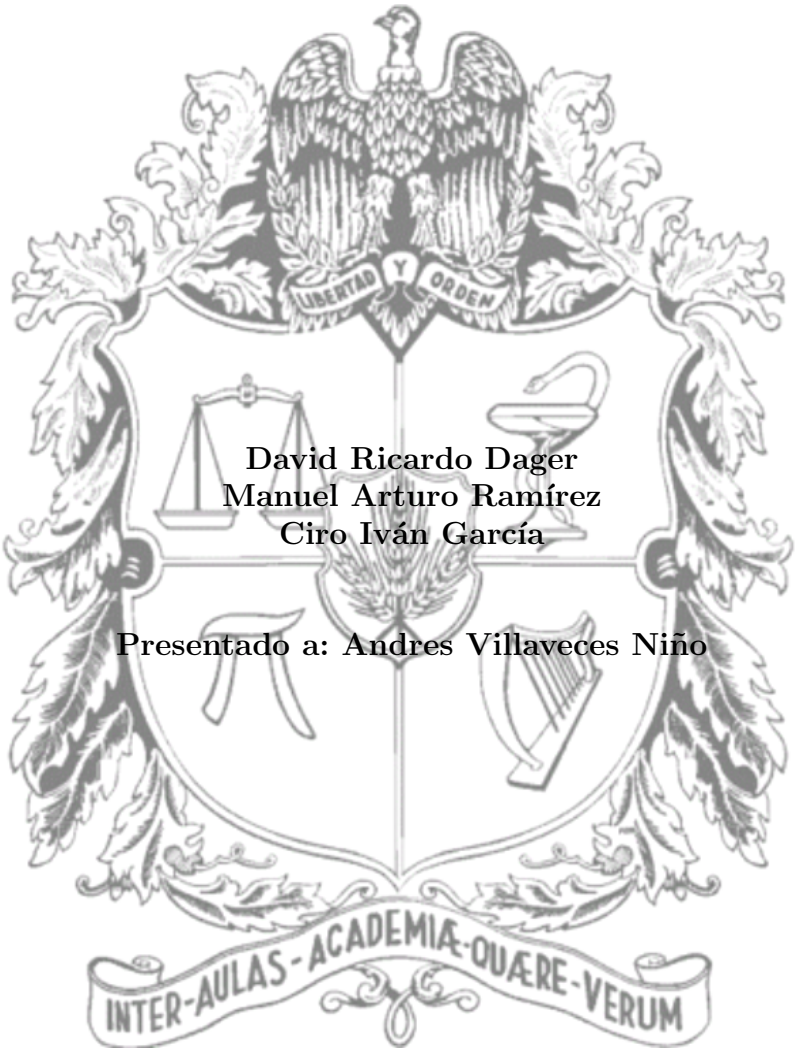
Proyecto Final de Matemáticas Discretas
Fractales Aplicados a la criptografía
Grupo: K-ON



David Ricardo Dager
Manuel Arturo Ramírez
Ciro Iván García

Presentado a: Andres Villaveces Niño

Universidad Nacional de Colombia
Facultad de Ingeniería
Departamento de Ingeniería de Sistemas e Industrial

2 de junio de 2014

Índice

1. Introducción

Gracias a la expansión de la red y de la información en estos ultimos años; el problema de transmitir información de forma correcta, eficiente, rápida y segura es uno de los mayores retos para el mundo entero. Es aquí donde la criptografía juega un papel importante en la vida cotidiana de todo ser humano, permitiendole comunicarse a plenitud con el entorno que le rodea sin temor alguno.

Hasta la fecha existen distintos modelos de criptografía tales como RSA, cuántica, asimétrica, etc. Los cuales cuentan con un desarrollo e investigación muy avanzado. Sin embargo poco a poco han emergido distintos modelos que buscan resolver el problema original desde otras perspectivas, indagando en áreas de la matemática que aún no han sido exploradas; como es el caso de la criptografía basada en fractales, modelo en el cual nos preguntamos por la naturaleza de la geometría fractal y del caos, en busca de soluciones más sencillas sin dejar de lado los aspectos importantes de un buen cifrado.

Tal como como es expuesto por Nadia y Mohamad [ASMM12] los sistemas de cifrado basados en fractales[1] son sistemas cuyo comportamiento no es fácil determinar o predecir, siendo este un factor decisorio a la hora de realizar criptoanálisis, ya que muchas de las técnicas usadas en otros modelos tradicionales de cifrado no se ajustan a la realidad de estos sistemas.

