(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 628 051**

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2013 PCT/EP2013/077693**

(87) Fecha y número de publicación internacional: **26.06.2014 WO14096363**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2013 E 13815502 (3)**

(97) Fecha y número de publicación de la concesión europea: **08.03.2017 EP 2936302**

(54) Título: **Generador de secuencias caóticas**

(30) Prioridad:

21.12.2012 FR 1262677

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.08.2017

(73) Titular/es:

Université de Nantes (100.0%)
1 quai de Tourville
44000 Nantes, FR

(72) Inventor/es:

EL ASSAD, SAFWAN y
NOURA, HASSAN

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Generador de secuencias caóticas

[0001] La presente invención se refiere a un generador de secuencias caóticas de valores enteros y un procedimiento de generación de secuencias caóticas asociado.

[0002] Más particularmente, la invención se refiere al campo de la seguridad de los datos compartidos, transmitidos y almacenados en las redes de transmisión de informaciones.

[0003] La transferencia de los datos confidenciales (documentos de empresa, informaciones médicas, resultados de búsqueda, informaciones personales de tipo fotos y vídeos, etc.) en un entorno abierto que utiliza los canales usuales de comunicación (cables, Internet, radio-móviles, satélites…) se debe realizar con una seguridad máxima y un rendimiento suficiente. A tal efecto, los cripto-sistemas basados en las señales caóticas son adecuados para conseguir los objetivos citados. Un elemento determinante en todo cripto-sistema basado en el caos es el generador de secuencias caóticas, que sirve para la generación de las claves secretas y para el proceso de cifrado/descifrado de los datos en las operaciones de sustitución y de permutación. La confidencialidad de los datos dependerá entre otros del grado del caos (es decir de lo aleatorio) de las secuencias producidas por el generador de las secuencias caóticas utilizado.

[0004] Las secuencias caóticas utilizables en los cripto-sistemas se caracterizan por unas propiedades de longitud de período y de difusión.

[0005] La solicitud de patente WO2011/121218 de Safwan El Assad y Hassan Noura, presenta un generador de secuencias caóticas que permite generar unas secuencias caóticas de longitud muy grande, por tanto de periodicidad insignificante, utilizables en unas aplicaciones criptográficas concretas con un gran nivel de seguridad.

[0006] La presente invención propone un generador que mejora la propiedad de «confusión-difusión» de los generadores de secuencias caóticas, a la vez que tiene una longitud de período suficientemente grande para una aplicación criptográfica con una buena seguridad.

[0007] Según un primer aspecto, la invención se refiere a un generador de secuencias caóticas de números de valores enteros representados en un número de bits predeterminado, estando destinadas dichas secuencias a ser utilizadas especialmente en unos sistemas de encriptación de informaciones basados en clave, constando dicho generador de un número m de medios de aplicación de funciones no lineales. El generador consta, en salida de dichos medios de aplicación de funciones no lineales, de unos medios de combinación aptos para combinar las salidas de dichos medios de aplicación de funciones no lineales por aplicación de una matriz de difusión binaria dada, que permite obtener un número m de salidas, siendo calculado cada valor de salida por una combinación binaria de salidas de dichos medios de aplicación de funciones no lineales.

[0008] De manera ventajosa, el generador propuesto mejora la característica de «confusión-difusión» de las secuencias caóticas generadas, a la vez que se conserva una buena propiedad de periodicidad. Además, un generador según la invención es fácil de aplicar y permite la generación de secuencias caóticas en un tiempo de cálculo bastante rápido comparado con los generadores estándar propuestos por el NIST («National Institute of Standards and Technology»).

[0009] El generador de secuencias caóticas según la invención puede presentar una o varias de las características posteriores, tomadas independientemente o en combinación:

- consta además de unos medios de alteración conectados en salida de unos medios de combinación;
- consta de m medios de alteración, estando conectado un denominado medio de alteración a cada salida de unos medios de combinación;
- un denominado medio de alteración comprende un registro con desplazamiento a reacción;
- dichos medios de aplicación de funciones no lineales constan de unos medios de aplicación de tarjetas caóticas de un primer tipo y unos medios de aplicación de tarjetas caóticas de un segundo tipo;
- los medios de aplicación de tarjetas caóticas de primer tipo y los medios de aplicación de tarjetas caóticas de segundo tipo se alternan;
- las tarjetas caóticas de primer tipo son unas tarjetas caóticas de tipo «skew tent» y las tarjetas caóticas de segundo tipo con unas tarjetas caóticas lineales por fragmentos PWLCM;

- el número de entradas y de salidas de los medios de combinación es igual a uno de los números siguientes: 4, 8, 32, 64.
- los medios de combinación constan, para la obtención de una salida, de un número m de interruptores conectados en salida de unos medios de aplicación de funciones no lineales, un interruptor cerrado correspondiente a la presencia de un elemento igual a uno en la matriz de difusión binaria y un interruptor abierto correspondiente a la presencia de un elemento igual a cero en la matriz de difusión binaria, estando las salidas de dichos interruptores conectadas a una puerta «o exclusivo».

