Design of Digital Signature Algorithm by Fractals and Chaos Theory

Dr. G. Geetha
Dean
School of Computer Science and Applications
Lovely Professional University, Phagwara.

K. Thamizhchelvy
Assistant Professor
Department of Computer Applications
Sathyabama University, Chennai.

ABSTRACT

Message Authentication Code is a function of the message and a secret key that produces a fixed-length value that serves as the authenticator. MAC provides authentication and confidentiality. This authentication technique does not include measures to counter repudiation by the source i.e. it does not provide digital signature. We propose a new Message authentication Image (MAI) Algorithm that provides confidentiality, authentication and digital signature. It uses Cryptographic and Steganographic ideas to conceal the data in the image. MAI is generated by using fractals. This approach explores the main feature of fractal image generated by Iterated Function System (IFS) techniques.

Keywords - Fractals, Message Hiding, Message Authentication Image (MAI), Message Authentication Code (MAC).

1. INTRODUCTION

With the rapid development in the communications and information transmissions there is a growing demand for new approaches that increase the security of cryptographic systems. Therefore some emerging theories, such as fractals, can be adopted to provide a contribution towards this goal. Cryptography is the science concerned with the transfer of information. Some of the basic goals of cryptography include Information security, information integrity, authentication, and non-repudiation, among others. This paper is concerned primarily with providing digital signature. Digital signature is an authentication technique that also includes measures to counter repudiation by the source.

Message authentication or digital signature mechanism can be viewed as having two levels. At lower level, there must be some sort of functions producing an authenticator – a value to be used to authenticate a message. This lower level functions is used as primitive in a higher level authentication protocol.

In this paper we propose a new MAI algorithm using chaos. The paper is organized as follows - Section 2 deals with literature survey on fractals in Image encoding and chaotic cryptographic algorithm used to generate a fractal, Section 3 deals with definitions and mathematical background, in Section 4, Chaotic Cryptographic algorithm is proposed, in Section 5, fractal generation using chaotic cryptographic algorithm is given, in Section 6 an overview of message authentication code, proposed message authentication image, in Section 7 we compare the existing algorithm with our proposed Digital Signature Algorithm and in section 8 we bring out the conclusion and future work.

2. LITERATURE SURVEY

2.1 Usage of fractals in image encoding

Fractals are seen everywhere in nature and yet so very mysterious. First imagined by Julia and Mandelbrot, fractals have an element of chaos, but also have an essence based in mathematics. But these are not the only way to represent fractals. Here, Sierpinski Gasket is drawn using an Iterated Function System. This fractal was originally thought up by W. Sierpinski and predates the Mandelbrot Set. It was originally produced by starting with a triangle, cutting out the middle, and repeating the process infinitely. In this way, you can see that at each iteration, one quarter of the original triangle is removed. That is, three quarters of the area of the original triangle is left after the first iteration. From this observation, it is not hard to infer that after n iterations, the area of the gasket would be (0.75)n times the area of the original triangle. So after an infinite number of iterations, you would find there was no area at all.

El-Khamy, S.E. Khedr et all [1] 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 all [2] 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 [3] developed a chaotic cryptographic algorithm backed by stochastic approach to matrices, nonlinearity and randomness. G.Geetha showed that non-linearity plays a vital role in cryptographic algorithms by appealing to chaos and quantum chaos [4, 5]. G.Geetha et al developed an Asymmetric key cipher using fractal dimension and Lyapunov Exponents.

Chin-Chen Chang et al [6] 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. Finally embedded the encrypted data into the middle-frequency domain of DCT.

Hsien-Chu Wu et and Chin-Chen Chang [7], 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 all [8], presented a fractal coder that derives highly image-adaptive partitions and corresponding fractal codes in a time-efficient manner using a region merging approach.

"Fractal Image Compression: Theory and Application" [9] 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.

2.2 Chaotic Cryptography

The idea of using chaos in cryptography can be traced back to Shannon's classic paper "Communication theory of secrecy systems" [10]. He had mentioned that the good mixing transformations used in a good secrecy systems can be constructed by the basic rolled-out and folded-over operations. Some researchers have pointed out that there exists tight relationship between chaos and cryptography [11, 12, 13, 14, 15 and 16]. The possibility for self-synchronization of chaotic oscillations has sparkled an avalanche of works on application of chaos in cryptography. Many fundamental properties of chaos such as ergodicity, mixing and exactness property and the sensitivity to initial conditions can be considered with the confusion and diffusion property of cryptography. So it is a natural idea to use chaos in cryptology.