A su vez Ljupco [Lju01] en su trabajo explora los alcances y limitaciones que tienen los SCF, algunas de las cuales llegan a tener un nivel de complejidad tan alto que no serán abordados en el presente trabajo. Estas limitaciones son a su vez un factor motivante en el desarrollo del presente trabajo; es por ello que hemos definido ***INSIGNIAS*** con el fin de resaltar los aspectos más importantes para el trabajo.

Comenzaremos explorando por qué resulta conveniente para nosotros el uso de fractales, Sección 2. La sección 3 describe el algoritmo de cifrado a un nivel de detalle alto. La matriz de cifrado junto con la función de cifrado, corazón del presente trabajo, son trabajadas en la sección 4. El resultado y los detalles de transmición para un mensaje serán expuestos en la sección 5. La sección 6 se encargara del algoritmo para decifrar el mensaje y su funcionamiento. Por último presentamos las conclusiones del trabajo en la sección 7.

2. Fractales

Los fractales son representaciones geométricas de gran interés para cualquier persona ya sea por la belleza de sus formas, su simplicidad o por la naturaleza que los gobierna. Más allá de estas razones existe un mundo matemático que poco a poco ha venido emergiendo y ha sido aplicado en campos como compresión de archivos, generación de graficas, simulaciones y por su puesto en la criptografía; campo en el cual nos puede llevar a encontrar nuevos resultados de gran interés.

[1] De ahora en adelante nos referiremos a ellos como SCF.

Hasta el momento hemos hablado sobre fractales sin embargo no se ha dado una definición rigurosa. Rubiano define un fractal de la siguiente manera "Un fractal es un subconjunto del plano que es autosimilar y cuya dimensión fractal excede a su dimensión topológica"[Ner02] sin embargo, Qué es dimensión fractal? Qué es dimensión topológica?. En una vista rápida a la teoría de (**falta definición eso lo hago luego**).

Es también importante resaltar lo que nos dicen Gutierrez y Hott [PE04] sobre la relación del caos y los fractales, "Los fractales son la representación gráfica del caos".

Los fractales presentan propiedades algunas de las cuales son de mayor interés para el presente trabajo, algunas de ellas son:

1. Tienen un comportamiento caótico.
2. Poseen una dimensión fraccionaria, infinita.
3. Son autosimilares
4. Son representados por un algoritmo *simple*[2]

El comportamiento caótico de los fractales hace de los SCF sistemas eficientes y seguros para la generación de un mensaje cifrado, tal cual como es sugerido por Nadia y Mohamad [ASMM12, NMR09] gracias al caos el trabajo que se debe realizar para vulnerar un SCF se vuelve costoso, necesita un análisis no convencional y requiere de una gran cantidad de tiempo, tanto humano como de máquina. El llamado *Efecto mariposa* propiedad intrinseca del caos y por ende de los fractales actua directamente sobre el sistema reflejandose en *dado un pequeño cambio sobre el mensaje original, la cadena cifrada sufrirá un cambio brusco.*

Por otra parte la propiedad de ser autosimilar es explotado en el diseño del algoritmo que represente al fractal. En una primera aproximación este algoritmo puede estar dado en términos de una función recursiva, infinita, que debe ser acotada en un momento dado ya sea por los limites físicos de la máquina o por algún otro límite impuesto por el usuario.

Se han mencionado algunas de las ventajas que poseen los fractales para el SCF sin embargo Howell y Reese [BAM03] en su trabajo exponen el mayor de los problemas en el uso de fractales aplicados a la criptografía; la complejidad para decifrar la información, lo cual es un paso obligatorio para la validación del sistema. Durante el desarrollo se ha prestado atención a este problema e intentaremos dar un tratamiento a la solución propuesta de tal forma que obtengamos un sistema verificable.

3. Desarrollo del problema

Luego de explorar diversas fuentes en busca de información sobre cifrado basado en fractales y caos se ha llegado a la conclusión de reunir varios aspectos de ellos con el fin de generar un SCF de alta calidad. Entre las ideas más relevantes cabe resaltar las propuestas de Howell y Reese [BAM03], Nadia y Muhammad [NMR09], Makris y Ioannis [GI12], Pichler y Scharinger [FJ], Jiri [Fri97] y por último la propuesta de Yuen y Wong [YW11].

