Journal of Computer Science

Original Research Paper

An Efficient Image Generation Algorithm Using Fractals and Chaos Theory

[1]Thamizhchelvy, K. and [2]G. Geetha

[1]*Faculty of Computing, Sathyabama University, Chennai, India*
[2]*Division of Research and Development, Lovely Professional University, Phagwara, India*

Article history
Received: 07-07-2014
Revised: 14-07-2014
Accepted: 27-08-2014

Corresponding Author:
Thamizhchelvy, K.
Faculty of Computing,
Sathyabama University, Chennai, India
Email: thamizhchelvy@gmail.com

Abstract: An Efficient Image Generation Algorithm is proposed. It generates Message Authentication Image (MAI) by using Fractals and chaos theory. The fractal images are generated by using Iterated Function System (IFS) techniques. We implemented and generated the fractal images exploring the properties of chaos. Chaos is an unpredictable behavior arises in a dynamical system so that the future behavior is not in a predictable way. Chaos is based on the initial condition that is generated by Pseudo Random Number Generator (PRNG). The chaotic behavior of the system is also analyzed. We use these Fractal images as a digital signature. This technique can be employed in online transactions like Banking, Shopping. to avoid phishing and also we can watermark this fractal image and use it for government and private identification proofs.

Keywords: Fractals, Iterated Function System (IFS), Message Authentication Image (MAI), Pseudo Random Number Generator (PRNG)

Introduction

Fractals

The geometric shapes of the fractals are very complex and it is infinitely detailed. The small sections of them are recursively defined and it is similar to large ones. The Function of the fractals is $f(x)$ is to consider x, $f(x)$, $(f(x))$, $f(f(f(x)))$. The definite properties of the complex systems of the fractals are closely related to Chaos.

Image Encoding Using Fractals

In nature everywhere the fractals are seen. The fractals have the elements of chaos and it is first imagined by Julia and Mandelbrot, but the essence is based in mathematics. This is not only the way to represents the fractals. Using Iterated Function System (IFS) technique the Sierpinski gasket is drawn. W. Sierpinski thought the fractal originally.

It is originally from the normal triangle, choose any vertices from the triangle and start from the middle to draw the triangle, repeat this process infinitely for number of iterations.

Figure 1 shows the simple and complex fractal images like koch snowflake, sierpinski triangle.

In this study we propose a new Image Generation Algorithm using chaos. The paper is organized as follows-section 2 deals with literature survey on fractals, section 3 explains the techniques of Chaos, Deterministic System and Pseudo Random Number Generator (PRNG), Lucas series and difference equations, in section 4, Image generation algorithm is proposed, in section 5, Chaotic Stegosystem with some experimental results, tables and Chaotic chart analysis are given and in section 6 we bring out the conclusion and future work.

Literature Survey

There is considerable amount of work done in fractal and chaos theory.

Bilal *et al*. (2013) proposed an algorithm hides the payload based on certain relationship between the cover image, chaotic sequence and the payload, instead of directly embedding payload into the cover image which often leaves telltale signs of steganography.