From 1989, many chaotic ciphers have been proposed and analyzed. Ljupco Kocarev et al demonstrated how to construct a DES like block cipher using chaotic maps in a general way. Very recently the idea of using chaos to generate S boxes and then to design new ciphers have been investigated by Ljupco Kocarev et al. in [17,18], Jesus Urias in [19] and S.Li et al. in [20]. The above works have shown that chaos can be used to design ciphers that are similar to traditional ciphers.

Even though the usage of chaos in Cryptography dates back to 1949, the notion in which Geetha et al. introduced chaos to develop a cryptosystem is novel. 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 cryptosystem.

3. DEFINITIONS AND MATHEMATICAL BACKGROUND

3.1 Non linear dynamical system

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

3.2 Difference Equation

Difference equation is an equation involving differences. We can see difference equation from three different views – as sequence of number, discrete dynamical system and Iterated function.

Difference equation is a sequence of numbers that generated recursively using a rule to relate to each number in a sequence to previous numbers in the sequence.

Difference equation is a discrete dynamical system. It takes some discrete input signal and produces output signal.

Difference equation is an iterated map

y(k+1) = f(y(k)) if we see the sequence as iterated function.

Example :

y(k+1) = f(y(k)) = y(k)2

y0=1 will produce the orbit {1,1,1…}

y0=2 will produce the orbit {2,4,16,256,….}

y0=.5 will produce the orbit {0.5,0.25,0.625,…}

We see that knowing the rule only is not enough to know the behavior of the sequence. Initial value is also important. Knowing the rule and the initial value, we can generate the whole sequence recursively. The value of k is an integer and rule to generate the sequence is called difference equation or the dynamical system or iterated function.

3.3 Stochastic interpretation of matrices

We denote the algebra of n x n real, respectively complex, matrices by Mn(R), respectively Mn(C); the semi-group of n x n doubly stochastic matrices by Ωn ; the semi-group of n x n real matrices with each row sum and column sum equal to 1 by $\hat{\Omega}$ n ; the multiplicative group of n x n nonsingular real matrices by GLn(R) and the multiplicative group of $\hat{\Omega}$ n by GLn(R). For A(aij) $\in$ Mn(R) , we write A>=0 if each aij >= 0, A>0 if each aij >0. We denote the sum of the ith row of A by ri(A) and the sum of the jth column by cj(A). The n x n identity matrix will be denoted by In.

A stochastic interpretation of real matrices lies in the following two theorems.

Theorem 1: Let A $\in$ Mn(R). Define $\tilde{A} \in \hat{\Omega}$ n+2 as follows:

$$\tilde{A} = \left(\begin{array}{ccc|cc} & & & 1-r1 & 0 \\ & A & & : & : \\ & & & : & : \\ & & & 1-tn & 0 \\ \hline 0 & ..... & 0 & 1 & 0 \\ 1-c1 & ..... & 1-cn & s-n & 1 \end{array}\right)$$

where ri =ri(A), cj=cj(A), s=r1+…..rn

Then the mapping ϕ : Mn(R) → $\hat{\Omega}$ n+2 where ϕ (A) = $\tilde{A}$, is an injective semi-group homomorphism. Moreover, the restriction ϕ * of ϕ to GLn(R) is a group monomorphism from GLn(R) is a group monomorphism from GLn(R) is a group monomorphism from GLn(R) to $\sum$ GLn+2(R)

Theorem 2: With the notation in theorem 1, write $\tilde{A}$ = $\tilde{a}$ ij and define for any real number t>=0,

$$\omega \text{ t} = \text{t} + \max(-\tilde{a} \text{ ij} : \tilde{a} \text{ ij} <=0),$$

$$\text{At} = \tilde{A} + \omega \text{ t E}, \quad \text{Pt} = \varepsilon \text{ t -1 At}$$

Where E is the (n+2) x (n+2) matrix with all entries equal to 1, and ε t = 1+(n+2) ω t

Theorem 3: There is an injective semi-group homomorphism

ϕ : Mn(C) → $\hat{\Omega}$ n+2

given by ϕ (C) = $\phi\ \theta$ (C),

where θ is the canonical embedding of Mn(C) in M2n(R) and

: M2n(R) → $\hat{\Omega}$ 2n+2 is the homomorphism given by theorem 1.

