USING THE CHAOS THEORY AND DYNAMIC KEYS IN DIGITAL WATERMARKING

Cristian-Gabriel APOSTOL[1]
Dorin-Marian PÎRLOAGA[2]
Marius ROGOBETE[3]
Ciprian RĂCUCIU[4]
[1] Eng. Ph.D., Military Electronics and Informatics Systems Faculty, Military Technical Academy, Bucharest, Romania
[2] Ph.D. Std., Eng., Military Electronics and Informatics Systems Faculty, Military Technical Academy, Bucharest, Romania
[3] Ph.D. Std., Military Electronics and Informatics Systems Faculty, Military Technical Academy, Bucharest, Romania
[4] Prof. Eng. Ph.D., Military Electronics and Informatics Systems Faculty, Military Technical Academy, Bucharest, Romania

Abstract: *Digital watermarking is an emerging multimedia security method that has been developed in recent times. It has two main applications: copyright protection and data integrity verification. In this paper we want to show that these applications can be combined with advanced chaotic sequences and dynamic keys in order to increase the security level. At the same time we will show how the two different applications of digital watermarking resist against attacks.*

Key-words: *Digital watermarking, security, multimedia, copyright protection, data integrity verification, chaotic sequences, dynamic keys, increased security level.*

1. INTRODUCTION

With the progress of Internet and digital techniques, it has become increasingly easy to distribute and get digital data. The biggest advantages of digital recording are that the quality does not degrade over time, transmission and copying and that the contents can be transmitted and "sold" over the digital network. The problem consists in protecting against piracy.

How to protect the copyright of digital products has become a great challenge. Digital watermarking is a technique which can be used in the protection and enforcement of intellectual property rights of the digital content involved in the transaction copyright. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. Copyright protection of multimedia data is a very challenging task that drew the attention of both scientists and copyright holders. Data hiding or steganography has emerged as a viable solution for this problem. Data hiding techniques aim at embedding statistically undetectable and perceptually transparent signals, called watermarks, in digital data (still images, audio, video) [1].

Similar to steganography, watermarking is about hiding information in other data. The difference is that a watermark should be somehow resistant against hacker attacks and attempts to remove it.In order to be of any value for copyright protection, watermarks should be permanently embedded into the digital products.

There is a number of desirable characteristics that a digital watermarking technology can offer, including security, imperceptibility, and robustness [2].

Watermarking techniques can be broadly classified into two categories: special domain methods and transform domain methods. Special domain methods embed the watermark into the gray values of the pixels directly and they are not robust against attacks. Transform domain watermarking techniques are more robust than spatial domain methods [3]. Before embedding robust watermarks into a host-image, engineers usually modulate the coefficients in a transform domain such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) [4].

2. SECURITY AND CHAOS

In recent studies chaotic sequences have proven that they can be used in security issues. They can be generated with the help of a chaotic map which is determined by initial condition and parameters. A large number of uncorrelated, random like, yet deterministic chaotic sequences can be exploited to encrypt the original watermark signal. The encrypted watermark signals are embedded in the image to form a set of watermarked images that will be distributed to different customers. In this way we can trace down the distribution of the image just according to the extracted watermark.

The PWLCM (Piece Wise Linear Chaotic Map) – marimea fontului pe site.

As shows in [1] the PWLCM has a more linear distribution than other chaotic maps and the random values are scrambled with the same probability. The chaotic values are obtained with the help of the chaotic map, by applying a number of iterations, in the following manner:

$$x(n+1) = f_{PWLC}(x(n)) \tag{1}$$

where, $f_{PWLC} : [0,1] \rightarrow [0,1]$ is defined as:

$$f_{PWLC}(x) = \begin{cases} \dfrac{x}{p}, & 0 \le x \le p \\ \dfrac{x-p}{0.5-p}, & p < x \le 0.5 \\ f_{PWLC}(1-x) & 0.5 < x \le 1 \end{cases} \tag{2}$$

Where *p* is the positive control parameter.