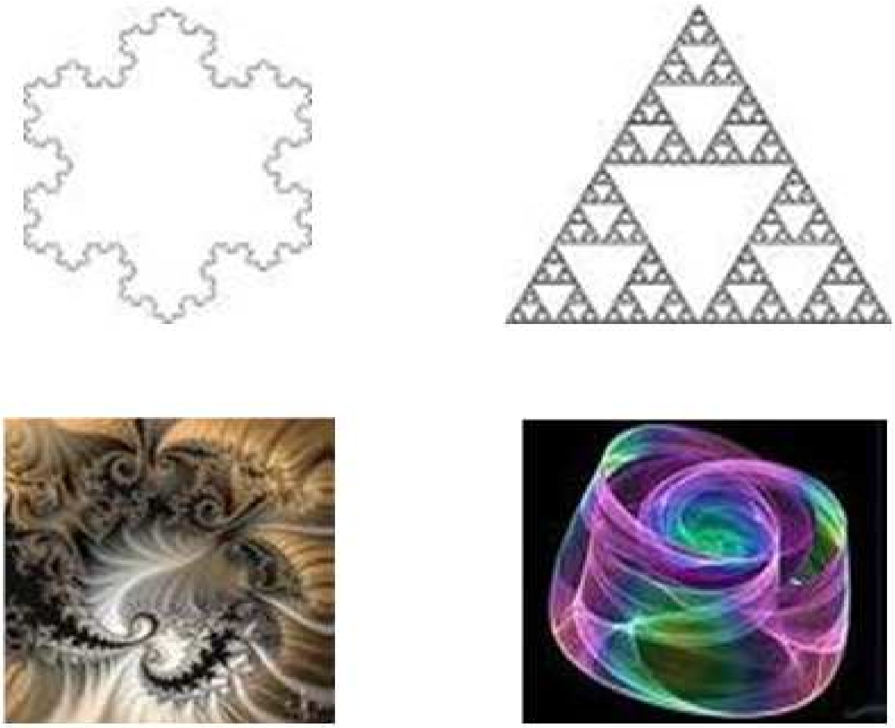


Fig. 1. Simple and complex fractal images

Tayel *et al*. (2012) proposed an algorithm based on coordinate the data in the image dimensions using chaos distribution arrangement. The data is embedded with the original image in the pixels least significant bits, so can't appears within the image. When the image received the embedded data is separated and rearranged using the initial condition of the chaos coordination.

Wu and Noonan (2012) proposed an algorithm uses a fractal image as the cover image, takes a random-like sequence generated by a chaotic map as the reference for embedded positions and employs a wavelet transform to realize the embedding procedure.

Thamizhchelvy and 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.

Kiani *et al*. (2011) discussed a new approach for embedding the authentication data using fractal and chaos technique is developed in this study. This approach is to meet the need for authentication, including fragility and inalterability. Using chaos technique and the keyword extracted from the image itself, it is so unlikely to predict the blocks used for embedding the data.

El-Khamy *et al*. (2000) proposed a new steganography technique for hiding images. It adopts both fractal and wavelet image processing techniques. The idea of the presented scheme is to hide the fractal codebook of a to be-hidden image in the wavelet domain of a host or hiding image. The presented technique had been tested and proved its robustness against additive white Gaussian noise AWGN.

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

Zhirabok and Shumsky (2012) studied the problem of synthesis of the regulator which stabilizes equilibrium of the deterministic system and provides required scattering of random states near this equilibrium for the corresponding stochastic system.

Bashkirtseva and Ryashko (2013) discuss the Attainability analysis in the problem of stochastic equilibria synthesis for nonlinear discrete systems.

Agaian and Susmilch (2006) proposed a fractal based approach for hiding sensitive information in a cover image including artificially generated fractal images). The fractal parameters of the image are altered by the steganographic data while the image is generated. This results in an image that is generated with the data already hidden in it and not added after the fact. They showed that the input parameters of the algorithm, such as the type of fractal and number of iterations, will serve as a simple encryption key for the hidden information. They also explain how the capacity of the image is affected by the variation of the parameters. Finally, they demonstrate that the proposed algorithms are immune to the commonly used steganographic detection algorithms.

Wu and Chang (2003) proposed 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. When their scheme uses this self-similar relationship, it affects both the embedding and extraction of the watermark. As seen from the experimental results, the proposed scheme provides more robust capability than other compression-based watermarking techniques.

Shannon (1949) paper" Communication theory of secrecy systems", he mentioned that the idea of using chaos in cryptography and this transformation are used in secrecy system. Some more researches also pointed out that there is the tight relationship between chaos and cryptography. The future behavior of chaos is unpredictable, if two close starting points diverge exponentially and it is arises in the dynamical system, based on this idea, (Geetha and Suresh, 2008) introduced chaos in cryptography as follows. The embedded morkov chain explains the stochastic matrix. With the help of this the sequence of Fibonacci is generated. In turn the Fibonacci sequence explains a non-linear system. Thus the Fibonacci sequence with the Morkov chain is a chaos. This could be embedded in fractal, based on this idea, we introduced chaos in steganography. It explains the generation of Message Authentication Image (MAI) using chaos theory and Iterated Function System (IFS) technique. We can use this image as digital signature.