Con el fin de poder tratar los detalles del SCF es prudente hablar de las definiciones base o preliminares.

DEFINICIÓN 1 : Definimos como Ω *el conjunto de carácteres* {*a,b,...,z,A,B,...,Z,0,1,2...,9,+,-,*,/,<,> ,#,*γ*,?, %,$,{,},coma,punto,[,],(,)*}*; donde* γ *es el espacio en blanco y sea* Ω^* *el conjunto de todas las cadenas sobre* Ω*.*

DEFINICIÓN 2 : Un SCF (ξ*) es una **función para la cual*

$$\xi : \Omega^* \longmapsto \Omega^*$$

$$x \longmapsto x^c$$

De donde $x \epsilon \Omega^*$ *y* x^c *se dice la cadena cifrada de* x*.*

[2]En el contexto del presente trabajo simple no se (**).

La definición 1 nos permite plantear nuestra primera insignia.[3]

INSIGNIA 1 : El SCF presentado está limitado a trabajar unicamente con conjunto de carácteres Ω.

El alfabeto de entrada es considerado una insignia dado que indica la directriz que deben seguir los textos de entrada para el SCF; para un carácter no pertenesca a este conjunto el comportamiento del SCF no ha sido determinado. Con nuestras las dos primeras definiciones podemos describir el funcionamiento interno del SCF, para este fin se ha escrito el siguiente algoritmo.

ALGORITMO 1 SCF (ξ) *: Dada una cadena* $x \epsilon \Omega^*$ *con* $\boldsymbol{j}$ *carácteres; se procesará de la siguiente manera.*

1. *Generar la matriz de cifrado.*
2. *Cifrar el mensaje*
   a) *Tomar el siguiente carácter de la cadena,* α_i.
   b) *Elegir un número, entero, aleatorio dentro del dominio [a,b],* φ_i.
   c) *Evaluar* $f_{encp}(\alpha_i, \varphi_i)$ *obteniendo* μ_i.
   d) *Almacenar* φ_i,α_i,μ_i.
   e) *Sí aun quedan carácteres volver a 1, si no transmitir.*

Al finalizar nuestro algoritmo sobre la cadena x tendremos la siguiente configuración para las entradas y salidas.

Llave	Entrada	f_{encp}
φ_1	α_1	μ_1
φ_2	α_2	μ_2
:	:	:
φ_j	α_j	μ_j

Del algoritmo 1 podemos introducir las siguientes preguntas aún sin responder.

- ¿Qué es la matriz de cifrado?
- ¿Quiénes son los extremos del dominio?
- ¿Qué es $f_{encp}(\alpha, \varphi)$?
- ¿Quién será x^c?

Las preguntas sobre la matriz de cifrado, los extremos del dominio y $f_{encp}(\alpha, \varphi)$ se trabajan en la sección 4. Igualmente la primera esta relacionada con la forma en la cual debemos transmitir el mensaje, motivo por el cual será resuelta en la sección 5.

4. Matriz de cifrado y función de encriptación f_{encryp}

En la sección 4 se menciono la matriz de cifrado y la función f_{encryp}; en la presente sección buscamos presentar al máximo de detalles estos dos componentes del trabajo, empezaremos hablando de la matriz de cifrado y su papel dentro del trabajo.

DEFINICIÓN 3 Matriz de Cifrado(Ψ*): Es una matriz de tamaño 8×8 la cual almacena todos los carácteres de* Ω.

[3]Las insignias son observaciones de gran importancia para el desarrollo del trabajo

DEFINICIÓN 4 Transformación discreta de Baker[4].

Sea N en conjunto N={0,1,2..,n-1} de números enteros y sea λ *un conjunto de enteros,* $\lambda=\{\lambda_1, \lambda_2, ..., \lambda_k\}$, *que satisface las siguientes propiedades:*

- $\lambda_1 + \lambda_2 + ... + \lambda_k = n$.
- $\lambda_i \mid n \ \forall \ i \in \{1,2,...,k\}$

Definimos la transformación discreta de Baker $T_{N,\lambda} : N \times N \longmapsto N \times N$ *de la siguiente manera:*

$$T_{N,\lambda}(x,y) = [q_i(x - \sigma_i) + y \ mod \ q_i, \frac{1}{q_i}(y - y \ mod \ q_s) + \sigma_i \tag{1}$$

De donde $\sigma_1 := 0$ *y* $\sigma_i := \lambda_1 + ... + \lambda_{i-1}$ *para* $2 \leq i < k$, $q_i := \frac{n}{\lambda_i}$ *y* $(x,y) \in [\sigma_i, \sigma_i + \lambda_i) \times N$.

