Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 3 (2011) 89–95

Procedia Computer Science

www.elsevier.com/locate/procedia

WCIT 2010

An Effective chaos-based image watermarking scheme using fractal coding

MohammadReza Keyvanpour*[a], Farnoosh Merrikh-Bayat[b]

[a]Department of Computer Engineering, Alzahra University, Tehran, Iran
[b]Department of Computer Engineering, Islamic Azad Uviversity, Qazvin Branch, Qazvin, Iran

Abstract

The image watermarking technology is a technique of embedding hidden data in an original image. In this paper, a new watermarking method for embedding watermark bits based on Chaos-Fractal Coding is given. A chaotic signal is defined as being deterministic, pseudo periodic and presenting sensitivity to initial conditions. Combining a chaos system with Fractal Coding plays an important role in the security, invisibility and capacity of the proposed scheme. The main idea of the new proposed algorithm for coding is to determine a set of selective blocks for steady embedding. Simulation results show that the CFC algorithm (Chaos-Fractal Coding) has a confident capacity. The embedding technique that proposed in this paper is quite general, and can be applied to the extracting scheme with demanded changes.

Selection and/or peer-review under responsibility of the Guest Editor.

Keywords: Image Watermarking; Fractal Coding; Chaos Cryptography; Arnold's Cat Map; Capacity.

1. Introduction

Image watermarking is a branch of information hiding which is used to hide proprietary information in digital image. In some applications, the sensitive images related to politics or commerce, such as military maps, medical images or multi-resolution images, should be protected in order to avoid unauthorized users knowing it. A digital watermark is a visible, or preferably invisible, identification code that is permanently embedded in digital media, to prove owner authentication thereby providing a level of document protection [2]. In 1963, Chaos evolved from the work of Edward Lorenz, a meteorologist at Massachusetts Institute of Technology [19]. An overview of early chaotic watermarking techniques can be found in [6] [24]. The use of chaotic functions for the generation of watermarks has also been proposed by Voyatzis and Pitas [5]. In image processing the chaotic functions that used are two-dimensional, and are known as chaotic maps [4]. There are many such functions but the most famous for images is the Arnold's cat map that is used in this paper for encrypting images. In 1996, Puate and Jordan proposed the first fractal watermarking whose concept was rooted on playing two different search region to embed watermark bit (one

* Corresponding author. Tel.: +098-281-3665275; fax: +098-281-3665279.
E-mail address: Keyvanpour@Alzahra.ac.ir (M. Keyvanpour), F.mbayat@Qiau.ac.ir (F. M. Bayat).

.

doi:10.1016/j.procs.2010.12.016

or zero) [3]. In 2000, Li and Wang utilized the isometric property to embed the watermark bit by two isometric kind of plane. Since then, there were few papers to investigate the digital watermarking based on fractal coding [16]. One of the aims of this paper will be the presentation and investigation of the characteristics of this phenomenon, which we will call it CFC. Because of semantic relationship between FC and CFC, their combination can produce a useful method in image processing. The remaining of this paper is organized as follows, Section 2 reviews briefly the chaotic encryption on image, and in section 3 the Arnold's Cat Map (ACM) on image is described. Section 4, explores the Fractal image Coding. In section 5 Embedding Watermark by chaos-fractal coding is presented, Sections 6, and 7 examine the experimental results and conclusion respectively.

2. Chaotic Encryption

At the first time, "Chaos Theory" is presented by James Yorke and Tien-Yien Li, in 1975. "secure communications using synchronized chaos would probably have to be more sophisticated than simply adding your signal to chaos to hide it", these accomplishments represent the first steps in using chaos in encryption [6] [17]. Chaos systems are fit for image encryption, aviation, cryptology and automation fields [8]. A chaotic signal is defined as being deterministic, pseudo periodic and presenting sensitivity to initial conditions. This last property means that, if the generator system is initialized with a slightly different initial condition, the obtained signal diverges very quickly from the original one [7] [16]. Chaotic map is used for proposed algorithm to increase the security level that must have regarded in watermarking schemes. One of the most important chaotic functions is cyclic chaotic function that 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 [18]. If (p, q) are the initial coordinates of a pixel, the outcome coordinated of the chaotic function (p', q') are given by:

$$\begin{bmatrix} p' \\ q' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \lambda & \lambda+1 \end{bmatrix} \cdot \begin{bmatrix} p \\ q \end{bmatrix} mod\ N \qquad (1)$$

