Chaotic-Correlation Based Watermarking Scheme for Still Images

E. Chrysochos[1], V. Fotopoulos[1], M. Xenos[1], M. Stork[2], A. N. Skodras[1], J. Hrusak[2]

[1]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, xenos}@eap.gr
[2]Department of Applied Electronics and Telecommunications,
University of West Bohemia
P.O. Box 314, 30614 Plzen, Czech Republic
Email: {hrusak, stork}@kae.zcu.cz

***Abstract* – In this work, a new blind watermarking scheme in frequency domain is presented. The proposed scheme is based on a chaotic function for embedding, and a correlation method for detection. Three-dimensional maps of PSNR and correlation are used for better selection of embedding parameters according to a quality threshold. The scheme shows increased robustness against JPEG compression and cropping. The watermark is also detectable after filtering attacks like low pass filtering, median filtering and Gaussian blur, noise attacks, as well as some geometrical attacks.**

1 INTRODUCTION

In recent years digital media have overcome analogue ones. Since playing records were substituted by Compact Disks the digital era has begun. Media industry, as expected, has turned its attention to acquiring the best digital technology to provide better quality products and distribute them world around. Digital era has brought many conveniences to consumers and media producers but some problems have risen too [1]. The bigger problem media industry faces today is copyright control, since it suffers from huge economic losses due to unauthorized copies. The distribution of media through internet, as well as the nature of digital data, facilitates unauthorized copy and distribution of proprietary media like pictures, songs or movies. Therefore media industry has turned to authentication and copyright protection as necessary practices [2]. The most common technique for authentication and copyright control is Digital Watermarking [3].

Digital Image Watermarking stands for embedding a signature signal, called 'watermark', in a digital image, in order to prove ownership, or check authenticity or integrity of a certain image. We refer to robust watermarking when the watermark is still detectable after various attacks (unintended or malicious), whereas we refer to fragile watermarking, when the slightest alteration of the image, would be noticeable in the context of the watermark. Robust watermarking is usually used for copyright control, whereas fragile watermarking is usually used for integrity check and authentication.

One category of digital watermarking is based on chaos theory and two dimensional chaotic functions, known as chaotic maps. Voyatzis and Pitas [4] first introduced chaos theory in digital watermarking.

Zhao et al [4] presented a watermarking algorithm in wavelet domain which used 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 [5] proposed a block-based, fragile watermarking technique in spatial domain. An authentication signature, along with a relation signature, which is for recovery purposes, is embedded in the two least significant bits of each pixel, for every block. Toral automorphism is applied, in this case, in order to create block relations. Therefore recovery and authentication data (recovery and authentication signature), of each block can be spread to other blocks by using a chaotic map as a spreading function.

Wu and Shih [7] proposed an algorithm based on a chaotic map and a reference register, for enlarging watermarking capacity, by breaking local spatial similarity and generating more significant coefficients in the frequency domain.

In the proposed scheme a two dimensional chaotic map is applied to images creating 'scrambled' images which are then transformed to frequency domain through DCT transform. A random generated sequence is embedded in some of the DCT coefficients. In order to decide which coefficients are more suitable for embedding, 3d maps of PSNR and correlation are used. Given a PSNR threshold, used as a quality

metric, the coefficients that give the maximum correlation are selected. For detection, a correlation method 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 2.1, the chaotic function and its properties are described. In section 2.2 and 2.3, the proposed watermarking scheme, based on chaotic function and correlation is presented. 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 systems (predictable if you have enough information) 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 forthcoming results are uncorrelated and seem random. One category of chaotic systems is chaotic maps. A chaotic map, which can be considered a two dimension chaotic function, is also a tool that could relocate the pixels of an image and break spatial continuity. If we transform the resulting chaotic image in the frequency domain, the significant coefficients are highly increased in comparison with the respective transformed image as has been shown in [7]. Therefore 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.

Voyatzis and Pitas in [4] 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 applied T times, where T is the period of the function, the pixels are found in 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

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

Where N denotes the width of the image and λ is an integer parameter that affects the period T of the chaotic function.

The effect of the chaotic map (1) on Lena image is shown in figure 1. After T iterations, where T depends on image size, the image is restored to its original status.