[0010] Según un segundo aspecto, la invención propone un procedimiento de generación de secuencias caóticas de números de valores enteros representados en un número de bits predeterminado, estando destinadas dichas secuencias a ser utilizadas especialmente en unos sistemas de encriptación de informaciones basados en clave, estando caracterizado el procedimiento porque consta de las etapas de:

- aplicación de m funciones no lineales en m valores iniciales dados, que permiten obtener m valores caóticos,
- combinación de m valores caóticos por aplicación de una matriz de difusión binaria, que permite obtener m valores caóticos combinados y
- aplicación de una alteración en al menos una subparte de m valores caóticos combinados.

[0011] Otras características y ventajas de la invención se desprenderán de la descripción que aparece a continuación, a título indicativo y en absoluto limitativo, en referencia a las figuras anexas, entre las que:

- la figura 1 es un sinóptico de un generador de secuencias caóticas según la invención;
- la figura 2 es un sinóptico que ilustra una aplicación de medios de combinación para la generación de una salida combinada y
- la figura 3 es un organigrama que ilustra las principales etapas de una realización de un procedimiento de generación de secuencias caóticas según la invención.

[0012] La figura 1 ilustra un generador de secuencias caóticas 2 según la invención, que permite generar m secuencias de valores enteros $X_i(n),\ 1 \leq i \leq m$, donde n es un entero y cada valor $X_i(n)$ se representa en un número N de bits predeterminado, por ejemplo N=32, lo que permite obtener una precisión finita de cálculo, independientemente de la plataforma material en la que se implementa el generador. Preferentemente, N es una potencia de dos. Las m secuencias generadas son combinables, si es necesario, en una sola secuencia de números caóticos $S = \{X_1(1),..., X_m(1), X_1(2),..., X_m(2),...X_j(i)...\}$. Las secuencias generadas se pueden utilizar en diversos cripto-sistemas que utilizan unos números pseudo-aleatorios, especialmente para unos procesos de cifrado/descifrado aplicados para asegurar unos datos compartidos, transmitidos y almacenados, pero igualmente para unas aplicaciones de esteganografía, de marca de agua digital y de generación de claves secretas.

[0013] El generador 2 de números caóticos toma como entrada inicialmente un conjunto de m condiciones iniciales $X_1(0)$, $X_2(0)$,..., $X_m(0)$, que definen los valores iniciales o simientes para n=0.

[0014] El generador 2 consta de m medios de aplicación de una función no lineal señalados como 4, 6, 8, 10. Los medios de aplicación de una función no lineal comprenden unos circuitos que aplican la función $x\log(x)$ o $x\exp[\cos(x)]$, o una tarjeta de Chebyshev, o una tarjeta «skew tent» o incluso una tarjeta caótica lineal por fragmentos o PWLCM («piecewise linear chaotic map»). Las funciones no lineales F_i () asociadas a cada entrada $X_i(n)$ se detallan a continuación en una realización preferida.

[0015] Preferentemente, los medios de aplicación de funciones no lineales de diferentes tipos se utilizan, a fin de maximizar la propiedad de difusión de la secuencia caótica generada.

[0016] En particular, según una realización preferida, los medios de aplicación de función no lineal están basados en tarjetas caóticas de dos tipos alternadas de una entrada en la entrada siguiente. Se ha constatado que una alternancia entre unas tarjetas caóticas «skew tent» de función no lineal $F_1()$ y unas tarjetas caóticas de tipo PWLCM de función no lineal $F_2()$ da muy buenos resultados. Sin pérdida de generalidad, la función $F_1()$ se aplica para $X_i(n\text{-}1)$ donde i es impar y la función $F_2()$ se aplica para $X_i(n\text{-}1)$ donde i es par.