(C) = $\tilde{C}$ = $\tilde{c}$ ij and define for each real number t>=0,

γ t = t + max(- $\tilde{c}$ ij : $\tilde{c}$ ij <=0),

Ct = $\tilde{C}$ + λ t E, Pt = δ t -1 Ct

4. CHAOTIC CRYPTOGRAPHIC ALGORITHM

4.1 Chaos as a non-linear 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. This function is the limit of sequence of simple measurable functions.

To define a simple measurable function,

Gn = a1ψe1 + a2ψe2 + ……… anψen .

Taking the sequence an as a convergence sequence, we can give a convergent simple measurable function. It is enough to prove the convergence of an. The non-linearity is introduced through difference equation or difference differential equation.

4.2 Simulation of linear difference equation

We can show that the solutions of a homogeneous linear difference equation with complex coefficients can be generated probabilistically with the help of above theorems.

We denote a given positive integer by n and a variable nonnegative integer by k.

Consider the homogeneous linear difference equation

uk+1 = a0uk + a1uk-1 + …. an-1uk-n+1, k>=n-1

where a0 , a1 ,…… an-1 $\in$ C and an-1 $\neq$ 0.

A sequence { uk }k>=0 that satisfies the above equation is uniquely determined by the initial values u0 , u1 ,…… un-1 and is called a solution of the above equation.

Denote the set of solutions of the above equation by U

We associate to the above equation the n x n matrix

$$A = \begin{pmatrix} a0 & a1 & a2 & .... & an-2 & an-1 \\ 1 & 0 & 0 & .... & 0 & 0 \\ 0 & 1 & 0 & .... & 0 & 0 \\ : & : & : & : & : & : \\ 0 & 0 & 0 & .... & 1 & 0 \end{pmatrix}$$

and define n solutions { uk (i)} k>=0 , i =1,….n such that they satisfy the initial conditions given by

$$A= \begin{pmatrix} un-1 & un-1 & .... & un-1 \\ un-2 & un-2 & .... & un-2 \\ : & : & & : \\ u1 & u1 & u1 & u1 \\ u0 & u0 & u0 & u0 \end{pmatrix}$$

Theorem 4

The solutions of the linear difference equation can be simulated by Markov chains on at most (2n+2) states

4.3 Illustration

The Fibonacci and Lucas numbers {Fk} , {Lk} satisfying the recurrence relation uk+1 = uk + uk-1, k>=1, with initial conditions F0=0, F1=1, Lo=2 and L1=1, can be simulated by the Makov chain {Xk} k>=0 with state space {1,2,3,4} and transition probability matrix

$$Pt = (1+4t) -1 \begin{pmatrix} t+1 & t+1 & t-1 & t \\ t+1 & t & t & t \\ t & t & t+1 & t \\ t-1 & t & t+1 & t+1 \end{pmatrix}, r>=0$$

For k>=1,

Fk = ¼ + (1+4t)k (P_{12}^{k} - ¼)

Lk = (1+4t)k (4pk – 1)-1,

Where pk = P(Xk-X0) with X0 uniformly distributed over {1,2,3,4}.

There are different measures available to measure the chaotic behaviour namely fractal dimension, correlation dimension, Kolmogorov-Sinai entropy, approximate entropy etc. We consider fractal dimension to quantify chaos.

In our encoding, we employ Iterated function system to replace the text with the corresponding embedded Markov system. Using the stochastic approach to matrix developed by Y.K.Leong [21] we give the infinite dimensional stochastic probability matrix corresponding to embedded Markov chain of a Markov process. This leads to a difference equation which in turn explains a non-linear dynamical system.

Combining these ideas, we develop a new variety of encoding system replacing the plaintext by the corresponding fractal set suggested by the combination of embedded Markov chain and difference equation. As the scheme is slow in execution, the encoding process and key generation requires special type of computational techniques. For this purpose, we appeal to algebraic functional programming. We employ fold and functors based on functional programming technique to speed up the process.

4.4 Construction of fractal using probabilistic method

Fractals provide a geometric framework for the modeling of self-similarity and have become widely used in recent years in broad range of applications. We can construct fractals in many ways. Here we suggest the probabilistic method.

Let us consider the case of the plain self-affine set. Let {S1,..,Sm} will be some system of affine contractive maps. Maps Si can be represented as: Si(x)=Ai(x-oi)+oi, where Ai - some matrix of 2x2 size and oi - a vector.