Chaos

Chaos theory explains the behavior of dynamical systems that are very sensitive to initial conditions-popularly known example is butterfly effect. The small differences in initial conditions (rounding errors in numerical computation) may yield widely diverging outcomes for such dynamical systems, long-term prediction is practically impossible. It happens even though these systems are deterministic, their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, it is very difficult to predict the deterministic nature of these systems. This type of behavior is known as deterministic chaos, or simply chaos.

Deterministic System

The chaos theory is deterministic system. If the initial state of the systems are known in advance then the future state of the system could predicted theoretically. The precision limits the future state and initial state can be measured, chaotic systems are examined by the strong dependence on the initial conditions.

Pseudorandom Number Generator (PRNG)

The evolution of the Pseudo Random Generator (PRNG) is deliberately made hard to predict even though it is a deterministic algorithm. The numerical sequences are produced by PRNG using deterministic algorithm. The statistical pattern tests are passed by the pseudorandom sequences for randomness. By make use of this algorithm, conditions are used to initialize it, called the "seed", the output can be predicted. Because the sequence of the numbers which is generated by the PRNG is predictable. But the Hardware random number generators produce the sequences of numbers are no in a predictable way and it provide the greatest security for date encryption. It is completely deterministic system. In higher levels, a seed state of a PRNG sometimes called as a "key" and it is used as arguments to a method of an algorithm to produce the random numbers. The deterministic part is the "key". If you run the algorithm with the same "key" it will produce the same random result but this is not truly random.

Lucas Series

Lucas numbers are expressed as a similar sequence (2, 1, 3, 4, 7, 11, 18, 29…) and the values are listed in Table 1. These sequences are notated L_n ($n = 1, 2,\ldots.$) to represent the first letters of the last names Lucas. Eventually, it was established that both sequences can be analytically extended on complex Z-planes and that they satisfy the same three-term recurrence relation, reflecting that the Lucas numbers are the sums of two neighboring terms.

Table 1. Lucas number sequence

n	0	1	2	3	4	5	6	7	8	…
L_n	2	1	3	4	7	11	18	29	47	

Definitions of the Lucas Numbers:

For ay complex *v*, Lucas numbers L_v are defined by the formulas:

$$L_v = \phi^v + \phi^{-v} cos(\pi v)$$

where, ϕ is the golden ratio. $\phi = \left(1+\sqrt{5}\right)/2$

The best-known properties and formula for the Lucas numbers simple values at zero and infinity

The Lucas numbers L_v has the following values at zero and infinity:

$$L_{v,}L_0 = 2, L_\infty = \infty$$

For the cases of integer arguments *n*/; 0≤*n*≤25, the values of the Lucas numbers L_m can be described by the following table.

Non Linear Dynamical System

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

Difference Equation

The differences involving in an equation are difference equation. The following are the three different views as sequence of number, discrete dynamical system and Iterated function.

Using a rule, a sequence of number is generated recursively and to relate to each number in a sequence to the previous numbers in the sequence.

Discrete dynamical system is a difference equation that takes some input signal and produce output signal.

Iterated map is also the difference equation.

Y(k+1) = f(y(k)),the sequence as iterated functions given below

Example:

y(k+1) = f(y(k)) = y(k)2
y = 0.5, the orbit {0.5, 0.25. 0.625…}
y = 1, the orbit {1, 1, 1……}
y = 2, the orbit {2, 4, 16, 256…..}

We noted that knowing the rule only is not enough to know the behavior of the sequence. The Initial value is also important. We can generate the whole sequence recursively by knowing the rule and initial value.

The integer value of the k and the rule to generate the sequence is called difference equation or the dynamical system or iterated function.