[0017] La función no lineal $F_1()$ basada en una tarjeta caótica de tipo «skew tent», llamada tarjeta caótica de primer tipo, es la siguiente:

$$F_1(X(n-1)) = \begin{cases} \left\lceil \frac{2^N \times X(n-1)}{P} \right\rceil & \text{si } 0 \le X(n-1) \le P \\ \left\lfloor 2^N \times \frac{2^N - X(n-1)}{2^N - P} \right\rfloor + 1 & \text{si } P < X(n-1) \le 2^N \end{cases}$$

[0018] Donde ⌜Z⌝ denota el entero más pequeño superior a Z (función «ceil»), y ⌞Z⌟ denota el entero mayor inferior a Z (función «floor»). El parámetro P es dicho parámetro de control discreto y es tal como $0 < P < 2^N - 1$, y N es el número de bits en el que se representa un valor $X(n)$ de la secuencia caótica. El parámetro P de control se codifica en este caso igualmente en N bits.

[0019] La función no lineal F_2 () basada en una tarjeta caótica de tipo PWLCM discretizada, llamada tarjeta caótica de segundo tipo, es la siguiente:

$$F_2(X(n-1)) = \begin{cases} \left\lfloor 2^N \times \frac{X(n-1)}{P} \right\rfloor & \text{si } 0 \le X(n-1) < P \\ \left\lfloor 2^N \times \frac{(X(n-1) - P)}{2^{N-1} - P} \right\rfloor & \text{si } P \le X(n-1) \le 2^{N-1} \\ F_2(2^N - X(n-1)) & \text{si } X(n-1) \ge 2^{N-1} \end{cases}$$

con un parámetro de control P tal como $0 < P < 2^{N-1}$. El parámetro P de control se codifica en este caso en N-1 bits.

[0020] Como variante, se utiliza otra alternancia de las tarjetas caóticas de tipo «skew tent» y de tipo PWLCM.

[0021] Así, cada función no lineal utilizada se define, en esta realización, por su tipo y por un parámetro P asociado.

[0022] Según incluso otra variante, más de dos tipos de tarjetas caóticas se utilizan, por ejemplo tres o cuatro tarjetas caóticas alternadas sucesivamente en las entradas del generador 2 de secuencias caóticas.

[0023] Las salidas $X'_i(n) = F_i(X_i(n-1))$ después de la aplicación de las funciones no lineales seleccionadas se suministran en la entrada de unos medios de combinación 20, aptos para aplicar una matriz de difusión binaria de dimensión mxm.

[0024] Cada salida $Y_i(n)$ de los medios de combinación 20 se calcula a partir de $X'_j(n)$, $j = 1,...,m$ y de la matriz de difusión $D_{i,j}$ del siguiente modo: $Y_i(n) = D_{i,j} \otimes X'_j(n)$, $j = 1,...,m$, donde el símbolo $\otimes$ designa la operación de combinación descrita más en detalle a continuación.

[0025] Las salidas de los medios de combinación 20, en mismo número que las entradas (m) son alteradas por unos medios de generación de secuencias de alteración señaladas como 22, 24, 26 y 28, que son unos registros de desplazamiento a reacción («linear feedback shift register»).

[0026] En esta realización, cada salida i de unos medios de combinación 20 se altera por adición, por medio de funciones «o exclusivo» 30, 32, 34, 36, de una secuencia binaria de alteración suministrada por cada registro de desplazamiento 22, 24, 26, 28, que permite obtener un valor caótico $X_i(n)$.

[0027] Los registros de desplazamiento 22, 24, 26, 28 son aptos para aplicar m polímeros primitivos de grados respectivos k_i, i=1,...,M. Cada registro de desplazamiento genera una secuencia de alteración $Q_i(n)$ representada en k_i bits.

[0028] Cada registro de desplazamiento se caracteriza por una buena función de auto-correlación, una distribución casi uniforme, un ciclo de longitud máxima igual a $2^{ki} - 1$ y una implementación informática o material

fácil.

[0029] Como variante, una alteración se aplica solo a un subconjunto de las salidas $Y_i(n)$ de los medios de combinación 20.

[0030] Los valores de salida $X_i(n)$ se suministran de nuevo en las entradas de los medios de aplicación de funciones no lineales, a fin de generar una nueva serie de m valores caóticos.

[0031] La figura 2 ilustra una aplicación de los medios de combinación que permiten generar un valor de salida $Y_i(n)$. Como se ilustra en la figura 2, la generación de un valor de salida $Y_i(n)$ se obtiene potencialmente a partir del conjunto de los valores de entrada $X_1(n\text{-}1),..., X_m(n\text{-}1)$. Las referencias de los elementos comunes con los de la figura 1 se reanudan.

[0032] Así, el generador 2 aplica primero los medios de aplicación de funciones no lineales a cada uno de los valores de entrada $X_1(n\text{-}1),..., X_m(n\text{-}1)$. Las salidas $X'_i(n)$ se suministran a unos interruptores 40, 42, 44, 46, cuya posición abierta o cerrada varía en función del valor de la matriz de difusión binaria aplicada por los medios de combinación 20.