Where N denotes the width of the image and λ is an integer parameter that affects the period T of the chaotic function [4]. There are many chaotic maps likes: Logistic map, Tent map, Sine map, Cubic map, Arnold's cat map, Chen map, Barker map, Standard map, that each of them has their special properties for specific usage. In this paper, an ACM-based public algorithm is presented for select the embedding places in image watermarking.

3. Arnold's Cat Map

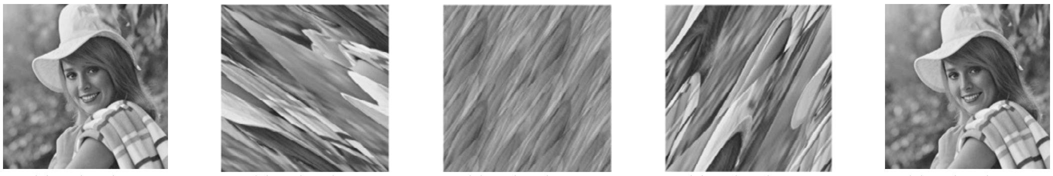
In the domain of the information security, the scrambling image is a very common way of image processing. The intention is that a regular image falls into confusion based on a reversible image transform. So the original content is concealed. The 2-dimensional Arnold transformation, usually called cat mapping is to transform one matrix into another. It can be viewed as a discrete chaotic system [1] [25]. The Arnold's Cat Map will be influenced by its initial conditions and it is also true that the outputs will appear to be random. If we let X=$\begin{bmatrix} p \\ q \end{bmatrix}$ be an N × N matrix of some image and, Arnold's Cat Map is the transformation (λ=1) [9] [19]:

$$\Gamma X \rightarrow A\ mod\ N \qquad (2)$$

Where p and q are positive integers, $\det(A) = 1$ and (p', q') is the new position of the original pixel position (p, q) when Arnold cat map is performed once. Iterated actions of A on a pixel $r_0 \in S$ from a dynamic system $(S \in \{n = 0,1,2, \dots , M\})$ [10]:

$$R_{n+1} = A^n r_0\ mod\ N \quad or \quad R_{n+1} = A r_n\ mod\ N \qquad (3)$$

Thus, the parameters p, q and the number of iterations M all can be used as the secret keys [4]. After several iterations, the correlation among the adjacent pixels can be disturbed completely. It means there are points in set S that are finally mapped onto them after a number of iterations. Because, these points are dense in set S, an element of complete regularity is introduce. The chaotic mapping of Arnold's cat map on Elaine image (512×512) is shown in Fig 1.



Elaine – iteration: 0 | Elaine – iteration: 1 | Elaine – iteration: 190 | Elaine – iteration: 383 | Elaine – iteration: 384

Fig 1. Process of Arnold's Cat Map on Elaine image

4. Fractal Image Coding

Recently, fractal block coding is investigated for watermarking. Based on the fractal codes, several watermarking techniques have been proposed [13] [26] [27]. For example in [15], search region is divided into two halves and the watermark is hided with regard to the best-pair domain block belongs to which half. The fractal-based schemes exploit the self-similarities that are inherent in many real-world images for the purpose of encoding an image as a collection of transformations. The explicit difference here is that the entire image is not self similar, but parts of the image are self-similar with properly transformed parts of it. This property cannot be change or omission unless that quality preservation for images not possible.

The critical step to model real world objects was the concept of Partitioned Iterated Function Systems (PIFS) proposed by Barnsley. The PIFS theory assumes that one small region of an image may be approximated by other self-similarity region in the same image by the use of the IFS simple transformation [3] [11]. In the first step, the original image is divided into non-overlapped R_i (Range) blocks, that cover all image, and overlapped D_i (Domain) blocks. The size of D_i blocks is larger than size of R_i blocks. Key issues in fractal coding are: How to form the range blocks and the domain blocks? Also, How to search the perfect domain block match for the range block? [12] [20] - [22].

