A NOVEL APPROACH TO GENERATE FRACTAL IMAGES USING CHAOS THEORY

K. Thamizhchelvy
Research Scholar, Department of Computer Applications, Faculty of Computing
Sathyabama University, Chennai, India
thamizhchelvy@gmail.com

G.Geetha
Professor and Head, Division of Research and Development
Lovely Professional University, Phagwara, India
gitaskumar@yahoo.com

Abstract

We propose the fractal generation method to generate the different types of fractals using chaos theory. The fractals are generated by Iterated Function System (IFS) technique. The chaos theory is an unpredictable behavior arises in the dynamical system. Chaos in turns explains the nonlinearity and randomness. Chaotic behavior depends upon the initial condition called as "seed" or "key". Pseudo Random Number Generator (PRNG) fixes the initial condition from the difference equations. The system uses the PRNG value and it generates the fractals, also it is hard to break. We apply the rules to generate the fractals. The different types of fractals are generated for the same data, because of the great sensitivity to the initial condition. It can be used as a digital signature in online applications such as e-Banking and online shopping.

Keywords*:* Fractals Iterated Function System (IFS), Pseudo Random Number Generator (PRNG), Chaos.

1. Introduction

1.1. Fractals

The geometric shapes of the fractals are very complex and it is infinitely detailed. The smaller sections of them are recursively defined and it is similar to large ones. In **Fig.1.**the function of the fractals is f(x) is to consider x, f(x),f(f(x)),f(f(f(x))), etc. The definite properties of the complex systems of the fractals are closely related to Chaos. Fractals are self-similar sets and it is independent of scale. A fractal is a geometric shape or natural objects that have some of the characteristics:

- Self-similarity
- Irregular shapes
- Distinct element
- Iterated functions
- Fractional dimension.

The following are some of the examples of fractals namely the Sierpinski Triangle, The Von Koch Curve, Koch Edge and Koch and complex fractal images.

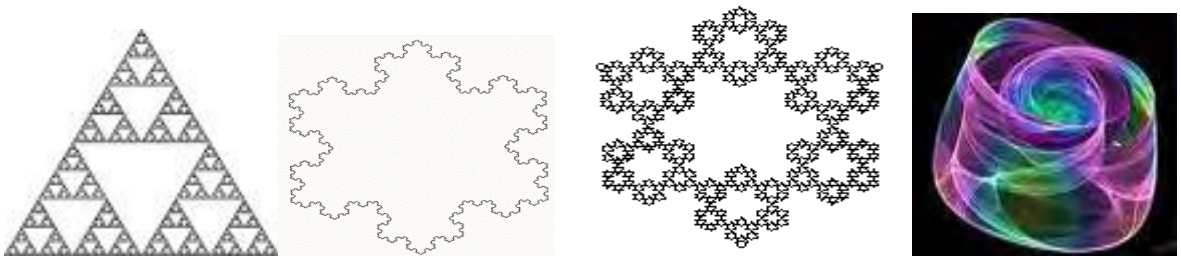


Fig. 1. Examples of Simple and Complex Fractal Images

In this paper we propose a novel approach to generate the fractal using chaos. The paper is organized as follows - Section 2 deals with literature survey, Section 3 deals with data hiding technique by chaos theory, in Section 4, Digital Signature and the basic uses of Message authentication Image are given, in Section 5, the novelty of the fractal generation method and few experimental results are proposed and analyzed, in Section 6, we bring out conclusion and future work.

2. Literature Survey

Many researchers found that there is the tight relationship between chaos and cryptography, based on this idea we introduce chaos in steganography to conceal the data in fractal images. The fractal images can be used as a digital signature for online credit card payment system. We discusses about the novelty of the credit card payment system using fractals and chaos theory.

[El-Khamy, S.E. Khedr *et al*. (2008)] proposed a new steganography technique for hiding images. It adopts both fractal and wavelet image processing techniques. The idea of the presented scheme was to hide the fractal codebook of a to-be-hidden image in the wavelet domain of a host or hiding image.

[Zolotavkin, Y. Lukichov *et al*.(2008)] suggested the criterion for detecting hidden data in the fractal code of images. The approach for estimating steganographic threats of every record in the fractal code was used. The estimation was based on the special features of fractal compression.