[0033] Por ejemplo, en el caso en que m=4, la matriz de difusión aplicada es por ejemplo la matriz siguiente:

$$MD4 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

[0034] Para el cálculo aplicado a $X'_3(n)$, los interruptores 40, 44 y 46 están cerrados y el interruptor 42 está abierto.

[0035] De manera más general, estando la matriz de difusión MDm de tamaño mxm compuesta por elementos $D_{i,j}$, un interruptor aplicado a la salida de los medios de aplicación de la función no lineal para la entrada $X_j(n\text{-}1)$ está abierto si $D_{i,j}=0$ y cerrado si $D_{i,j}=1$. Una subparte determinada por los valores Di,j de la matriz de difusión está combinada por un «o exclusivo» 48 aplicado bit a bit, que permite obtener un valor combinado $Y_i(n)$ representado en N bits.

[0036] Así, resulta evidente que los medios de combinación 20 son fáciles de implementar por unos interruptores y unas puertas «o exclusivo», lo que permite generar unos cálculos rápidos.

[0037] Así, en salida, los medios de combinación 20 generan unos valores de muestras combinados:

$$Y_i(n) = D_{i,j} \otimes X'_j(n), \quad j = 1,...,m$$

[0038] Donde $D_{i,j}$ es un elemento de la matriz de difusión binaria como se explica más arriba, $X_i'(n)$ es la salida de los medios de aplicación de función no lineal $F_i()$ aplicados y el símbolo $\otimes$ representa la operación de combinación.

[0039] Preferentemente, como se ilustra en el ejemplo de matriz de difusión dado más arriba para m=4, la matriz de difusión MDm es una matriz tal que $MDm^{-1} = MDm$, lo que facilita la implementación de la operación de descifrado en una aplicación de un generador de secuencias caóticas en un cripto-sistema basado en clave dinámica.

[0040] En una realización, m=8 y se utiliza preferentemente la matriz de difusión MD8 siguiente:

$$MD8 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

[0041] En otra realización, m=16 y se utiliza preferentemente la matriz de difusión MD16 siguiente:

$$MD16 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

[0042] Cabe destacar que para una aplicación por cálculo algorítmico de la matriz de difusión binaria MD16 anterior, es posible realizar unos cálculos intermedios de términos comunes en varias salidas. Este reagrupamiento permite disminuir igualmente el número de puertas «o exclusivo» que se va a aplicar en una implementación material. No obstante, una implementación material simple, basada en 96 puertas «o exclusivo es suficientemente rápida para la aplicación de los medios de combinación 20.

[0043] En otra realización, m=32 y la matriz de difusión MD32 propuesta se construye aplicando el

procedimiento descrito por Koo *et al* en el artículo «On constructing of a 32x32 binary matrix as a diffusion layer for a 256-bit block cipher», publicado en Proceedings ICISC 2006, edición Springer Verlag LNCS 4296, páginas 51-64.

[0044] En este artículo, se propone generar una matriz de difusión para unas aplicaciones criptográficas a partir de la ecuación siguiente:

$$MD32 = Mod(L_l \times M_m \times L_l^t, 2)$$

Donde $L_l^t = L_l$.

[0045] Las matrices L y M se definen del siguiente modo:

$$L_l = \begin{bmatrix} B_{1,1} & B_{1,2} & \cdots & B_{1,8} \\ B_{2,1} & B_{2,2} & \cdots & B_{2,8} \\ \vdots & \vdots & \ddots & \\ B_{8,1} & B_{8,2} & \cdots & B_{8,8} \end{bmatrix} \quad o \quad B_{i,j} = \begin{cases} I_{4x4} & \text{si } h_{i,j} = 1 \\ O_{4x4} & \text{si } h_{i,j} = 0, \ h_{i,j} \in H_l \end{cases}$$

[0046] Con I_{4x4} la matriz identidad de tamaño 4x4, O_{4x4} la matriz cero de tamaño 4x4, y:

$$H_l = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

[0047] La matriz M_m que entra en la construcción de la matriz de difusión binaria es:

$$M_m = \begin{bmatrix} H_{m1} & O_{8x8} & O_{8x8} & O_{8x8} \\ O_{8x8} & H_{m2} & O_{8x8} & O_{8x8} \\ O_{8x8} & O_{8x8} & H_{m3} & O_{8x8} \\ O_{8x8} & O_{8x8} & O_{8x8} & H_{m4} \end{bmatrix}$$