The main idea of a fractal based image coder is to determine a set of contractive transformation to approximate each block of the image, with a larger block. Simple looking at contractive transformation tells us how we can expect a collection of transformations to define an image: Let's consider the metric space (ε, d) where d and ε are the given metric and the space of the digital images, respectively. It is a contractive transformation like provided that [23]:

$$d(\beta(x), \beta(y)) \leq s d(x, y), \qquad x, y \in \varepsilon, 0 \leq s \tag{4}$$

In this case, exists a point x^* such that:

$$\beta(x^*) = x^* \qquad \lim_{n \to \infty} \beta^n(x) = x^*, \qquad \forall x \tag{5}$$

This point is called a fixed point [13] [22]. In reality, only 10-20 iterations are needed for the suitable estimation to visibly converge within a reasonably small error tolerance [14].

After contraction of D_i blocks the most similar block is searched for each R_i block by using of metrics which describes distance between D_i and R_i blocks. For reconstruction of R_i blocks from the most similar D_i blocks, it is possible to use the following transformation:

$$R_i = s \cdot D_i + o \tag{6}$$

Where s is the offset of greyscale intensity and o is the brightness coefficient [12]. The proposed algorithm will use fractal image coding for select the suitable embedded places. These places are displayed by vectors that their started points are significant for proposed scheme.

5. Proposed Algorithm

The embedded algorithm of watermarking is as follows (The watermark embedding process is depicted in Fig. 2):

Step 1: Select the special image for embedding watermark and specified its size as the certain parameter in chaotic process.
Step 2: Use Arnold's cat map equation to encrypt the original image.
Step 3: The period T of the chaotic function (2) for the image is calculated (depend to image size).
Step 4: The Arnold's cat map is applied $\left[\frac{T}{2}\right]$ times to the host image for creating the chaotic image with best distribution.
Step 5: The initial space which is used for searching is calculated by using the specified key.
Step 6: Selecting embedding fractal blocks in the chaotic image which is obtained in previous step.
Step 7: The final watermarked image is generated by embedding watermark bits in selected pixels.

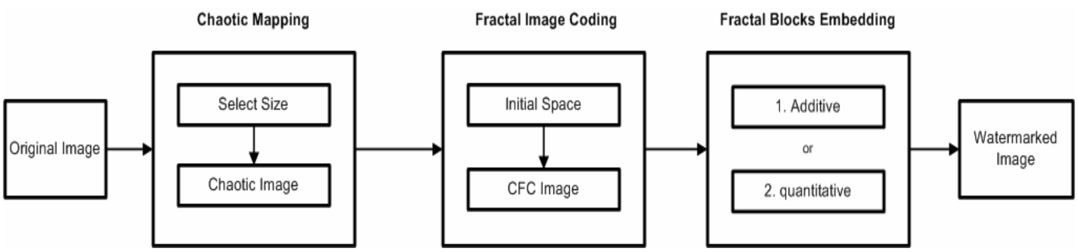


Fig 2. The watermark embedding process

6. Experimental Result

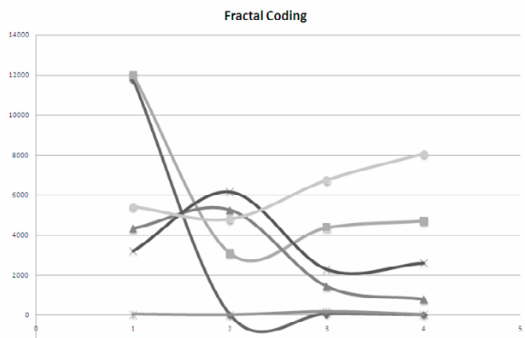
In order to test this algorithm, a watermark embedding is made of Lena, Baboon, Boats, Camera, Egg and Nilebend images size of 512×512. In order to compare the performance of the specified watermark embedding method, used images were studied about the amount of capacity. General comparison and obtained results are presented in Fig .3 (a,b). Embedding places that are produced by this method have good distribution, this property has important role in efficient robustness and high capacity. Table .1 (c) shows the average and Deviation number of bits (capacity) that retrieved after chaotic encryption and fractal coding. As it can be seen in the Fig .3 (a), the confident capacity of the CFC method is very high. The main advantage of using CFC in image processing, especially in image watermarking, is that it is adapted with the human visual system as shown in the Fig 5. For better demonstration of the achieved qualitative improvement, the comparative experiment by using CF method is performed which the results are presented in Fig 4.