1. As the starting point we will take the fixed point of the first map S1: x:=o1;Here we use that all fixed points of contractions S1,..,Sm belong to the fractal. As the starting point we can choose any point, and the generated sequence of points will converge to the fractal anyway, but some wrong points will appear on the screen.
2. Draw the current point x=(x1,x2) on the screen: putpixel (x1,x2,15);

Select in a random way a number j from 1 to m and recalculate coordinates of the x point:j:=Random(m)+1;x:=Sj(x);

3. Go to step 2, or stop if sufficiently many number of iterations are done

Remark. If the contraction coefficients of maps Si are different, then the fractal will be filled with points irregularly. In a case, when maps Si are similarities, this can be avoided by small complication of algorithm. On the 3-rd step of algorithm, number j from 1 to m should be selected by probabilities p1=r1s,..,pm=rms, where ri denotes similarity coefficient of the map Si, and number s (known as similarity dimension) is found from the equation r1s+...+rms=1. This equation can be solved, by Newton method.

4.5 Algorithmic steps

Plaintext is converted into binary.

- Mapping is done using difference equation.
- Replacement is made by corresponding fractal constructed using the probabilistic method.
- The position into which the replacement is done is identified by pseudo random number generator
- If the same random number is generated by the PRNG, next iteration is done.
- If the PRNG generates a value in the non-difference sequence, null is introduced.
- This system is implemented using Fibonacci sequence (difference equation) and Sierpinski gasket (fractal set).
- The non-linear dynamics explained by the difference equation can be viewed as the same non linearity generated by the fractals.

5. FRACTAL GENERATION RESULTS

In Figure 1, we hide the message in sierpinski triangle using the features of chaos. Let A, B, C be the vertices of the triangle. Start with a random point in the plane, and move the point one-half of the distance to one of the vertices. Choose to move with equal likelihood toward each of A, B and C. From the new point, randomly choose one of the vertices and repeat. The attractor for this process is the sierpinski gasket, an example of iterated function system. In this triangle we represent 1, 0 and null.

Example: Let the binary plaintext be 11011011

Let us consider the Fibonacci sequence 5, 8, 13, 21, 34, 55, 89, 144…..We can start with any number. The starting number corresponds to the initial condition. Let us generate the pseudo random number. If we are going to encode eight bits and the starting value of the Fibonacci series is 5, then we give the range between 5 and 144. If the range of the seed is larger, we get more randomized result. If we choose a bigger number as the starting value, then the range will be larger and hence the seed is highly randomized.

Position	Value
5	1
8	null
13	null
21	1
34	null
55	null
89	null
144	null

Using the Pseudo random number, encryption is done. For example, if the PRNG generates 7, then triangle representing null is created, if it generates 5, triangle representing 1 is created and so on. Conditional statements will be framed so as to form a fractal. Key is generated based on the random number generation and the initial condition. We have taken Fibonacci sequence and Sierpinski gasket as an example.

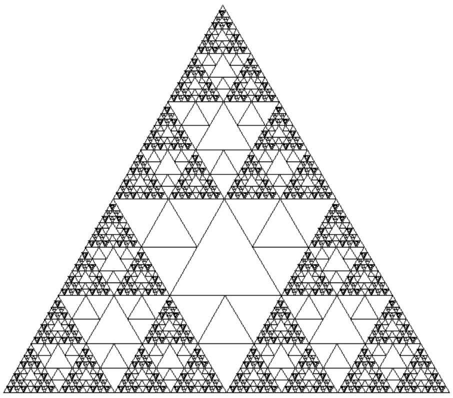


Fig 1 : Sierpinski triangle with embedded message

6. MESSAGE AUTHENTICATION

The process of determining the identity of a user. In effect, authentication validates that the user is who he or she claims to be. Message authentication may also verify sequencing and timeliness.