[0048] Donde O_{8x8} es la matriz cero de tamaño 8x8 (matriz que solo contiene 0) y las matrices H_{m1} a H_{m4} son

las siguientes:

$$H_{m1}=\begin{bmatrix}0&1&1&1&1&1&1&1\\1&0&1&1&1&1&1&1\\1&1&0&1&1&1&1&1\\1&1&1&0&1&1&1&1\\1&1&1&1&0&1&1&1\\1&1&1&1&1&0&1&1\\1&1&1&1&1&1&0&1\\1&1&1&1&1&1&1&0\end{bmatrix};\ H_{m2}=\begin{bmatrix}1&0&1&1&0&0&0&0\\0&1&1&1&0&0&0&0\\1&1&1&0&0&0&0&0\\1&1&0&1&0&0&0&0\\0&0&0&0&1&0&1&1\\0&0&0&0&0&1&1&1\\0&0&0&0&1&1&1&1\\0&0&0&0&1&1&0&1\end{bmatrix}$$

$$H_{m3}=\begin{bmatrix}1&1&0&1&0&0&0&0\\1&1&1&0&0&0&0&0\\0&1&1&1&0&0&0&0\\1&0&1&1&0&0&0&0\\0&0&0&0&1&1&0&1\\0&0&0&0&1&1&1&0\\0&0&0&0&0&1&1&1\\0&0&0&0&1&0&1&1\end{bmatrix};\ H_{m4}=\begin{bmatrix}1&1&1&1&1&1&1&0\\1&1&1&1&1&1&0&1\\1&1&1&1&1&0&1&1\\1&1&1&1&0&1&1&1\\1&1&1&0&1&1&1&1\\1&1&0&1&1&1&1&1\\1&0&1&1&1&1&1&1\\0&1&1&1&1&1&1&1\end{bmatrix}$$

[0049] Como ya se ha explicado más arriba, independientemente de la elección de m entre los valores 4, 8, 16, 32, las m salidas de medios de combinación 20 se alteran a través de unas secuencias de alteración generadas por unos registros de desplazamiento. Un registro de desplazamiento 26 se representa en la figura 2. La secuencia de alteración se aplica en la salida $Y_i(n)$ por la puerta «o exclusivo» 34.

[0050] Las salidas $Y_i(n)$ para i=1,…,m se alteran en el instante inicial y todos los Δ_i, donde Δ_i es el valor de la órbita caótica sin alteración. La medición de la órbita caótica se efectúa preferentemente según la técnica descrita en la solicitud de patente WO2011/121218.

[0051] Alternativamente, otras técnicas conocidas de medición de órbita caótica se pueden utilizar.

[0052] La alteración aplicada puede escribirse por tanto del siguiente modo, para cada i, de 1 a m:

$$X_i(n)=\begin{cases}Y_i(n) & \text{si } \mathrm{mod}(n,\Delta_i)\neq 0\\ Y_i(n)\oplus \mathrm{mod}\left(Q_i\left(\frac{n}{\Delta_i}+1\right),2^{k_i}\right) & \text{si } \mathrm{mod}(n,\Delta_i)=0\end{cases}$$

[0053] Donde el símbolo $\oplus$ representa la operación «o exclusivo».

[0054] La ecuación anterior muestra que la alteración se aplica en los k_i últimos bits de peso reducido de $Y_i(n)$ en los instantes $n = lx\Delta_i$, l = 0,1,.....

[0055] Para el valor m=32, se aplican los siguientes polinomios g_i, siendo aplicado un polinomio g_i por el

registro de desplazamiento aplicado para alterar la secuencia $Y_i(n)$:

$$g_1(x) = x^{15} + x^{13} + x^{10} + x^1 + 1$$
$$g_2(x) = x^{17} + x^3 + x^2 + x^1 + 1$$
$$g_3(x) = x^{19} + x^5 + x^2 + x^1 + 1$$
$$g_4(x) = x^{23} + x^{12} + x^5 + x^4 + 1$$
$$g_5(x) = x^{21} + x^2 + 1$$
$$g_6(x) = x^{17} + x^7 + x^4 + x^3 + 1$$
$$g_7(x) = x^{15} + x^9 + x^4 + x^1 + 1$$
$$g_8(x) = x^{19} + x^9 + x^8 + x^7 + x^6 + x^3 + 1$$
$$g_9(x) = x^{21} + x^{14} + x^7 + x^2 + 1$$
$$g_{10}(x) = x^{15} + x^7 + x^4 + x^1 + 1$$
$$g_{11}(x) = x^{17} + x^{16} + x^3 + x^1 + 1$$
$$g_{12}(x) = x^{21} + x^{13} + x^5 + x^2 + 1$$
$$g_{13} = x^{15} + x^{14} + x^{12} + x^2 + 1$$
$$g_{14} = x^{15} + x^{13} + x^{10} + x^9 + 1$$
$$g_{15} = x^{23} + x^5 + x^4 + x^1 + 1$$
$$g_{16} = x^{17} + x^{12} + x^6 + x^3 + x^2 + x + 1$$
$$g_{17} = x^{15} + x^{13} + x^9 + x^6 + 1$$
$$g_{18} = x^{21} + x^{14} + x^7 + x^6 + x^3 + x^2 + 1$$