7. Conclusions

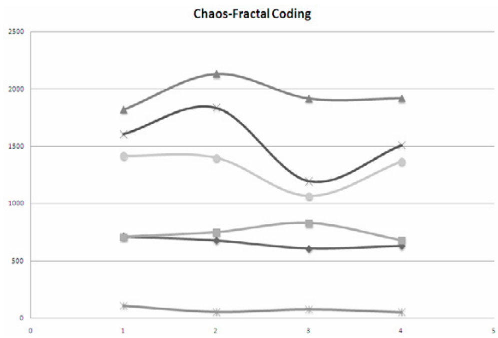
This paper presented a new technique based on the chaotic Arnold's cat map by use of a fractal coding method to denote the best embedding places for image watermarking schemes. The experiment results demonstrated that the proposed chaotic algorithm yields the acceptable visual quality. We concluded that Chaos-Fractal Coding (CFC) method has more uniform capacity distribution than Fractal Coding (FC). The security of watermarking is highly improved by using chaos encryption, especially against intentional attacks, because this concept can be use for design of public keys. We believe the CFC method can be applied to similar applications in the field of image processing, where the secure selection of pixels is needed. Thus, it can be considered as an effective tool for image authentication.

Table 1. Comparative results: capacity & their deviations

	Tst1	Tst2	Tst3	Tst4	Tst5	Tst6
FC Capacity	11754	1	51	2	4424	945
FC Deviation	4798.55	0.41	20.82	0.82	1806.09	385.79
CFC Capacity	717	682	610	634	563	550
CF Deviation	292.71	278.43	249.03	258.83	229.84	224.54

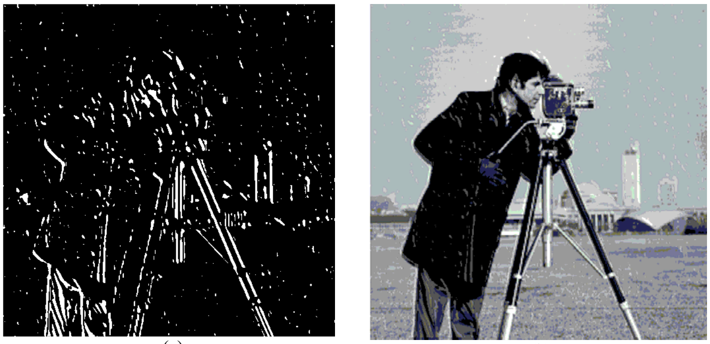


(a)



(b)

Fig 3. (a) Embedding blocks capacity in Fractal coding method, (b) Embedding blocks capacity in Chaos-Fractal Coding method



(a) (b)

Fig 4. (a) Embedding places by FC method, (b) Watermarked image after additive embedding (10X magnification).

a)

b)

Fig 5. (a) Embedding places by CFC method, (b) Watermarked image after additive embedding (10X magnification).

References

1. T. Sun, X. Shao, X. Y. Wang, A Novel Binary Image Digital Watermarking Algorithm Based on Dwt and Chaotic Encryption, The 9th IEEE International Conference for Young Computer Scientists, 2008.
2. A. Mooney, J. G. Keating, Generation and Detection of Watermarks Derived from Chaotic Functions, Perseus Books Publishing, 2000.
3. J. Paute, F. Jordan, Using Fractal Compression Scheme to Embed a Digital Signature into an Image, Proc. Spie Photonics East Symposium, Boston, USA, (1996) pp. 18-22.
4. E. Chrysochos, V. Fotopoulos, A. N. Skodras, Robust Watermarking of Digital Images Based on Chaotic Mapping and DCT, IEEE International Conference: Applied Electronics 2008, Pilsen, Czech Republic, 2008.
5. G. Voyatzis, I. Pitas, Application of Toral Automorphisms in Image Watermarking, IEEE International Conf on Image Processing, Lausanne, Switzerland, (1996) Vol. 2 237-240.
6. W. Ditto, T. Munakata, Principles and Applications of Chaotic Systems, Emerging Technologies Ai, Communication of The ACM, (1995) Vol. 38, No. 11.