[Thiyagarajan and G.Geetha (2007)] developed a chaotic cryptographic algorithm backed by stochastic approach to matrices, nonlinearity and randomness.

[G.Geetha(2007)] showed that non-linearity plays a vital role in cryptographic algorithms by appealing to chaos and quantum chaos.

[G.Geetha and Suresh kumar.M (2008)] developed an Asymmetric key cipher using fractal dimension and Lyapunov Exponents.

[Chin-Chen Chang *et al.* (2005)] proposed an approach for hiding a secret image in a cover image and used fractal image compression method to compress the secret image, encrypt this compressed data by DES.

[Hsien-Chu Wu and Chin-Chen Chang (2003)], suggested a fractal-based watermarking scheme that efficiently protects the intellectual property rights of digital images. The main feature of fractal encoding is that it uses the self-similarity between the larger and smaller parts of an image to compress the image.

[Hannes Hartenstein *et al*. (2000)] presented a fractal coder that derives highly image-adaptive partitions and corresponding fractal codes in a time-efficient manner using a region merging approach.

[Thamizhchelvy.K and G.Geetha (2012)] proposed a Message Authentication Image (MAI) algorithm to protect against e-banking fraud and the latest e-banking fraud techniques, such as Phishing, Trojans and man-in-the-middle attacks. This MAI Algorithm provides confidentiality, authentication and digital signature. It uses both Cryptographic and Steganographic ideas to conceal the data in the image. MAI generates fractals and embeds the password using chaos technique.

[Fisher . Y (1995)] presents the theory and implementation of new methods of image compression based on self-transformations of an image. These transformations lead to a fractal structure as well as being very similar to some methods of generating fractals.

3. Data Hiding Technique by Chaos Theory

Chaos is an unpredictable behavior arises in a deterministic system so that future behavior is eventually unpredictable. Chaos arises in the dynamical system the great sensitivity to the initial condition it is hard to break.

3.1. Non Linear Dynamical System

Any system that does not satisfy the principle of superposition or homogeneity can be called nonlinear dynamical system.

Chaos can be viewed as a non-linear dynamical system coupled with randomness. Randomness can be introduced through the choice of random variables. These random variables can take discrete or continuous values with discrete or continuous observations.

A sequence{X(t)} of random variables which are functions of time having discrete or continuous parameter space taking discrete or continuous values is defined as a stochastic process. A function f(x) taking positive values for all x, with definite integral over the real line is 1, can be taken as the probability density function of a random variable X.

A random variable being a measurable function defined on Borel field of subsets of the sample space. The non-linearity is introduced through difference equation or difference differential equation.

3.2. Initial Condition – (PRNG)

The Pseudo Random Number Generator (PRNG) is a deterministic procedure that generates a random seed and set as initial condition. The initial condition determines the chaotic behavior of the system, based on the initial condition the system generates different types of fractals. The fractals can be used as a digital signature in any online transactions for the credit card payment system.

4. Digital Signature

A digital signature explains the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

4.1. The basic uses of Message Authentication Image

The Fractal image is used as a message authentication image to verify the digital signature. In Fig.2.the generated fractal is attached with the original message and it is encrypted by using the sender's private key and it sent to the receiver as a digitally signed documents. The received digitally signed document is verified by decrypting with the receiver's public key, and then compares the fractal images to prove the digital signature.

The system shows that the message is received from the authenticated person, the message is not altered by anyone and the sender cannot deny that the message was not sent by me, it means that the digital signature is achieved in the system. The Image generation algorithm proves that they are original.