$$g_{19} = x^{21} + x^{10} + x^6 + x^4 + x^3 + x^2 + 1$$

$$g_{20} = x^{23} + x^{17} + x^{11} + x^5 + 1$$

$$g_{21} = x^{15} + x^{14} + x^9 + x^2 + 1$$

$$g_{22} = x^{17} + x^9 + x^8 + x^6 + x^4 + x^1 + 1$$

$$g_{23} = x^{15} + x^{13} + x^{12} + x^{10} + 1$$

$$g_{24} = x^{21} + x^8 + x^7 + x^4 + x^3 + x^2 + 1$$

$$g_{25} = x^{15} + x^{12} + x^3 + x^1 + 1$$

$$g_{26} = x^{17} + x^8 + x^7 + x^6 + x^4 + x^3 + 1$$

$$g_{27} = x^{19} + x^{13} + x^8 + x^5 + x^4 + x^3 + 1$$

$$g_{28} = x^{15} + x^{13} + x^7 + x^4 + 1$$

$$g_{29} = x^{21} + x^{14} + x^{12} + x^7 + x^6 + x^4 + x^3 + x^2 + 1$$

$$g_{30} = x^{19} + x^{12} + x^{10} + x^9 + x^7 + x^3 + 1$$

$$g_{31} = x^{17} + x^{16} + x^{14} + x^{10} + x^3 + x^2 + 1$$

$$g_{32} = x^{15} + x^1 + 1$$

[0056] En el caso en que m=4,8 o 16, un número m de polinomios primitivos se selecciona en la lista anterior, pudiendo ser efectuada esta selección de forma arbitraria.

[0057] Según una variante no representada, a fin de mejorar incluso los rendimientos del generador caótico según la invención, es posible aplicar la técnica denominada de sub-muestreo, que consiste en iterar la aplicación de los medios de aplicación de función no lineal s veces, con s un entero positivo superior a 3. No obstante, el tiempo computacional se aumenta si se aplica esta variante.

[0058] El generador de secuencias caóticas, descrito más arriba según diferentes realizaciones, permite generar unas secuencias caóticas que tienen buenos rendimientos criptográficos, especialmente unas

probabilidades de bits iguales a 0 y 1 muy próximas a 0,5 para todas las salidas $X_i(n)$, i = 1,...,m.

[0059] Como se explica más arriba, en la realización preferida, se aplica una alternancia de los tipos de tarjetas caóticas que definen las funciones no lineales aplicadas por los medios de aplicación de funciones.

[0060] Así, un generador 2 de secuencia caótica está completamente definido por una clave secreta que consta de: m condiciones iniciales sobre N bits, m/2xN bits para representar los parámetros de las tarjetas caóticas de primer tipo, m/2x(N-1) bits para representar los parámetros de las tarjetas caóticas de segundo tipo, m condiciones iniciales de registros de desplazamiento lo que corresponde como mínimo a mx15bits.

[0061] Así, para esta realización, los tamaños de clave secreta son los siguientes: TK_4=314 bits para m=4, TK_8=628 bits para m=8, TK_{16}=1256 bits para m=16 y TK_{32}=2512 bits para m=32.

[0062] Como se puede constatar, los tamaños de claves son grandes, incluso para un número de entradas igual a 4.

[0063] La figura 3 ilustra las principales etapas de un procedimiento de generación de secuencias caóticas de valores enteros según una realización de la invención. Tal procedimiento se puede implementar por un código informático, ejecutado por una unidad central de un procesador, por ejemplo de un ordenador.

[0064] En entrada 50 del procedimiento se suministran las m condiciones iniciales, que son los valores iniciales $X_1(0),...,X_m(0)$, estando codificado cada valor sobre N bits. Además, los parámetros que permiten definir las funciones no lineales y las alteraciones que se van a aplicar se suministran igualmente en entrada del procedimiento, así como el número Ns de muestras que se van a generar para cada una de las m salidas. Por ejemplo, una clave secreta de formato determinado contiene todas las condiciones iniciales y todos los parámetros en un orden predefinido.