3. DATA INTEGRITY DIGITAL WATERMARKING USING CHAOTIC MAPS (PWLCM)

3.1 Embedding Process

In order to insert the watermark information in the original image we have to take the following steps:

a) Image Transformation of *H* from the RGB (Red-Green-Blue) domain to the YCbCr (Luminance and Chrominance) domain

b) 8×8 block splitting of the luminance *L*.
c) 8×8 block DCT transform.
d) Block Quantization using the standard JPEG quantization table; we obtain the quantized DCT coefficients f_{Q_k}.
e) Set LSB plane to zero of the quantized DCT coefficients $f_{Q_k}^{0}$.
f) Chaotic iteration of the PWLCM with a *dynamic key* for every coefficient:

$$n_i = n + \sum\nolimits_{k=1}^{i} f_{Q_k} \tag{3}$$

We start the iteration from the initial value $f_Q \,/\, f_{\max}$.

g) Thresholding the chaotic value and obtain the watermark information.
h) Embedding the watermark information in the LSB of $f_{Q_k}^{0}$ and obtaining the watermarked quantized DCT coefficients $f_{Q_k}^{W}$.
i) Block de-quantization
j) Block IDCT
k) RGB transformation and obtaining the watermarked image $H^{'}$.

3.2 Extraction Process

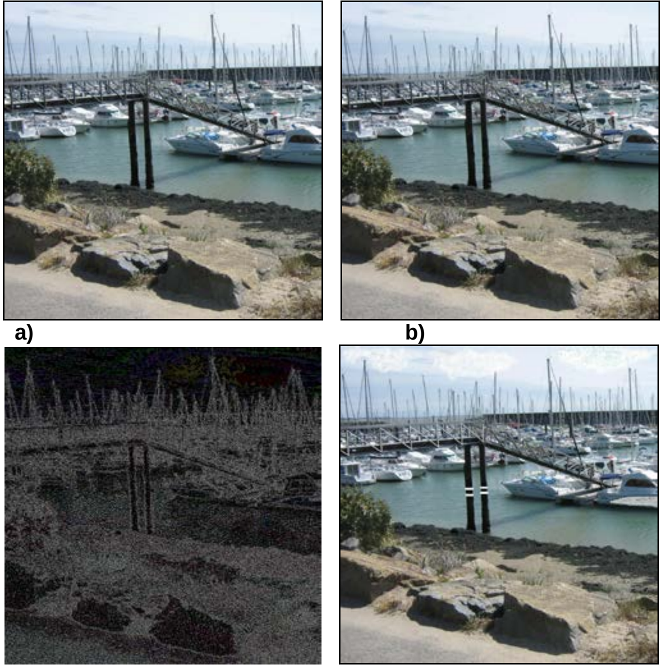
a) Luminance transformation of the host image *H*.
b) 8×8 block splitting of the luminance *L*.
c) 8×8 block DCT transform.
d) Block Quantization using the standard JPEG quantization table; we obtain the quantized DCT coefficients f_{Q_k}.
e) LSB extraction
f) Chaotic iteration of the PWLCM with a *dynamic key* for every coefficient:

$$n_i = n + \sum\nolimits_{k=1}^{i} f_{Q_k} \tag{4}$$

We start the iteration from the initial value $f_Q \,/\, f_{\max}$.

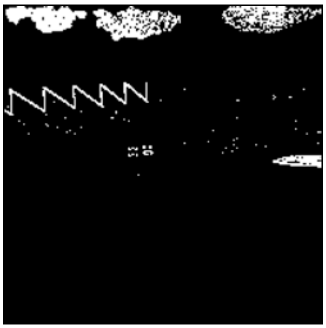
g) Thresholding the chaotic value and obtain the watermark information.

If the watermark information is the same as the LSB of the quantized DCT then the image was not falsified. If they are different, the entire 8×8 pixels block is considered to be tampered.



a) **b)**

c) **d)**



e)

Figure 1: a) Original "Yacht" image; b) Watermarked "Yacht" image; c) The 20 times amplified difference between the original image and the watermarked image; d) Falsified image; e) Detected tampered regions

4. COPYRIGHT PROTECTION DIGITAL WATERMARKING USING CHAOTIC MAPS (PWLCM)

4.1 Embedding process

a) Image Transformation of *H* from the RGB (Red-Green-Blue) domain to the YCbCr (Luminance and Chrominance) domain
b) 8 × 8 block splitting of the luminance *L*.
c) 8 × 8 block DCT transform.
d) Block Quantization using the standard JPEG quantization table; we obtain the quantized DCT coefficients f_{Q_k} .
e) Determine the positions of the coefficients inside the blocks that will carry the watermark bits:

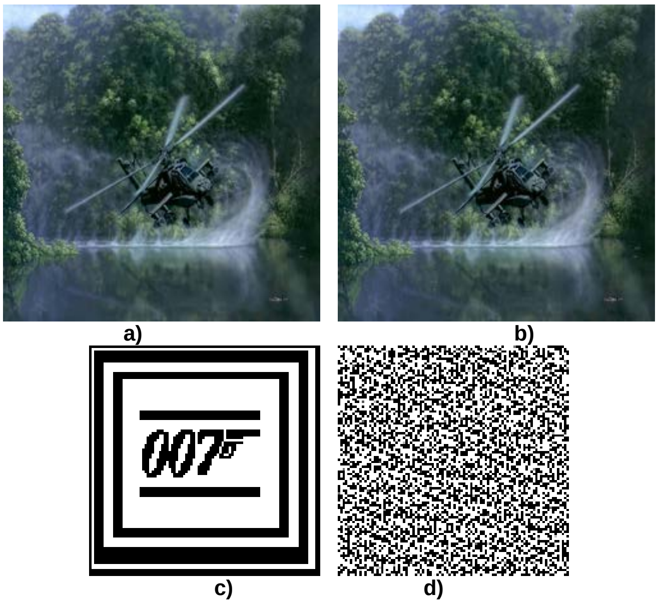
In order to achieve this we iterate the PWLCM n_2 times and obtain x_{n_2} , $0 \le x_{n_2} \le 1$. With the help of x_{n_2} we determine the first position k_1 of the coefficient inside the first block that will hide the first watermark bit. k_i with *i=1,2,...,* $M_W \times N_W$ is a number between 1 and 10 and it is obtained by dividing the interval of the chaotic values (0,1) into 10 equal subintervals. For the second block the number of iterations applied to the PWLCM chaotic map is increased with the value of the position of the previouslee selected coefficient t, in order to get a different position of the information carrying coefficients for every block. In this manner we obtain a feedback chain mechanism.

$$n_i = n_{i-1} + k_{i-1} \tag{5}$$

f) Embedding the watermark bits, in the LSB of the selected medium frequency quantized DCT coefficients in every block, using the Zigzag scan order.
g) Block de-quantization
h) Block IDCT
i) Image Transformation from Luminance and Chrominance domain to the new Red Green Blue colour domain and obtain the watermarked image *H'*.

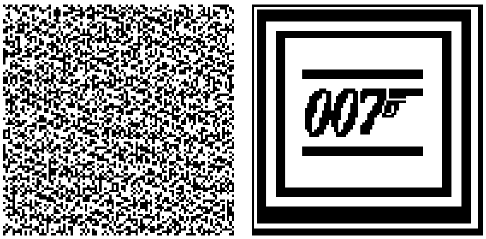
4.2 Extraction Process

The extraction consists in following the first 5 steps of the embedding process in the same manner on the watermarked image. The difference consists in the *f)* step: LSB extraction from the selected quantized DCT coefficients.



a) **b)**

c) **d)**



e) f)

Figure 2: a) Original image; b) Watermarked image; c) watermark; d) encrypted watermark; e) extracted watermark; f) decrypted watermark