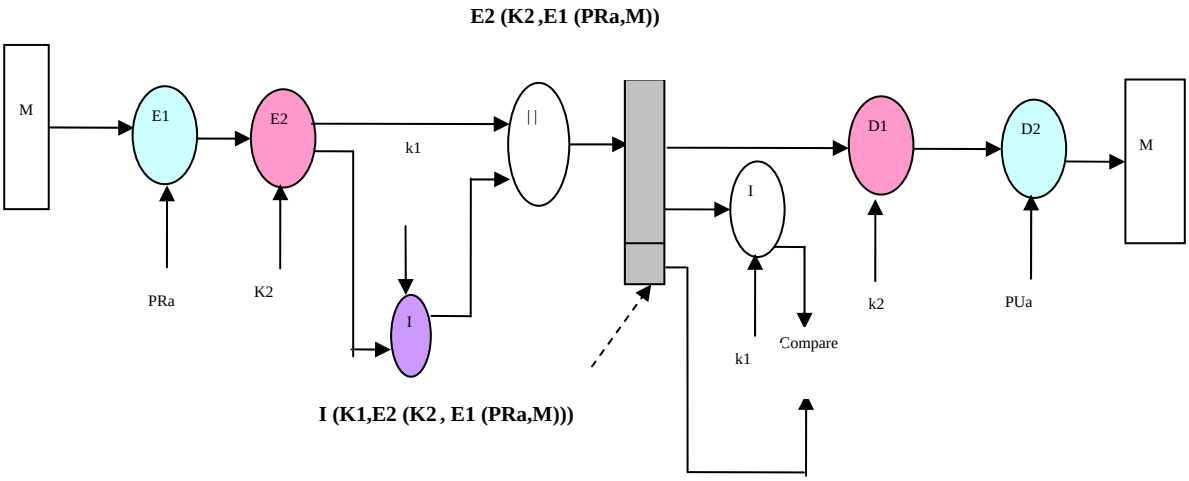


Fig.2. Message Authentication, Confidentiality and Digital Signature

5. Experimental Results

In **Table 1** and **Table 2** shows that the generated fractal sets with different segments and stages. The novelty of the fractal generation is also analyzed and the values are listed in **Table 3.** The chaotic behavior of the system is shown in **Fig.3.**

5.1. Table Description

- The different types of fractals are created for the same and different credit card numbers and the results of the various fractal images are listed in **Table 3.**
- It produces the different shapes of fractals for the same credit card number.
- ***Example***: The credit card number (327611110000301) is same but the Pseudo Random Number Generates the key = 11 and it fixes that as an initial value and generate the original fractal image.
- The steganalyst tries to access the same credit card number (327611110000301) and fixes wrongly as the initial condition as 7. It produces different fractal image (Duplicate Image).
- When the images are compared and validated then it proves that they are original then digital signature is achieved otherwise they are not original.

5.2. Fractal Set

Table 1. The Stages and Segments for Fractal Set (F1 & F2)

SI.No.	Fractals	Stages	Segments
1	F1	5	2 8 32 128 512
2	F2	5	1 4 16 64 256

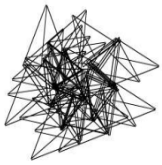
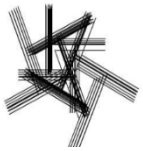
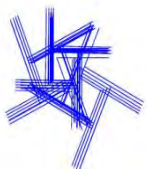
Table 2. The Stages and Segments for Fractal Set (F3 & F4)

SI.No.	Fractals	Stages	Segments
1	F3	7	3 6 12 24 48 96 192
2	F4	6	4 8 16 32 64 128

5.3. The Novelty of Fractal Images

The following Table 3 shows that how the fractal images are created for the set of credit card numbers.

Table 3. Different Shapes of Fractals and its Novelty

SI. NO.	Credit Card Numbers	Generated Fractals	PRNG	No of Segments	Novelty
1	327611110000301 (Same credit card number)		Initial value = 11	512	Original Image
			Initial Value = 7	256	Duplicate Image
2	423466935431111 (Same credit card number)		Initial value=18	192	Original Image
			Initial value=29	128	Duplicate Image