[0065] Una primera etapa de inicialización 52 consiste en inicializar una variable n entera a 1. A continuación, una función no lineal Fi() se aplica a $X_i(n-1)$ en la etapa 54 de generación de números caóticos, para i=1,...,m. Como se explica más arriba, las funciones no lineales son de diferentes tipos según los índices i, por ejemplo una función de primer tipo para los índices impares y una función de segundo tipo para los índices pares. De manera opcional, cada etapa de generación 54 se itera un número s de veces en la etapa 56.

[0066] Un conjunto de m valores caóticos $\{X'_1(n),..., X'_m(n)\}$ se obtiene después de la etapa 56 cuando todos los valores $X_1(n-1)$ se han tratado.

[0067] A continuación, se aplica una etapa 58 de aplicación de matriz de difusión binaria. Una matriz de difusión binaria de tamaño mxm se memoriza, y la aplicación de la matriz consiste en una multiplicación seguida de la aplicación de una operación «o exclusivo» bit a bit, para cada i de i=1 a m, como se explica más arriba en referencia a la figura 2.

[0068] Un conjunto de valores caóticos combinados $\{Y_1(n),..., Y_m(n)\}$ se obtiene después de esta etapa.

[0069] A continuación, una alteración tal como se ha descrito más arriba se aplica a la etapa 60 sobre cada $Y_j(n)$ para obtener un valor $X_j(n)$, para j=1,...,m, y los valores $X_i(n)$ obtenidos se memorizan.

[0070] A continuación, se verifica en la etapa de prueba 62 si n es inferior a Ns, que es el número total de muestras que se van a generar por secuencia, en la etapa 62. Si n es inferior a Ns, la etapa 62 va seguida de la etapa 64 de incremento de n, seguida de la etapa 54 ya descrita.

[0071] Si n es superior a Ns, el procedimiento termina, siendo suministradas las secuencias caóticas $\{X_i(m)\}$ para i=1,..., m y n=1,...Ns en salida de este procedimiento.

[0072] Cabe destacar como variante, que la técnica de alteración solo se aplica a un sub-conjunto de valores caóticos combinados $Y_j(n)$.

[0073] Los inventores han aplicado diversas pruebas definidas por el NIST, denominadas pruebas de NIST, que permiten medir las propiedades de confusión-difusión de las secuencias caóticas generadas y han podido demostrar muy buenas propiedades.

En particular, las probabilidades de los valores 0 y 1 medidas sobre 10000 muestras generadas son muy próximas a 0,5, por tanto la distribución es casi uniforme y la inter-correlación de las secuencias generadas es muy reducida.

[0074] La tabla 1 a continuación ilustra la correlación $\rho(X_i,X_j)$ calculada para Ns=10000 muestras, para m=4:

Tabla 1

Índices	1	2	3	4
1	1	0,00271649	-0,0020199	-0,01118557
2	0,00271649	1	-0,01352033	-0,00860343
3	-0,0020199	-0,01352033	1	0,0083838
4	-0,01118557	-0,00860343	0,0083838	1

[0075] La tabla 2 ilustra las probabilidades de tener unos bits iguales a «0» y a «1», señaladas respectivamente como Pr_0 y Pr_1, en una secuencia caótica de Ns=10000 muestras, para m=4:

Tabla 2

	Pr_0	Pr_1
X_1	0,50049688	0,49950313
X_2	0,50073125	0,49926875
X_3	0,49981875	0,50018125
X_4	0,50096250	0,4990375

[0076] Para demostrar la sensibilidad a la clave secreta, se ha efectuado la prueba siguiente. Para cada entrada de índice i, las condiciones iniciales $X_i(0)$ se han modificado por cambio del bit de peso escaso: $X_i^*(0) = X_i(0) \oplus 1$, y se han generado las salidas respectivas $X_i^*(n)$, para todos los i que van de 1 a m. A continuación, se ha calculado la correlación $\rho(X_i, X_i^*)$, así como la distancia de Hamming PDH entre las secuencias $X_i(n)$ y $X_i^*(n)$:

$$PDH(X_i, X_i^*) = \frac{\sum_{l=1}^{Nsx2^N} X_i(l) \oplus X_i^*(l)}{Ns \times 2^N} \times \%$$

[0077] Donde Ns es el número de muestras probadas. Ns=10000 para los resultados dados en la tabla 3 posterior, y m=4. La distancia de Hamming se expresa en porcentaje.

Tabla 3

	PDH	ρ
X_1	50,0846875	0,00085691
X_2	50,0190625	0,01004383
X_3	49,971875	-0,00973299
X_4	49,9796875	-0,0053712

[0078] Como se puede constatar a partir de las tablas de 1 a 3, se obtienen muy buenos resultados con m=4. Se han obtenido unos resultados mejorados aún para los valores superiores de m, a saber m=8, 16 y 32.