Image Generation Algorithm

Algorithmic Steps:

- The given data is converted into binary
- Difference equation is used for mapping
- Replacement is made by corresponding fractal constructed using the rules framed in an algorithm
- Pseudo Random Number Generator (PRNG) is used to identify the position into which the replacement is done
- Next iteration is done, if the same random number is generated by the PRNG
- Null is introduced, if the PRNG generates a value in the non-difference sequence
- This system is implemented using LUCAS (difference equation) and Generated fractal sets
- The difference equation explains the non-linear dynamic, it can be viewed as the same non linearity generated by the fractals

Algorithm Description

Image Generation Algorithm generates a fractal image with the given data. The following are the process to be carried out in an algorithm:

- The given data is converted into binary. Based on the given binary the Image generation algorithm generates the fractal
- The PRNG generates the sequence random number; we use the first value as the initial condition. Based upon the initial condition it starts to draw the representation for the given binary data according to the rules framed in an Image generation algorithm
- The number generated by the PRNG is hard to break. Based upon this idea we fix the initial condition as a seed. If the initial condition

changes the total behavior of the algorithm is changes and it fail to produce the Original fractal image, it may lead to chaos

- In Image generation algorithm we use the Lucas series (simple difference equation) for fixing the position and rules framed for the representation of fractal
- We use 0, 1 and Null bits. Rule 1 is used to represent the bit 1, Rule 2 is used to represent the bit 0 and Rule 3 is used to represent the bit null. Based on the given bit the algorithm generates the fractal Image
- The number generated by the Pseudo Random Number Generator (PRNG) must belongs to the Lucas series, if it belongs to the series (e.g., 2 1 3 4 7 11 18 29……..) it uses the bit 1 and 0, otherwise it use the bit null
- Finally the Image generation algorithm generated the resultant Fractal Image (MAI). We use it as digital signature

Algorithm

```
Input:  D is the given Data
        The Prediction rules {R1, R2 and R3}
        Rule: 1→ if bit is equal to 1, Draw R1 representation.
        Rule: 0→ if bit is equal to 0, Draw the R2 representation.
        Rule: Null → if bit is equal to Null, Draw the R3 representation.

Output: MAI is the Resultant fractal image.

Do Begin;
    Read (D); // Read the given data
    B = Binary (D); // Convert the given data into binary data.
    MAI = Generate fractal (B); // Generate the fractal Image with the given data and use it as digital signature.
    Watermark (MAI); //Apply the watermark technique to embed the resultant fractal image for any applications.

End;

  Function generate fractal (B)
  Val = Random Integer (); //Pseudo Random Number Generator (PRNG) generate the random number and fix the initial value as a Seed.
  If Val ϵ s-type {s1, s2, s3…..sn} then // 'Val' belongs to any type of series.
      Pos = Val; // Fix the position
        For Each bit 'b' ϵ B do
            Extract a bit 'b'
                Case based on bit 'b'
                    Case 1:
                        If bit 'b' is equal to 1 then
                            Draw Fractal (pos, R1); //Apply Rule1 using IFS Technique.
                        End If;
                    Case 0:
                        If bit 'b' is equal to 0 then
                            Draw Fractal (pos, R2); // Apply Rule2 using IFS Technique.
                        End If;
                    Case Null:
                        If bit 'b' is equal to null then
                            Draw Fractal (pos, R3); //Apply Rule 3 using IFS Technique.
                        End If;
                End case;
            End for;
        Return (Res-MAI);
    End If;
End Function;
```

Chaotic Stegosystem Results

Chaos is a complex type of behavior exhibited by non-linear systems. Chaos is introduced through difference equations and the corresponding Markov process with embedded Markov chain with infinite transition probability matrix. This concept is used in the development of a chaotic stegosystem.

Experimental Result 1

The Image generation Algorithm generates the resultant fractal image and it is shown in Fig. 2. It has 9 stages, 1023 segments and its corresponding length details are given.

Experimental Result 2

The Image generation Algorithm generates the resultant fractal image and it is shown in Fig. 3. It has 8 stages, 1022 segments and its corresponding length details are given.