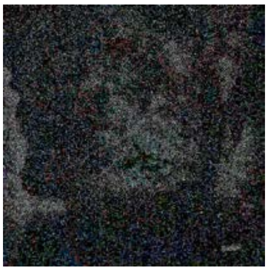
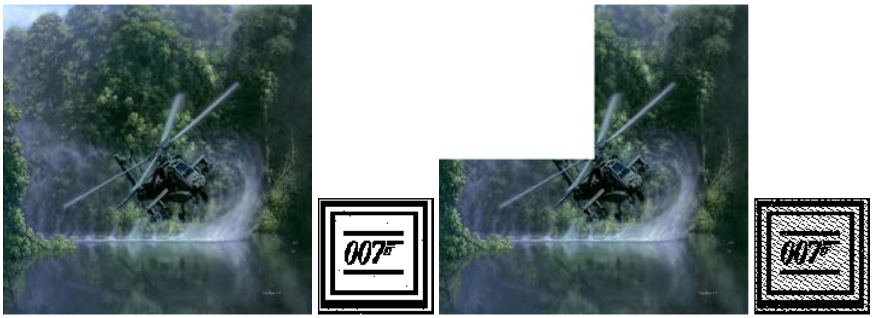
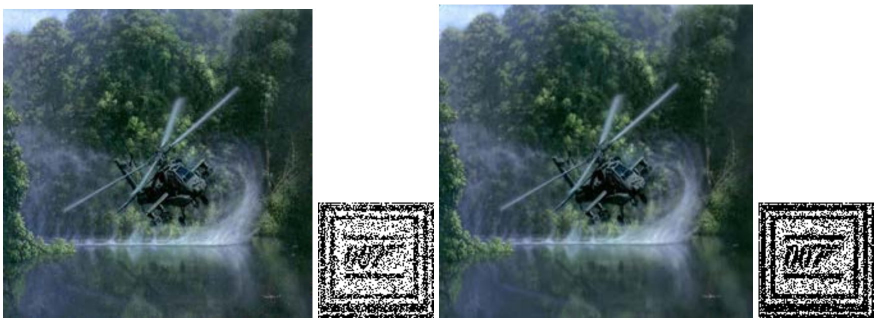


Figure 3: 30 times amplified difference between a) and b)



a) b) c) d)

Figure 4: a) JPEG compressed image; c) Cropped (0.25) image; b); d) extracted watermarks



a) b) c) d)

Figure 5: a) Salt & Pepper Noised (0.01) image; c) Median Filtered image; b); d) extracted watermarks

5. CONCLUSIONS

The need of information security has determined a continuous activity to find new solution to design more and more secure and robust protection methods. The dynamic keys combined with the randomness of the PWLCM increase the number of iterations for every component in a different way. This ensures security and robustness in the same time as we can see from the attack results. Invisibility is obtained because we mark the LSB of the medium frequency quantized DCT coefficients. Blind watermarking is achieved in both of the presented methods because we don't need the original image for extraction. The PWLCM is efficiently used to scramble the message inside the cover image, with its help the horizontal and vertical pixel positions are selected. We use a single PWLCM function, with the zigzag scan order one for vertical pixel selection and horizontal coefficient selection. The uniform distribution of the chaotic values generated with the PWLCM hides information in all of the pixels with an equal probability and it has been demonstrated that it has better results than the logistic map because of its non-uniform distribution. The distribution of PWLCM has uniform values compared to the distribution of the logistic map as shown from the simulations; this is a contribution to the initial design for increasing the level of security. It's also important to note the sensitivity to initial value and parameter of the chaotic functions used, i.e. small changes in key values (initial conditions) will lead to drastic changes in the resulted values produced by iterating the chaotic functions.

We can obtain blind detection by hiding the key in the image, for example the key can be composed of the initial value: the first pixel divided by 255 in order to have a value in the [0,1] interval and the number of iterations the dimension of the image. The watermarking technology has a wide variety of applications like copyright protection and data integrity verification. For further study I would like to integrate this technology with the WiMAX radio communications standard for user and data authentication inside the network architecture.

REFERENCES:

[1] Cristian-Gabriel Apostol, Cristian-Iulian Rincu, Digital watermarking secured with PWLCM, chaotic feed-back and LSB data hiding, *2010 International Conference on Communications*, Vol. 2, pp. 439-442. Print ISBN: 978-1-4244-6360-2

[2] Daniel Caragata, Anca-Livia Radu, Safwan El-Assad, Cristian-Gabriel Apostol, Chaos Based Fragile Watermarking Algorithm for JPEG Images, ICITST-2010, London, U.K. E-ISBN : 978-0-9564263-6-9

[3] Weiwei Xiao, Zhen Ji, Jihong Zhang, Weiying Wu, A watermarking algorithm based on chaotic encryotion, Proceedings of IEEE TENCON'02, Volume 1, pp. 545-548, Print ISBN: 0-7803-7490-8

[4] Zhao Yantao, Ma Yunfei, A robust chaos-based DCT-domain watermarking algorithm*,* IEEE ICSSE 2008, pp. 935-938, Print ISBN: 978-0-7695-3336-0

[5] Rasul Enayatifar, Fariborz Mahmoudi, Khadije Mirzaei, Using the Chaotic Map in Image Steganography, IEEE 2009 International Conference on Information Management and Engineering, Print ISBN: 978-0-7695-3595-1