Sin embargo al utilizar la transformación (1) en nuestro sistema no genero los resultados esperados; por ello siguiendo el esquema planteado por Jiri [Fri97] de la forma en la cual se debe proceder para trabajar el mapa de Baker sobre una matriz se ha planteado la siguiente definición alterna:

DEFINICIÓN 5 Transformación discreta de Baker II :

Sea N en conjunto N={0,1,2..,n-1} de números enteros y sea λ *un conjunto de enteros,* $\lambda=\{\lambda_1, \lambda_2, ..., \lambda_k\}$, *que satisface las siguientes propiedades:*

- $\lambda_1 + \lambda_2 + ... + \lambda_k = n$.
- $\lambda_i \mid n \ \forall \ i \in \{1,2,...,k\}$

Definimos la transformación discreta de Baker $B_{N,\lambda} : N \times N \longmapsto N \times N$ *de la siguiente manera:*

$$B_{N,\lambda}(x,y) = (n - \sigma_i - \lfloor \frac{n - (x+1)}{q_i} \rfloor - 1, \frac{y - \sigma_i}{q_i} + [n - (x+1)] \ mod \ q_i) \tag{2}$$

De donde $\sigma_1 := 0$ *y* $\sigma_i := \lambda_1 + ... + \lambda_{i-1}$ *para* $1 \leq i < k$, $q_i := \frac{n}{\lambda_i}$ *y* $(x,y) \in N \times [\sigma_i, \sigma_i + \lambda_i)$.

Según Jiri[Fri97] la transformación $B_{N,\lambda}$ permuta la matriz como se sigue. Dada una matriz cuadrada de dimensión N se divide en $\mid \lambda \mid$ matrices de tamaño $N \times \lambda_i$, cada una de las cuales a su vez es dividida en λ_i matrices de dimensión $\frac{N}{\lambda_i} \times \lambda_i$ con N elementos, llamaremos a estas últimas cajas, la propuesta de Jiri[Fri97] es dada una caja se debe proceder de forma forma análoga al mapa de Baker columna a columna. En ejemplo para una matriz de 8×8 es el siguiente. Supongase el conjunto λ={1,2,4,1}.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Una vez aplicamos la transformación $B_{8,\lambda}$ obtenemos.

Un aspecto importante para el trabajo es la dimensión de la matriz de cifrado, llevandonos a la siguiente insignia.

INSIGNIA 2 El sistema tendrá un excelente desempeo para N tales que el número de divisores sea máximo.

[4] Algunos autores también se refieren como Permutaciones de Bernoulli.

64	56	48	40	32	24	16	8
12	4	13	5	14	6	15	7
28	20	29	21	30	22	31	23
44	36	45	37	46	38	47	39
60	52	61	53	62	54	63	55
26	18	10	2	27	19	11	3
58	50	42	34	59	51	43	35
57	49	41	33	25	17	9	1

Para validar esta insignia se realizaron pruebas con matrices cuya dimensión era un número primo dando como resultado que tan solo se generaban dos matrices para cualquier cantidad arbitraria de mensajes.

A este punto contamos con las herramientas necesarias para hablar del proceso que se sigue para generar la matriz de cifrado, para ello nos apoyamos de la noción de *función iterada*, que consiste en evaluar k-veces la función sobre si misma $f^k = f \circ ... \circ f$; un ejemplo, para (k=3) $f^3 = f(f(f(x)))$. La matriz de cifrado es generada en los siguientes pasos.

- Por medio del mensaje de entrada se genera el valor u.
- Se evalua la transformación de Baker iterando sobre ella u veces, $B^u_{N,\lambda}(\Psi)$.

De donde el valor u es obtenido de la siguiente manera.

$$u := (\alpha_1 * (1 \ mod \ q) + \alpha_2 * (2 \ mod \ q) + ... + \alpha_j(n \ mod \ q)) \ mod \ j$$

Donde $q \approx 18 * N$.

Para medir la sensibilidad del sistema frente a pequeos cambios, fueron ejecutadas 1000 pruebas con distintas permutaciones sobre un mensaje x obteniendo que se generaba la misma matriz de cifrado con una probabilidad del 0.05. El mensaje usado en las pruebas fue el siguiente.