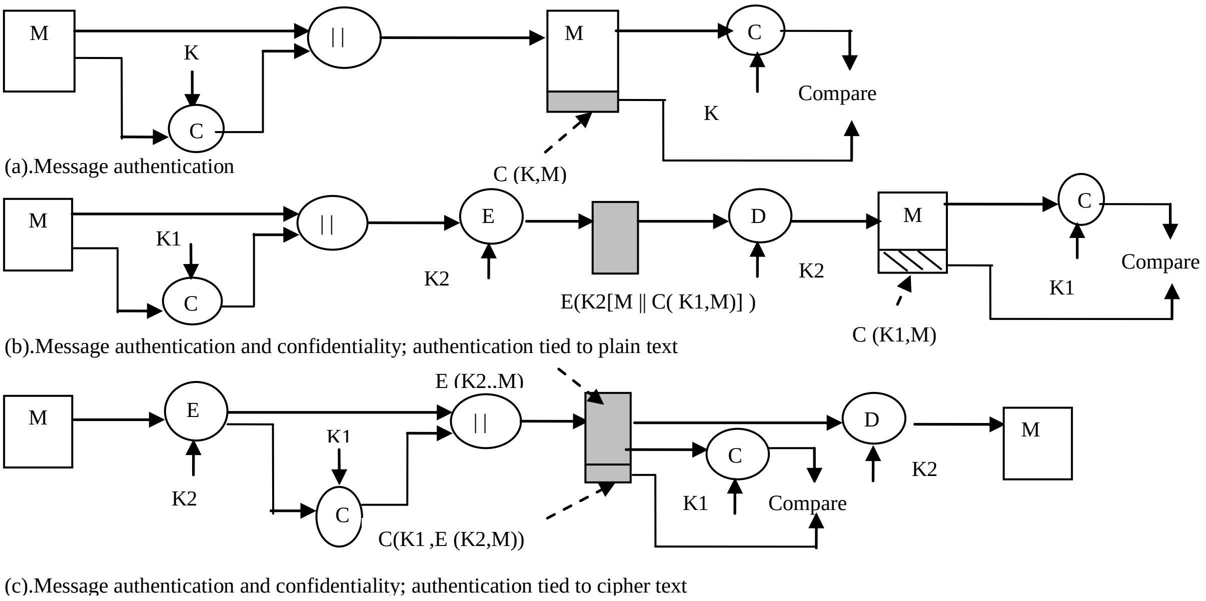
6.1 Why is strong authentication needed?

Single-factor authentication usually consists of "something you know". However, generally, these could be susceptible to attacks that could compromise the security of the application. Some of the more common attacks can occur at little or no cost to the perpetrator and without detection.

Such programmers are readily available over the internet. If undetected, the perpetrator could access the information without alerting the legitimate user. This is the reason of using a strong user authentication process to protect the data and systems.

The need for strong user authentication has many benefits.

1. Strong user authentication is amply demonstrated by the use of ATMs - access to an ATM is protected by a strong user authentication; a bankcard, and a PIN.
2. Reducing the risk of unauthorized access, two-factor authentication also provides institutions with a foundation to enforce electronic transactions and agreements.



(a).Message authentication

(b).Message authentication and confidentiality; authentication tied to plain text

(c).Message authentication and confidentiality; authentication tied to cipher text

Fig 2 : Basic Uses Of MAC

6.2 Message Authentication Code (MAC)

In cryptography, a message authentication code (often MAC) is a short piece of information used to authenticate a message. A MAC algorithm, sometimes called a keyed (cryptographic) hash function, accepts as input a secret key and an arbitrary length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. While MAC functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgery under chosen-plaintext attacks.

MAC algorithms can be constructed from other cryptographic primitives, such as cryptographic hash functions (as in the case of HMAC) or from block cipher algorithms (OMAC, CBC-MAC and PMAC). However many of the fastest MAC algorithms such as VMAC are constructed based on universal hashing.

In Figure 3, the sender of a message runs it through a MAC algorithm to produce a MAC data tag. The message and the MAC tag are then sent to the receiver. The receiver in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver then compares the first MAC tag received in the transmission to the second generated MAC tag. If they are identical, the receiver can safely assume that the integrity of the message was not compromised, and the message was not altered or tampered with during transmission.