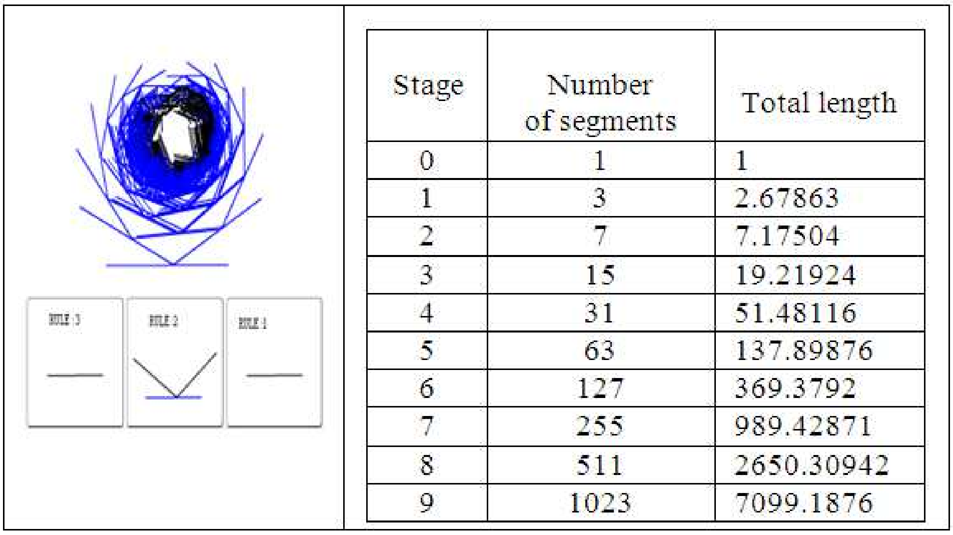
Experimental Result 3

The Image generation Algorithm generates the resultant fractal image and it is shown in Fig. 4. It has 6 stages, 1458 segments and its corresponding length details are given.

Table Description

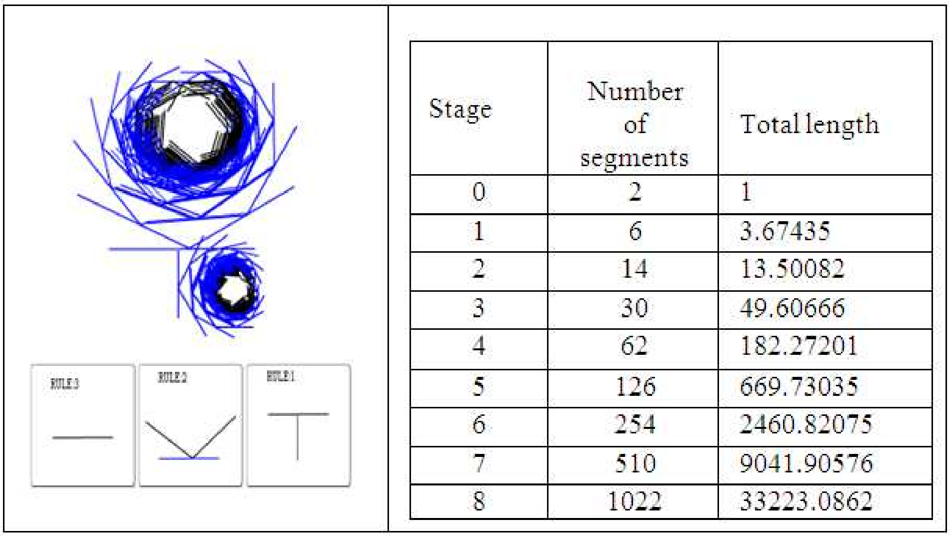
Table 2:

- The given data is 1982 and its corresponding binary value is 11110111110. The Image generation algorithm generate a fractal based on the given data
- First, the PRNG generates the sequence random number 4, 5, 6, 7, 8….521; we use the first value as the initial condition 4. Based upon the initial condition it starts to draw the representation for the given binary data according to the rules framed in an Image generation algorithm
- The image generation algorithm use the Lucas series ranges from (4 7 11 18 29 47 76 123 199 322 521) for fixing the position and rules to be followed for the representation of fractal
- We use 0, 1 and Null bits. Rule 1 is used to represent the bit 1, Rule 2 is used to represent the bit 0 and Rule 3 is used to represent the bit null. Based on the given bit the algorithm generates the fractal image
- Finally the Image generation algorithm generated the resultant Fractal Image. We use this Fractal image as a digital signature