"Los indigenas, que llegaron luciendo sus pinturas, plumas, arcos y flechas tradicionales, descendieron pacificamente del techo del Congreso poco despues, recorrieron la gran avenida donde se encuentran los ministerios y luego se sumaron a varios cientos de manifestantes anti Copa y del movimiento de los Sin Techo que marchaban hacia el estadio."

Para la función de cifrado f_{encryp} se requieren tres valores α, ϕ y ρ, los cuales son el carácter a cifrar, el contador de iteraciones y el número de iteraciones que se realizarán al carácter α respectivamente.

El algoritmo de cifrado va a estar determinado por la posición del carácter α en la matriz de cifrado, cada nueva posición x_1 estaba dada por la ecuación basada en el fractal de Collatz (**) biblografía (**) siguiente:

$$x_1 = \begin{cases} \frac{x}{2} & \text{si } x \text{ es par} \\ 3x + 1 & \text{si} x \text{es impar} \end{cases}$$

Sea x_1 la coordenada x o y de α en la matriz de cifrado.

El valor de ρ es aleatorio, elegido en el rango de [0,81), dicho valor representa la cantidad de iteraciones que se harán al carácter α, el cuál será necesario para la función de decifrado. Después de cada iteración el valor de ϕ (siempre empezará en 0) aumentará en 1, el algoritmo se dentendrá cuando ϕ y ρ sean iguales. Se podría decir que un valor puede salirse de la dimensión de nuestra matriz (y lo hace) por lo que realizamos una modificación:

$$x_1 = \begin{cases} \frac{x}{2} \bmod 9 & \text{si } x \text{ es par} \\ (3x + 1) \bmod 9 & \text{si x es impar} \end{cases}$$

El módulo en base 9 nos permite que cada coordenada siempre esté dentro de nuestra matriz de cifrado. Al hacer esto notamos que al aplicar la función f_{encryp} algunos valores llegaban al mismo destino; 1, 7 y $8 = 4$, 2 y $3 = 1$, por lo que decidimos hacer un casteo de los valores que causaban conflicto para poder obtener una función biyectiva (condición inicial de nuestra función f_{encryp}).

5. Transmisión del mensaje

Al igual que la función de encriptación la tranmisición final del mensaje representa uno de los puntos críticos para el SCF. Al abordar esta tarea es necesario preguntarnos e intentar centrar nuestra discusión en las siguientes dos preguntas:

- ¿Qué información transmitir?
- ¿Cómo la información tramsmitida puede afectar la seguridad y validez del SCF?

En la introducción al trabajo hablamos de la limitación propuesta por Howell [BAM03] sobre el decifrado del mensaje; con el fin de poder tener el control y tener recursos para desarrollar esta labor, se ha decidido que el mensaje final contiene los siguientes elementos.

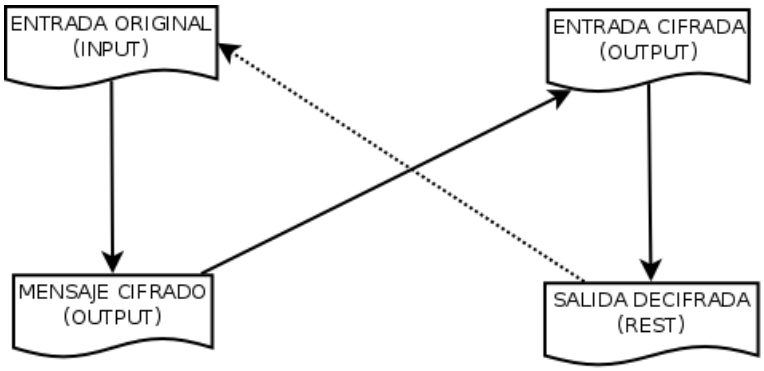
- Matriz de cifrado (Ψ).
- Cadena cifrada de x (x^c).

Previo a la discusión sobre la importancia de estos dos componentes es necesario conocer a forma de la cadena cifrada de x. x^c presentará la siguiente configuración.

μ_1	φ_1	φ_2	μ_2	...
μ_{100}	φ_{100}	φ_{101}	μ_{101}	...

Es decir se transmitiran intercalados la carácteres cifrados y sus respectivas llaves, además de esto las llaves estarán dadas como un carácter de la matriz (Ψ); esto no representa problema alguno ya que como se vio en la función de cifrado la llave tomara los valores [0,N*N).

