median filtering and Gaussian blur, while retaining high visual quality. The watermark is also detectable after JPEG compression, for quality factors as low as 10, and is not compromised by noise attacks like salt and pepper, dust and speckles, Gaussian and uniform noise. The scheme is also robust to some geometrical attacks like cropping, aspect ratio changes, resizing and rotation, given image synchronization.

A crucial factor is the proper selection of the embedding parameters (*strength*, *start* and *N*) which affect the correlation factor and the robustness of the watermark.

Our future work is to combine the proposed algorithm with an image quality metric, suitable for our purpose, in order to produce a scheme which will automatically select the optimum parameters to achieve higher robustness.

ACKNOWLEDGEMENTS

This work was funded by the European Union - European Social Fund (75%), the Greek Government - Ministry of Development - General Secretariat of Research and Technology (25%) and the Private Sector in the frames of the European Competitiveness Programme (Third Community Support Framework - Measure 8.3 - programme ΠΕΝΕΔ - contract no.03ΕΔ832).

REFERENCES

[1] Berghel H. and O'Gorman L., "Protecting ownership rights through digital watermarking", *IEEE Computer Mag*, pp.101-103, July 1996.

[2] Fotopoulos V. and Skodras A., "Digital image watermarking: An overview", in *EURASIP Newsletter*, ISSN 1687-1421, Vol. 14, No. 4, Dec. 2003, pp. 10-19, 2003.

[3] Cox J. and Miller L., "The first 50 Years of electronic watermarking", *EURASIP Journal on Apllied Signal Processing*, pp. 126-132, Feb 2002.

[4] Potdar V.M., Han S. and Chang. E., "A survey of digital image watermarking techniques", in *3rd IEEE International Conference on Industrial Informatics (INDIN)*, Perth, Australia, 10-12 Aug 2005.

[5] Voyatzis G. and Pitas I., "Applications of toral automorphisms in image watermarking", in *Proc IEEE International Conf. on Image Processing*, Lausanne, Switzerland, Sep 1996, vol2, pp.237-240.

[6] Zhao D., Guanrong C. and Wenbo L., "A chaos-based robust wavelet-domain watermarking algorithm", *Chaos, Solitons and Fractals*, vol. 22, pp. 47-54, 2004.

[7] Yeh G.H. and Lee G.C., "Toral fragile watermarking for localizing and recovering tampered image", in *IEEE Symposium on Intelligent Signal Processing and Communication Systems*, Hong Kong, Dec 2005, pp. 321-324.

[8] Wu, Y.T. and Shih, F.Y. "Digital watermarking based on chaotic map and reference register", *Pattern Recognition*, vol.40, no. 12, pp. 3753-3763, Dec 2007.

[9] Fotopoulos V. and Skodras A., "Transform domain watermarking: adaptive selection of the watermark's position and length",in *Proc. Visual Communications and Image Processing (VCIP2003)*, Lugano, Switzerland, 8-11 July 2003.

[10] Gilani S.A.M., Kostopoulos I. and Skodras A., "Color image-adaptive watermarking", in *Proc. 14th Int. Conf. on Digital Signal Processing (DSP2002)*, Vol. 2, pp. 721-724, Santorini, Greece, 1-3 July 2002.

[11] Fotopoulos V. and Skodras A., "Improved watermark detection based on similarity diagrams", in *Signal Processing: Image Communication*, Vol. 17, pp. 337-345, 2002.