7. K. T. Alligood, T. D. Sauer, A. Yorke, An Introduction to Dynamical Systems, Springer, New York, 1996.
8. P. Bas, J.M. Chassery, F. Davoine, Using the Fractal Code to Watermark Images, In Proc ICIP'98, (1998) Vol. 1, pp. 469–473.
9. S. Steven. H, Nonlinear Dynamics and Chaos, Cambridge, Ma, Perseus Books Publishing, 1994.
10. I.A. Ismail, M. Amin, H. Diab, An Efficient Image Encryption Scheme Based on Chaotic Logistic Maps, International Journal of Soft Compution (2007) Vol. 2 285-29.
11. Y. Fiisher, Fractal Image Compression: Theory and Application, Springer, Verlage, (1994) No. 0-387-94211-4.
12. M. Candik, D. Levicky, Z. Klenovicova, Fractal Image Coding with Digital Watermarks, Radioengieering, (2000) Vol. 9, No. 4.
13. M. H. Pi, C. Hung Li, H. Li, A Novel Fractal Image Watermarking, IEEE Transactions On Multimedia, (2006) Vol. 8, No. 3.
14. Q. J. He, Iterated Functions Systems and Fractal Coding, Math 308 Essay, 1999.
15. F. Hartung, J. k. Su, B. Girod, Spread Spectrum Watermarking Malicious Attacks and Counterattacks, Spie – Security and Watermarking of Multimedia Contents, (1999) pp. 58-147.
16. P. Davern , M. Scott, Fractal Based Image Steganography, Information Hiding: First International Workshop, No. 1174, pp. 279– 294, Springer Lecture Notes, U.K, 1996.
17. A. Mooney, J. G. Keating, I. Pitas, A Comparative Study of Chaotic and White Soise Signals in Digital Watermarking, Chaos Solition and Fractal 35,(2008) pp. 913-921.
18. Z. Dinghui, G. Qiuje, P. Yonghua, Z. Xinghua, Discrete Chaotic Encryption and Decryption of Digital Images, IEEE International Conference on Computer Science and Software Engineering, 2008.
19. Z. Peng, W. Liu, Color Image Authentication Based on Spatiotemporal Chaos and SVD, IEEE International Conference on Computer Science and Software Engineering, 2008.
20. G. Peterson, Arnol's Cat Map Survey, Math 45-Linear Algebra, 1997.
21. P.S. Lio, C.C. Chen, J. S. Pan, Robust Fractal Watermarking On Continue-Tone Image, 18th Ippr Conference on Computer Vision, Graphics and Image Processing-CVGIP, 2005.
22. N.A. Koli, M. S Ali, A Survey on Fractal Image Compression Key Issue, Information Technology Journal, (2008) pp. 1085-1095.
23. Z. Yao, Fixed Point in Fractal Image Compression as Watermarking, ICIP IEEE, 2003.
24. S. Vasyura, Y. A. Zolotavkin, Detection of Hidden Content Images Compressioned by Fractal Algorithm, Information Technology and Computer Engineering, (2008) No. 3.
25. N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, A. Tefas, V. Solachidis, I. Pitas, Applications of Chaotic Signal Processing Techniques to Multimedia Watermarking, In Proceeding of the IEEE Workshop on Nonlinear Dynamics in Electronic Systems, Cantania Italy, (2000) pp. 1-7.
26. S. Katzenbeisser, F.A.P. Petitcolas, Information Hidding Techniques for Steganography and Digital Watermarking, Boston: Artech House, 2000.
27. C.H. Li, S.S. Wang, Digital Watermarking Using Fractal Imag Coding, Ieice Trans. Fund,(2006) Vol. E83-A, No. 6, pp. 1286–1288.