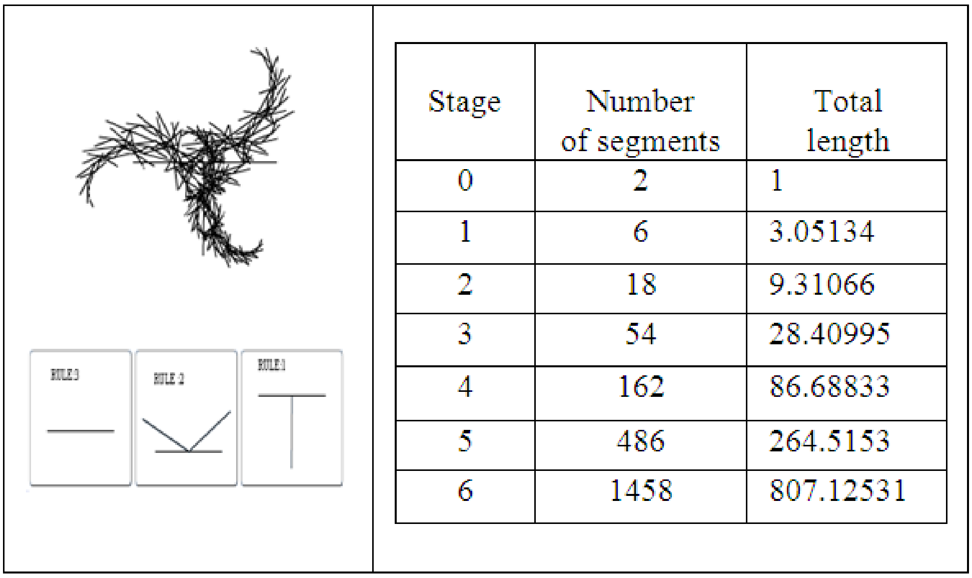
Stage	Number of segments	Total length
0	1	1
1	3	2.67863
2	7	7.17504
3	15	19.21924
4	31	51.48116
5	63	137.89876
6	127	369.3792
7	255	989.42871
8	511	2650.30942
9	1023	7099.1876

Fig. 2. Fractal image with 1023 segments



Stage	Number of segments	Total length
0	2	1
1	6	3.67435
2	14	13.50082
3	30	49.60666
4	62	182.27201
5	126	669.73035
6	254	2460.82075
7	510	9041.90576
8	1022	33223.0862

Fig. 3. Fractal image with 1022 segments



Stage	Number of segments	Total length
0	2	1
1	6	3.05134
2	18	9.31066
3	54	28.40995
4	162	86.68833
5	486	264.5153
6	1458	807.12531

Fig. 4. Fractal image with 1458 segments

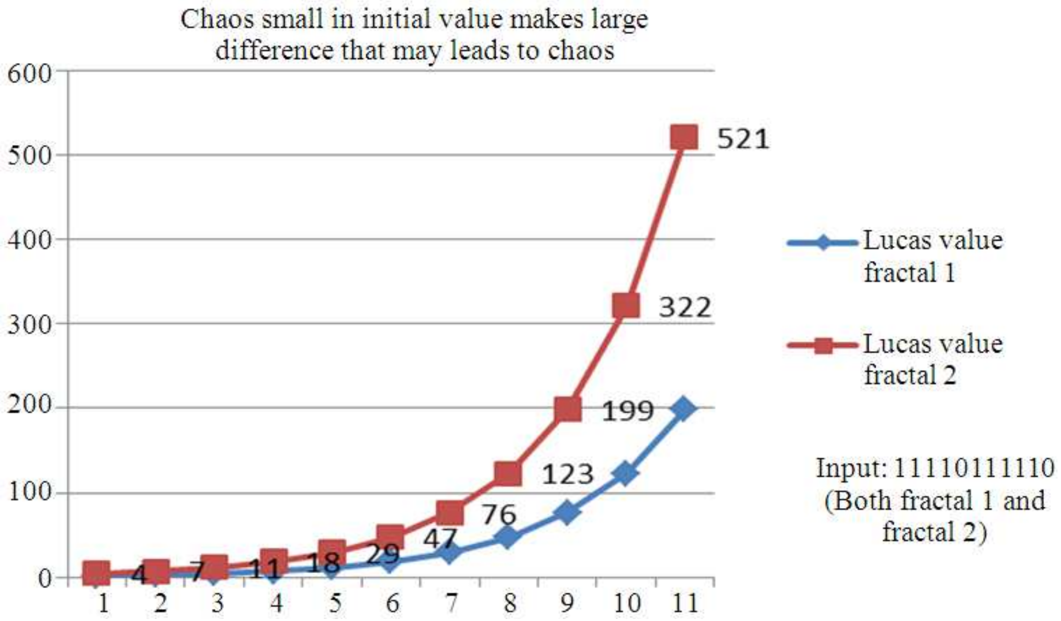


Fig. 5. A chaotic behavior chart analysis

Table 3:

- The given data is 1982 and its corresponding binary value is 11110111110. The Image generation algorithm generate a fractal based on the given data
- First, the PRNG generates the sequence random number 1, 3, 4, 5, 6, 7, 8….199; we use the first value as the initial condition 1. Based upon the initial condition it starts to draw the representation for the given binary data according to the rules framed in an Image generation algorithm
- The image generation algorithm use the Lucas series ranges from (1 3 4 7 11 18 29 47 76 123 199) for fixing the position and rules to be followed for the representation of fractal
- We use 0, 1 and Null bits. Rule 1 is used to represent the bit 1, Rule 2 is used to represent the

bit 0 and Rule 3 is used to represent the bit null. Based on the given bit the algorithm generates the fractal image

- Finally the Image generation algorithm generated the resultant Fractal Image. For the same data and rules we obtained the different Image because of the initial condition. Smaller changes in the initial condition may lead to a large difference, chaos is introduced
- The number generated by the PRNG is hard to break. Based upon this idea we fix the initial condition as a seed. If the initial condition changes the total behavior of the algorithm is changes and it fail to produce the Original fractal image, it may lead to chaos

Chart-Chaotic Chart Analysis

Input: 11110111110

Description:

Image Generation Algorithm generates two different fractals for the same given binary values. The values and positions are listed in Table 4.

The PRNG fix the initial conditions for fractal 1 = 1 and fractal 2 = 4. There is only a small change in the initial condition between 1 and 4, but the outcome is different. In this case the chaos is introduced, i.e. small changes may leads to the larger difference that may lead to chaos.

Figure 5 shows the chart analysis of the chaotic behavior of the dynamical system.

Table 2. Original Fractal Image = No changes in Initial condition (4).

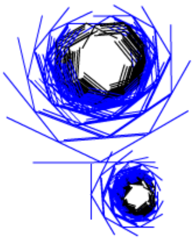
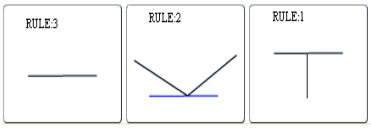
SI.NO	Data	Binary values	Image generation algorithm		Resultant image
1.	1982	11110111110	Type of series	LUCAS	
			PRNG generates	4	
			Initial condition	4 (Chaotic behaviour arises)	
			Rules used	R1,R2,R3	
					
			Sequences generated	4	1 ->(R1)
				5	Null ->(R3)
				6	Null
				7	1
				8	Null
				9	Null
				10	Null
				11	1
				.	.
				.	.
				.	.
				521	0 ->(R2)
			Positions	4	1
				7	1
				11	1
				18	1
				29	0
				47	1
				76	1
				123	1
				199	1
				322	1
				521	0

Table 3. Different fractal image obtained = changes in initial condition (1) (lead to chaos)

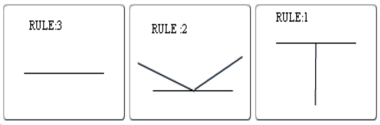
SI.NO	Data	Binary values	Image generation algorithm		Resultant image
1.	1982	11110111110	Type of series	Lucas	
			PRNG generates	1	
			Initial condition	1(Lead to Chaos)	
			Rules used	R1,R2,R3	
			Sequences generated	1	1 -> (R1)
				3	1
				4	1
				5	Null
				6	Null
				7	1
				8	Null
				9	Null
				.	.
				.	.
				.	.
				199	0 ->(R2)
			Positions	1	1
				3	1
				4	1
				7	1
				11	0
				18	1
				29	1
				47	1
				76	1
				123	1
				199	0