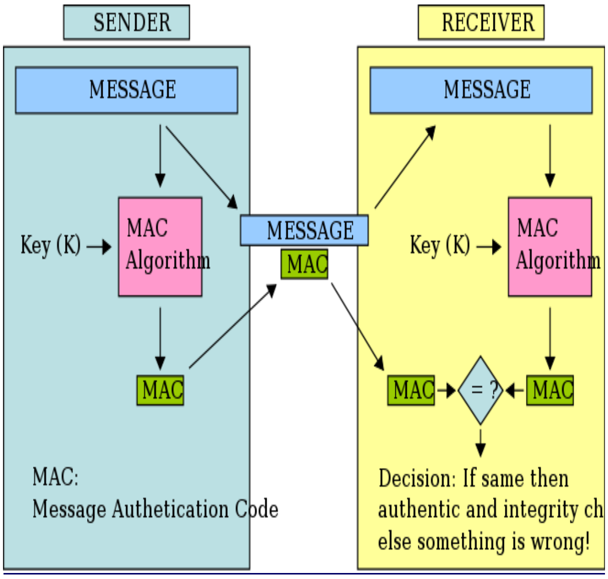


Fig 3 : Message Authentication Code

In Figure 2.a, provides authentication. In Figure 2.b, authentication and confidentiality; authentication tied to the plain text. In Figure 2.c, authentication and confidentiality; authentication tied to the cipher text.

6.3 Message Authentication Image (MAI)

A Message Authentication Image (MAI) is generated by using fractal. This approach explored the main feature of fractal image generated by Iterated Function System (IFS) techniques as shown in section 5 of this paper. The application of chaos in generating the MAI makes it difficult for the steganalyst, to identify the hidden data, as the security is based on the initial condition. MAI finds its application to avoid phishing. We propose to extend this as our future work.

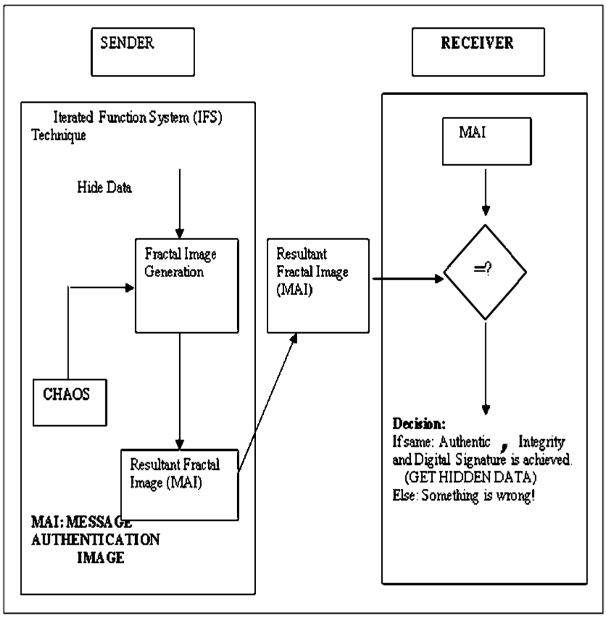

SENDER
RECEIVER
Iterated Function System (IFS) Technique
Hide Data
Fractal Image Generation
Resultant Fractal Image (MAI)
CHAOS
Resultant Fractal Image (MAI)
MAI: MESSAGE AUTHENTICATION IMAGE
MAI
=?
Decision:
If same: Authentic , Integrity and Digital Signature is achieved.
(GET HIDDEN DATA)
Else: Something is wrong!

Fig 4 : Message Authentication Image

The basic operation of the MAI is as follows:

Sender:

- Generate a Fractal Image by using IFS techniques.
- While generating the Image, apply the principle of Chaos i.e. Non-linearity and randomness, as a tool to hide data.
- Message Authentication Image is generated.
- Send it to receiver.

Receiver:

- After receiving the Image the User compares the received Fractal Image with the Original Fractal Image.
- Can verify the authenticity, confidentiality and digital signature.

In MAC algorithm it provides authentication and confidentiality but in MAI algorithm it provides authentication, confidentiality and Digital signature. In Figure 5.d, It encrypt a given message by using private key PRa and K2. It uses the key K1 to hide the encrypted data into an image I (K1, E2 (K2 , E1 (PRa,M))) to achieve the digital Signature.

6.4 MAI is better than MAC

- Non-Linearity and Randomness used while generating fractal makes it hard to break.
- MAC uses cryptographic primitives like HMAC, OMAC, PMAC, VMAC etc. MAI uses both cryptographic primitives and steganographic ideas to conceal the data in the image.
- MAC is used only for the message authentication whereas MAI can be used for Digital Signature.

7. COMPARISION OF MAC AND MAI

The following table describes the comparison between MAC and our proposed Digital Signature Algorithm.