5.4. Chart - Analysis of Fractals

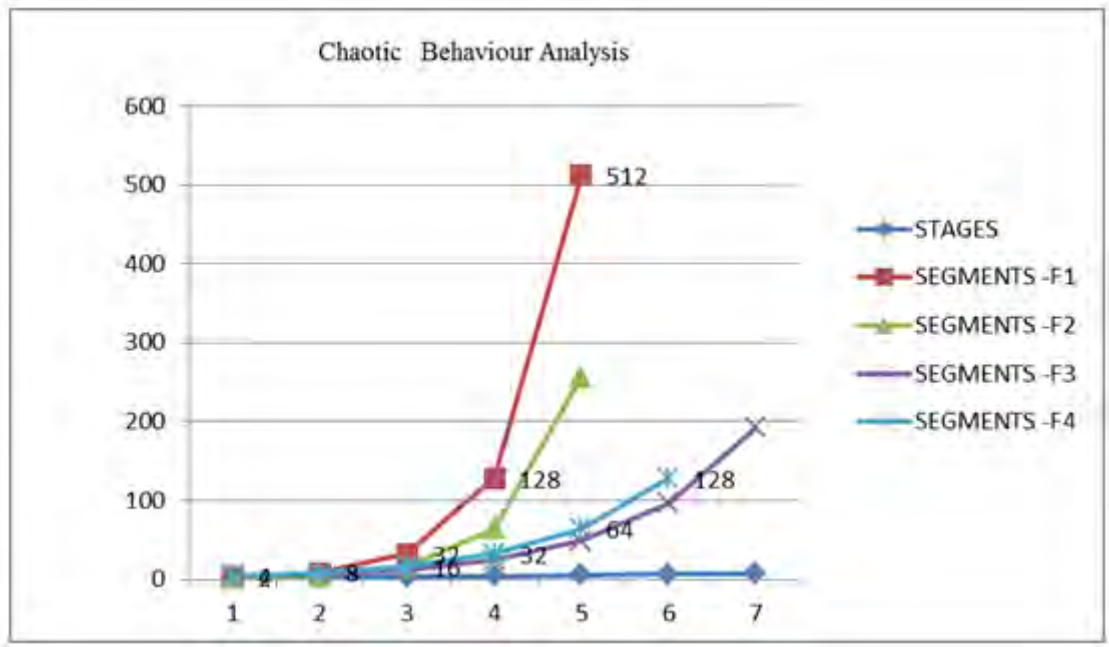


Fig.3.The analysis of various Fractal Set

6. Conclusion

We proposed the fractal generation method to generate the different types of fractals using chaos theory. Chaos in turns explains the nonlinearity and randomness. Chaos is based upon the initial condition that is generated by PRNG. We applied the rules to generate the fractal and also we proposed the novelty of credit card numbers using fractal and chaos theory, it proves the digital signature. It can be used in applications such as e-Banking and online shopping etc. We plan to implement these applications as our future work.

References

[1] Chin-Chen Chang (2005) et al., A DCT-domain system for hiding fractal compressed images, In the Proceeding of Advanced Information Networking and Applications, AINA, ISBN: 0-7695-2249-1, pp 83-86, volume 2.

[2] El-Khamy, S.E. Khedr, M. AlKabbany (2008). A hybrid fractal-wavelet data hiding technique, National Radio Science Conference, NRSC ISBN: 978-977-5031-95-2 pp 1-9.

[3] Fisher, Y., (1995) Fractal Image Compression:Theory and Application. Springer-Verlag. NewYork, USA. ISBN: 0-387-94211-4, pp: 341.

[4] Geetha .G (2007), Non-linearity in Ciphers, In the Proceeding of TISC.

[5] Geetha G, Suresh Kumar M (2008). Asymmetric key cipher based on Nonlinear dynamics, In the Proceeding of ICETET, First International Conference on Emerging Trends in Engineering and Technology, pp 1250-1254.

[6] Hannes Hartenstein et al (2000). Region-based fractal image compression, In the Proceeding of Image Processing, ISSN: 1057-7149,PP 1171-1184.

[7] Hsien-Chu Wu, Chin-Chen Chang (2003). Hiding digital watermarks using fractal compression technique, Journal of Fundamenta Informaticae **,** Volume 58 Issue 2, Pages: 189 – 202.

[8] Thamizhchelvy.K ,G.Geetha (2012). E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm, Turing100-International Conference on Computing Sciences, 14-15, IEEE.

[9] Thiyagarajan.M, Geetha.G (2007), Complex facets of Cryptography, In the Proceeding of International conference on Systemics, Cybernetics and Informatics, ICSC, pp 555 – 559.

[10] Zolotavkin, Y. Lukichov et al. (2008), A novel approach to the security of data hidden in multimedia objects, in the proceeding of International Carnahan Conference on Security Technology, ICCST, ISBN: 978-1-4244-1816-9, pp 23-28.