2.2 EMBEDDING PROCEDURE

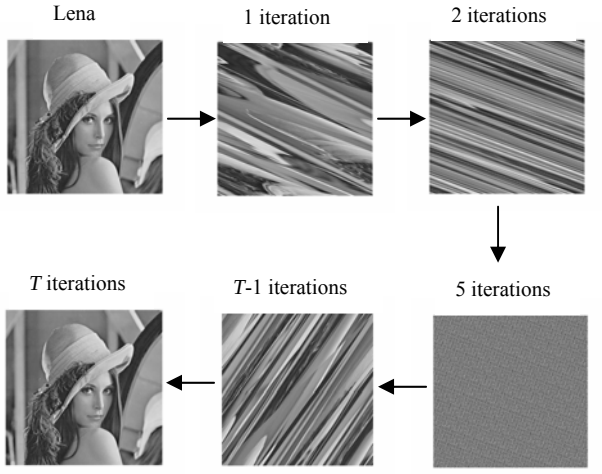

Figure 1 – Application of chaotic map on Lena image

In order to embed the information in the host image certain parameters must be specified. These parameters are embedded in one integer number called key. The key consists of five parts. The first part denotes the starting coefficient (*start*) from where the embedding procedure begins. The second part denotes the total number of DCT coefficients to be altered (*N*). The third part denotes the *seed*, an integer from which the random sequence derives. The fourth part (two digits N2, N3) denotes the length of the second and third part respectively, while the fifth part (*iter*) determines how many times the chaotic function is applied on the image, before the embedding procedure takes place. The strength of the embedding procedure (*a*), as well as the PSNR threshold (*PSNRthres*) considered acceptable, are needed.

The steps of the embedding algorithm for a grayscale image are the following:

a. A random sequence (*w*) is generated according to *seed*. 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 for the particular image is calculated.
c. The chaotic function is applied $\lfloor T / iter \rfloor$ times to the host image creating the chaotic image. The chaotic image seems more like noise, as shown in figure 1.
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:

$$C' = C + a \cdot w \cdot |C| \qquad (2)$$

where 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 is applied $T - \lfloor T / iter \rfloor$ times to the watermarked chaotic image, producing the final watermarked image.

In order to achieve higher correlation factor, i.e. higher robustness to attacks, the above procedure is repeated many times for different *start* and *N* parameters. For each combination of *start* and *N*, PSNR and correlation values are calculated producing respective three-dimensional maps, as shown in figures 2 and 3.

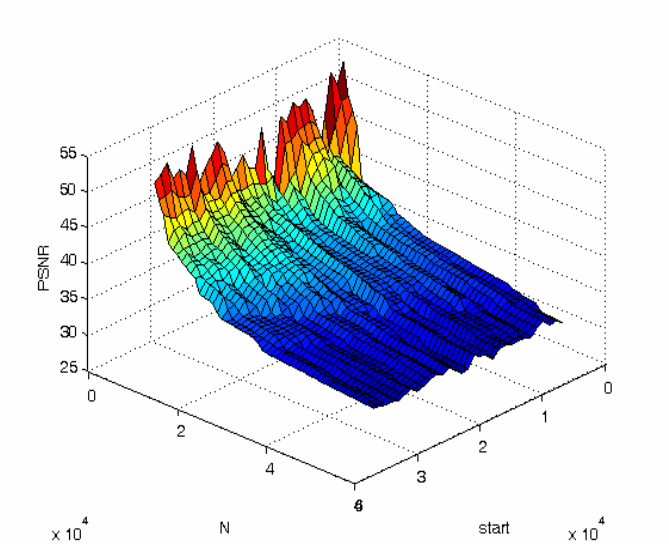

Figure 2 – Application of chaotic map on Lena image for *strength*=0,5

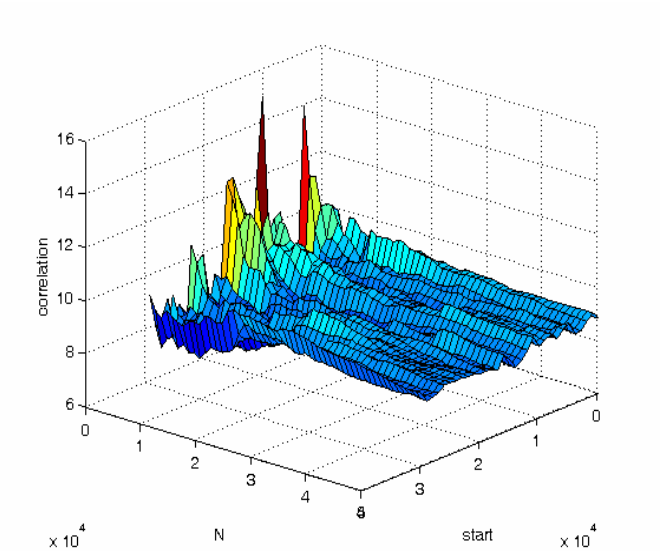

Figure 3 – 3D correlation map with regard to *N* and *start* for *strength*=0,5

For the final embedding, the better combination of *start* and *N* according to PSNR threshold is selected. That is the values of *start* and *N* that give higher correlation factor with respect to *PSNRthres*. The parameters used for embedding generate the key.

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 [8]. Therefore the watermark could be embedded more than once, achieving higher robustness.