De ahora en adelante nos referiremos a φ_i como la llave asociada al carácter μ_i. Una vez conocidos los elementos que componen nuestro mensaje final es necesario conocer la importancia de cada uno dentro del proceso de decifrado, recordemos que un buen método de cifrado debe comportarse de la siguiente manera.



La función de Ψ dentro del mensaje final es vital como se menciono en la sección para una cadena x la matriz que se genera puede ser distinta a la de otro mensaje con una probabilidad alta; alguien podria pensar en reconstruir Ψ a partir de x^c sin embargo esta tarea puede representar un imposible dado que las condiciones iniciales de x no existen y como se explico en la sección 4 es necesario conocer x para generar la matriz que le corresponde. Todo lo anterior se resume en la siguiente insignia.

INSIGNIA 3 Para poder conocer x a partir de x^c es necesario conocer Ψ.

Este resultado es importante para evaluar la seguridad del SCF. Al intentar vulnerar un sistema lo primero en lo que podemos pensar es tratar con fuerza bruta procediendo de la siguiente manera, dada

x^c probar con todas las posibles combinaciones para la matriz Ψ, mas este ataque es ejecutado en un tiempo de orden $(h * b)!$, donde h,b representan el número de filas y columnas de Ψ.

La importancia de μ es algo trivial ya que sin este carácter no hay mensaje. Por otra parte la importancia de la llave esta dado el comportamiento de la función de cifrado y las propiedades del fractal, si no se tuviera el valor de esta llave. No se podria aplicar con presición la transformación inversa, se podria intentar con todos los valores desde el 0 hasta el 80 pero esto represente un ataque de fuerza bruta poco eficiente.

6. Algoritmo para el decifrado

7. Conclusiones

Al finalizar el desarrollo del trabajo podemos concluir:

- El desarrollo de un SCF el cual pueda ser utilizado en procesos cotidianos es aún complejo y requiere de bastante investigación sobre la matemática que rigen los cuerpos caóticos y los fractales.

Queremos agradecer de manera especial al profesor Andres Villaveces, por su constante apoyo al trabajo.

Referencias

[A.12] Sáenz Ricardo A. Las matemáticas de los fractales. 2012.

[AD03] Kuperin Yu. A. and Pyatkin D.A. Two-dimensional chaos: The baker map under control. 2003.

[ASMM12] Nadia M. G. Al-Saidi, Mohamad Rushdan Md., and Said Arkan J. Mohammed. Finite and infinite field cryptography analysis and applications. 2012.

[BAM03] Howell Brandi, Reese Anna, and Basile Michael. Fractal cryptology. Technical report, New Mexico High School, New Mexico, 2003.

[CEE91] A.J. Crilly, R.A. Earnshaw, and H. Jones Editores. *Fractals and Chaos*. Springer-Verlag, New York, 1991.

[FJ] Pichler Franz and Scharinger Josef. Finite dimensional generalized baker dynamical systems for cryptographic applications.

[Fri97] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 1997.

[FY07] Huang Feng and Feng Yong. Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm. *Journal of Harbin Institute of Technology*, 2007.

[GI12] Makris George and Antoniou Ioannis. Cryptography with chaos. 2012.

[HW05] Kwok H.S and Tang K.S Wallace. A fast image encryption system based on chaotic maps with finite precision representation. *Chaos, Solitons and Fractals*, 2005.

[Lju01] Kocarev Ljupco. Chaos-bases cryptography: A brief overview. 2001.

[Man89] B.B. Mandelbrot. Fractal geometry: what is it, and what does it do? 1989.

[Mar] Sorando José María. Fractales, geometría del caos.

[Mar04] Churchill Martin. Introduction to fractal geometry. 2004.

[Mig] Reyes Miguel. Fractales.

[Mik05] Ashby Mike. How to write a paper, 2005.

[Ner02] Rubiano O. Gustavo Nervado. *Fractales para Profanos*. Unilibros, Bogotá, 2002.

[NMR09] M.G. Al-Saidi Nadia and Md. Said Muhammad Rushdan. A new approach in cryptographic systems using fractal image coding. 2009.

[oToE] The University of Tokyo and Department of English. In your words or other's.

[PE04] Gutierrez Pablo and Hott Ewaldo. Introducción al mundo fractal, 2004.

[YW11] Ching-Hung Yuen and Kwok-Wo Wong. Chaos-based encryption for fractal image coding. 2011.