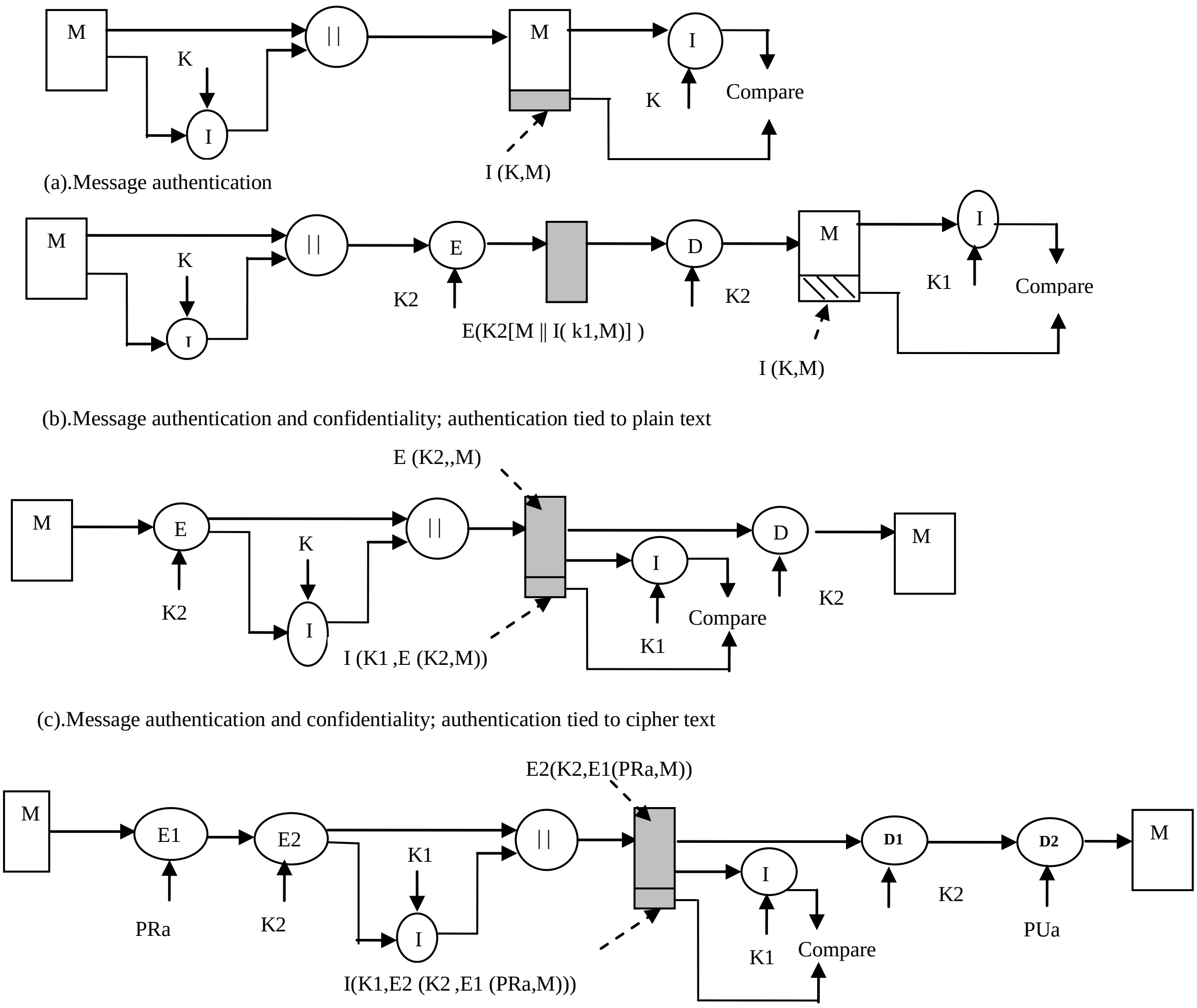
Table 1. Comparison of MAC and MAI

S. No	Security Services	MAC	MAI
1	Message Authentication	Yes	Yes
2	Confidentiality	Yes	Yes
3	Digital Signature	No	Yes
4	Result	Code	Image
5	Mechanism	Existing Cryptographic Algorithms	Non-Linearity & Randomness
6	Strength	Weak	Strong

8. CONCLUSION

We proposed a new Message authentication Image (MAI) Algorithm that provides confidentiality, authentication and digital signature. We implemented and generated a sierpinski triangle exploring the properties of chaos and message hiding techniques and proposed a new MAI technique. The hidden data is robust enough to withstand image processing technique. This technique can be employed in online transactions like Banking, Shopping etc. to avoid phishing. We plan to implement the application of MAI as our future work.