Table 4. The Lucas values and its Positions of Fractal 1 and Fractal 2

	Lucas values	
Binary value	Fractal 1	Fractal 2
1	1	4
1	3	7
1	4	11
1	7	18
0	11	29
1	18	47
1	29	76
1	47	123
1	76	199
1	123	322
0	199	521

Conclusion

We Proposed Image Generation Algorithm that generates Message Authentication Image (MAI) using chaos theory and Iterated Function System (IFS) technique. This algorithm generates two different fractal images for the same given data and also it analysis and identified the chaotic behavior. The Message Authentication Image (MAI) can be used as a digital signature. This algorithm can be used for online application like e-banking, e-voting. Further, it can be applied in government and Identifications proofs. We plan to implement the application of Image generation algorithm as our future work.

Funding Information

The authors have no support or funding to report.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Agaian, S.S. and J.M. Susmilch, 2006. Fractal steganography using artificially generated images. Proceedings of the IEEE Region 5 Conference, Apr. 7-9, IEEE Xplore Press, San Antonio, TX, USA, pp: 312-317. DOI: 10.1109/TPSD.2006.5507412

Bashkirtseva, I. and L. Ryashko, 2013. Attainability analysis in the problem of stochastic equilibria synthesis for nonlinear discrete systems. Int. J. Applied Math. Comput. Sci., 23: 5-16. DOI: 10.2478/amcs-2013-0001

Bilal, M., S. Imtiaz, W. Abdul, S. Ghouzali and S. Asif, 2013. Chaos based Zero-steganography algorithm. Multimedia Tools Applic., 72: 1073-1092. DOI: 10.1007/s11042-013-1415-y

El-Khamy, S.E., O. Abdel-Alim and M.M. Saii, 2000. Neural network face recognition using statistical feature extraction. Proceedings of the 17th National Radio Science Conference, Feb. 22-24, IEEE Xplore Press, Minufiya, pp: C31/1-C31/8. DOI: 10.1109/NRSC.2000.838960

Geetha, G., 2007. Non-linearity in Ciphers. Proceedings of the TISC.

Geetha, G. and K.M. Suresh, 2008. Asymmetric key cipher based on non-linear dynamics. Proceedings of the 1st International Conference on Emerging Trends in Engineering and Technology, Jul. 16-18, IEEE Xplore Press, Nagpur, Maharashtra, pp: 1250-1254. DOI: 10.1109/ICETET.2008.119

Kiani, K., M. Arian and V. Soleimani, 2011. Image authentication using fractal watermarking and chaos theory. Proceedings of the 4th International Conference on Signal Processing and Communication Systems, Dec. 13-15, IEEE Xplore Press, Gold Coast, QLD, pp: 1-5. DOI: 10.1109/ICSPCS.2010.5709758

Shannon, C.E., 1949. Communication theory of secrecy systems. Bell Syst. Technol. J., 28: 656-715. DOI: 10.1002/j.1538-7305.1949.tb00928.x

Tayel, M., H. Shawky and A.E.S. Hafez, 2012. A new chaos steganography algorithm for hiding multimedia data. Proceedings of the 14th International Conference on Advanced Communication Technology, Feb. 19-22, IEEE Xplore Press, PyeongChang, pp: 208-212.

Thamizhchelvy, K. and G. Geetha, 2012b. E-banking security: Mitigating online threats using Message Authentication Image (MAI) algorithm. Proceedings of the International Conference on Computing Sciences, Sept. 14-15, IEEE Xplore Press, Phagwara, pp: 276-280. DOI: 10.1109/ICCS.2012.29

Wu, H.C. and C.C. Chang, 2003. Hiding digital watermarks using fractal compression technique. J. Fundamenta Inform., 58: 189-202.

Wu, Y. and J.P. Noonan, 2012. Image steganography scheme using chaos and fractals with the wavelet transform. Int. J. Innovat. Manage. Technol., 3: 285-289.

Zhirabok, A. and A. Shumsky, 2012. An approach to the analysis of observability and controllability in nonlinear systems via linear methods. Int. J. Applied Math. Comput. Sci., 22: 507-522. DOI: 10.2478/v10006-012-0038-1