2.3 WATERMARK EXTRACTION

In order to detect whether an image is watermarked or not, the *key*, used in the embedding procedure is required. The steps, of the detecting algorithm in a grayscale image are the following:

a. Parameters *start*, *N*, *seed* and *iter* are calculated by *key* as following:

$$N_2 = (key \bmod 100) \operatorname{div} 100 \quad (3)$$

$$N_3 = (key \bmod 100) \operatorname{div} 10 \quad (4)$$

$$start = key \operatorname{div} (10^{N_2+N_3+3}) \quad (5)$$

$$rem1 = key \bmod (10^{N_2+N_3+3}) \quad (6)$$

$$N = rem1 \operatorname{div} (10^{N_3+3}) \quad (7)$$

$$rem2 = rem1 \bmod (10^{N_3+3}) \quad (8)$$

$$seed = rem2 \operatorname{div} 1000 \quad (9)$$

$$iter = key \bmod 10 \quad (10)$$

b. The period (*T*) of the chaotic function for the specified image is calculated.
c. The chaotic image is generated by applying the chaotic function $\lfloor T / iter \rfloor$ times to the initial image.
d. The DCT coefficients of the chaotic image are calculated, as a whole, formulating the respective DCT matrix
e. A vector is produced by zigzag scanning the DCT matrix.
f. According to *seed* a random sequence (*w*) is generated.
g. The correlation between the random sequence and the respective coefficients of the DCT vector is calculated.
h. If the output is higher than a predefined threshold (*corthres*), the image is considered to be watermarked; otherwise the image is considered not watermarked.

3 EXPERIMENTAL RESULTS

The robustness of the watermark depends on the strength parameter (strength) used during the embedding procedure. As the strength increases the robustness of the scheme raises respectively. Nevertheless, the quality of the watermarked image is conversely proportional to strength parameter and robustness.

The correlation method is based on the fact that the sequence (w) generated by *seed*, is normally distributed with zero mean and unit variance. The correlation factor varies depending on the starting coefficient (*start*) and the number of coefficients affected (*N*).

In our experiments the acceptable PSNR threshold (PSNTthres) was set to 40, while the correlation threshold (corthres) which determines whether an image is watermarked or not was set to 4. Strength parameter for the embedding procedure was set to 0,5 and a series of images were used for experimentation. For most images the results were similar, therefore due to limited space, only the results regarding Lena are presented in this work, for comparisons with other methods.

Three-dimensional maps for PSNR and correlation values, with regard to *N* and *start*, were generated for Lena image as shown in figure 2 and 3 respectively. With respect to *PSNTthres* the automated scheme selected parameters *N*=1000, *start*=11002 as optimal for embedding, achieving correlation factor of 15,098 with PSNR value of 40,00dB.

The proposed chaotic-correlation based scheme shows robustness against filtering attacks like low pass filtering, median filtering and Gaussian blur. The watermark was also detectable after JPEG attack, as low as 5% quality, as depicted in figure 4b. In Lena's 512x512 case that corresponds to a compression ratio of 46:1. The watermark was also not compromised by noise attacks like dust and speckles, Gaussian and uniform noise. The scheme exhibits increased robustness against cropping attack. The watermark was detectable after 75% of the image was cropped, as showed in figure 4a. The scheme also shows robustness against geometrical attacks like aspect ratio changes, resizing and rotation, given image synchronization.

a) Cropping attack 75%
Correlation = 4,05

b) JPEG attack with quality factor=5
Correlation = 4,138

Figure 4 – Attacks against watermarked Lena image

The proposed scheme is more robust compared to [6] and [4], as [6] is a fragile implementation and [4] is based on subjective visual observation for detection, and stands up to 6:1 JPEG compression. The method of [5] 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 [7] is outperformed, as it merely withstands JPEG compression down to quality 20 (with PSNR=35,24dB), opposed to JPEG compression with quality factor 5 and PSNR=40,00dB, presented in this work.

4 CONCLUSIONS

A robust watermarking scheme for images, in DCT domain, is presented. The embedding procedure is based on a chaotic function, while the detection of the watermark is based on correlation comparison. In order to select the optimum parameters of *start* and *N*, three-dimensional maps of PSNR and correlation are used.

The proposed scheme shows robustness against filtering attacks like low pass filtering, median filtering and Gaussian blur. The watermark was detectable after JPEG compression, as low as 5% quality, and was not compromised by noise attacks like dust and speckles, Gaussian and uniform noise. The watermark was also robust against up to 75% cropping. The scheme shows robustness to geometrical attacks like aspect ratio changes, resizing and rotation, given image synchronization.

ACKNOWLEDGEMENTS

This work was funded by the European Union - European Social Fund (75%), the Greek Government - Ministry of Development - General Secretariat for 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). It was also funded by the General Secretariat for Research and Technology in the frames of the Czech-Greece Joint Research and Technology Programmes 2005-2007 (grant 4.3.6.1γ-220).

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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.