The following diagram illustrates how MAI can be used for message authentication, confidentiality and digital signature.



(a).Message authentication

(b).Message authentication and confidentiality; authentication tied to plain text

(c).Message authentication and confidentiality; authentication tied to cipher text

(d).Message authentication ,confidentiality and digital signature; authentication tied to cipher text

Fig 5 : Basic uses of MAI

9. REFERENCES

[1] El-Khamy, S.E. Khedr et all ,“A hybrid fractal-wavelet data hiding technique”,In the Proc. Of National Radio Science Conference, NRSC 2008, ISBN: 978-977-5031-95-2 pp 1-9.

[2] Zolotavkin, Y. Lukichov et all ,“A novel approach to the security of data hidden in multimedia objects”, In the Proc. Of International Carnahan Conference on Security Technology, ICCST 2008, ISBN: 978-1-4244-1816-9 ,pp 23-28.

[3] Thiyagarajan.M, Geetha.G “Complex facets of Cryptography”, In the Proc. of International conference on Systemics, Cybernetics and Informatics, ICSCI 2007, pp 555 – 559.

[4] G.Geetha, Thiyagarajan M, “Quantum dots as a cryptographic tool, Presented in International Conference on nanomaterials, communication and broad casting systems, SASTRA, Thanjavur, 2007.

[5] G.Geetha, “Non-linearity in Ciphers”, In the Proc. of TISC 2007.

[6] Chin-Chen Chang et all ,“A DCT-domain system for hiding fractal compressed images”, In the Proc. Of Advanced Information Networking and Applications, AINA 2005, ISBN: 0-7695-2249-1, pp 83-86,vol.2.

[7] Hsien-Chu Wu et and Chin-Chen Chang, “Hiding digital watermarks using fractal compression technique”, In the Journal of Fundamenta Informaticae,ISSN 0169-2968, Volume 58, Number 2/2003.

[8] Hannes Hartenstein et all, “Region-based fractal image compression”, In the Proc. Of Image Processing, ISSN: 1057-7149,PP 1171-1184.

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

[10] Shannon C.E, “Communication theory of Secrecy Systems”, Bell Sys.Tech. J., 28(4), pp 656-715, 1949.

[11] Alwarez G, Monotoya E, Pastor G, Romera M, "Chaotic cryptosystems", In Proc. IEEE Int. Carnaltan conf. Security technology, pp 332-338, IEEE 1999.

[12] Jiri Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", Int.J.Bifurcation and chaos, 8(6):1259-1284, 1998.

[13] Ljupco Kocarev, Goce Jakimoski, Tony Stojanovski and Ulrich Parlitz, "From Chaotic maps to encryption schemes", In Proc. IEEE Int. Symposium circuits and Systems 98, Vol.4, pp514-517, IEEE 1998.

[14] Marco Gotz, Kristina Kelber, and Wolfgang Schwarz, "Discrete time Chaotic Encryption systems Part I: Statistical design approach", IEEE Trans, Circuits and Systems-I, 44(10): pp963-970, 1997.

[15] Brown R and Chua L.o, "Clarifying Chaos Examples and counter examples", Int.J.Bifurcation and chaos, 6(2)219-249, 1996.

[16] Shujun Li, Xuanqin Mou and Yuanlong Cai, " Pseudo random bit generator based on couple chaotic systems and its application in stream ciphers cryptography", In Progress in Cryptology – IndoCrypt 2001, LNCS vol.2247, pp 316-329, Springer-Verlag, Berlin, 2001.

[17] Ljupco Kocarev.Goce Jakimoski, "Logistic map of a block encryption algorithm", Physics Letters A, 289(4.5), pp 199-206, 2001.

[18] Goce Jakimoski and Ljupco Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps", IEEE Circuits and Systems-I, 48(2): pp 163-169, 2001.

[19] Jesus Ufs, Edgardo Ugalde and Gelasio Salazar, "A cryptosystem based on cellular automata", Chaos 8(4): pp 819-822, 1998.

[20] Shujun Li, Xuan Cheng, Xuanqin Mou and Yuanlong Cai, "Chaotic encryption scheme for real time digital video", In Real-time Imaging VI, Proceedings of SPIE vol.4666, pp 149-160, 2002.

[21] Leong Y.K., "Stochastic approach to Matrices", SIAM J Appl Math, Vol.47, pp 1094-1102, 1987.