[0079] Así, el generador de secuencias caóticas según la invención permite obtener unas secuencias caóticas con muy buenos rendimientos criptográficos de confusión-difusión, protegidas por unas claves secretas de más de 300 bits, que encuentran unas aplicaciones en todos los campos que necesitan unas secuencias de números pseudo-aleatorios: cifrado por bloque y por flujo, esteganografía, marca de agua digital resistente y generación de claves secretas.

REIVINDICACIONES

1. Generador (2) de secuencias caóticas de números de valores enteros representados en un número de bits predeterminado, estando destinadas dichas secuencias a ser utilizadas especialmente en unos sistemas de encriptación de informaciones basados en clave, constando dicho generador de un número m de medios (4, 6, 8, 10) de aplicación de funciones no lineales, **caracterizado porque** consta, en salida de dichos medios (4, 6, 8, 10) de aplicación de funciones no lineales, de unos medios de combinación (20) aptos para combinar las salidas de dichos medios (4, 6, 8, 10) de aplicación de funciones no lineales por aplicación de una matriz de difusión binaria dada, que permite obtener un número m de salidas, siendo calculado cada valor de salida por una combinación binaria de salidas de dichos medios (4, 6, 8, 10) de aplicación de funciones no lineales, siendo suministrados de nuevo los valores de salida en entrada de los medios de aplicación de funciones no lineales.

2. Generador de secuencias caóticas según la reivindicación 1, **caracterizado porque** consta además de unos medios (22, 24, 26, 28) de alteración conectados en salida de los medios de combinación (20).

3. Generador de secuencias caóticas según la reivindicación 2, **caracterizado porque** consta de m medios (22, 24, 26, 28) de alteración, estando conectado un llamado medio de alteración a cada salida de los medios de combinación (20).

4. Generador de secuencias caóticas según cualquiera de las reivindicaciones 2 o 3, **caracterizado porque** un llamado medio (22, 24, 26, 28) de alteración comprende un registro de desplazamiento a reacción.

5. Generador de secuencias caóticas según cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** dichos medios (4, 6, 8, 10) de aplicación de funciones no lineales constan de unos medios de aplicación de tarjetas caóticas de un primer tipo y unos medios de aplicación de tarjetas caóticas de un segundo tipo.

6. Generador de secuencias caóticas según la reivindicación 5, **caracterizado porque** los medios de aplicación de tarjetas caóticas de primer tipo y los medios de aplicación de tarjetas caóticas de segundo tipo se alternan.

7. Generador de secuencias caóticas según cualquiera de las reivindicaciones 5 o 6, **caracterizado porque** las tarjetas caóticas de primer tipo son unas tarjetas caóticas de tipo «skew tent» y las tarjetas caóticas de segundo tipo son unas tarjetas caóticas lineales por fragmentos PWLCM.

8. Generador de secuencias caóticas según cualquiera de las reivindicaciones anteriores, **caracterizado porque** el número de entradas y de salidas de los medios de combinación es igual a uno de los números siguientes: 4, 8, 32, 64.

9. Generador de secuencias caóticas según cualquiera de las reivindicaciones anteriores, **caracterizado porque** los medios de combinación (20) constan, para la obtención de una salida, de un número m de interruptores (40, 42, 44, 46) conectados en salida de los medios (4, 6, 8, 10) de aplicación de funciones no lineales, un interruptor cerrado correspondiente a la presencia de un elemento igual a uno en la matriz de difusión binaria y un interruptor abierto correspondiente a la presencia de un elemento igual a cero en la matriz de difusión binaria, estando las salidas de dichos interruptores conectadas a una puerta «o exclusivo» (48).

10. Procedimiento de generación de secuencias caóticas de números de valores enteros representados en un número de bits predeterminado, aplicado por un generador de secuencias caóticas según la reivindicación 1, estando destinadas dichas secuencias a ser utilizadas especialmente en unos sistemas de encriptación de informaciones basados en clave, estando el procedimiento **caracterizado porque** consta de las etapas de:

- aplicación (54) de m funciones no lineales en m valores iniciales dados, que permiten obtener m valores caóticos,
- combinación (62) de m valores caóticos por aplicación de una matriz de difusión binaria, que permite obtener m valores caóticos combinados, siendo los valores caóticos combinados suministrados de nuevo como valores iniciales en la etapa de aplicación (54).

11. Procedimiento de generación de secuencias caóticas según la reivindicación 10, **caracterizado porque** consta además de una etapa de aplicación (66) de una alteración en al menos una subparte de los m valores caóticos combinados.

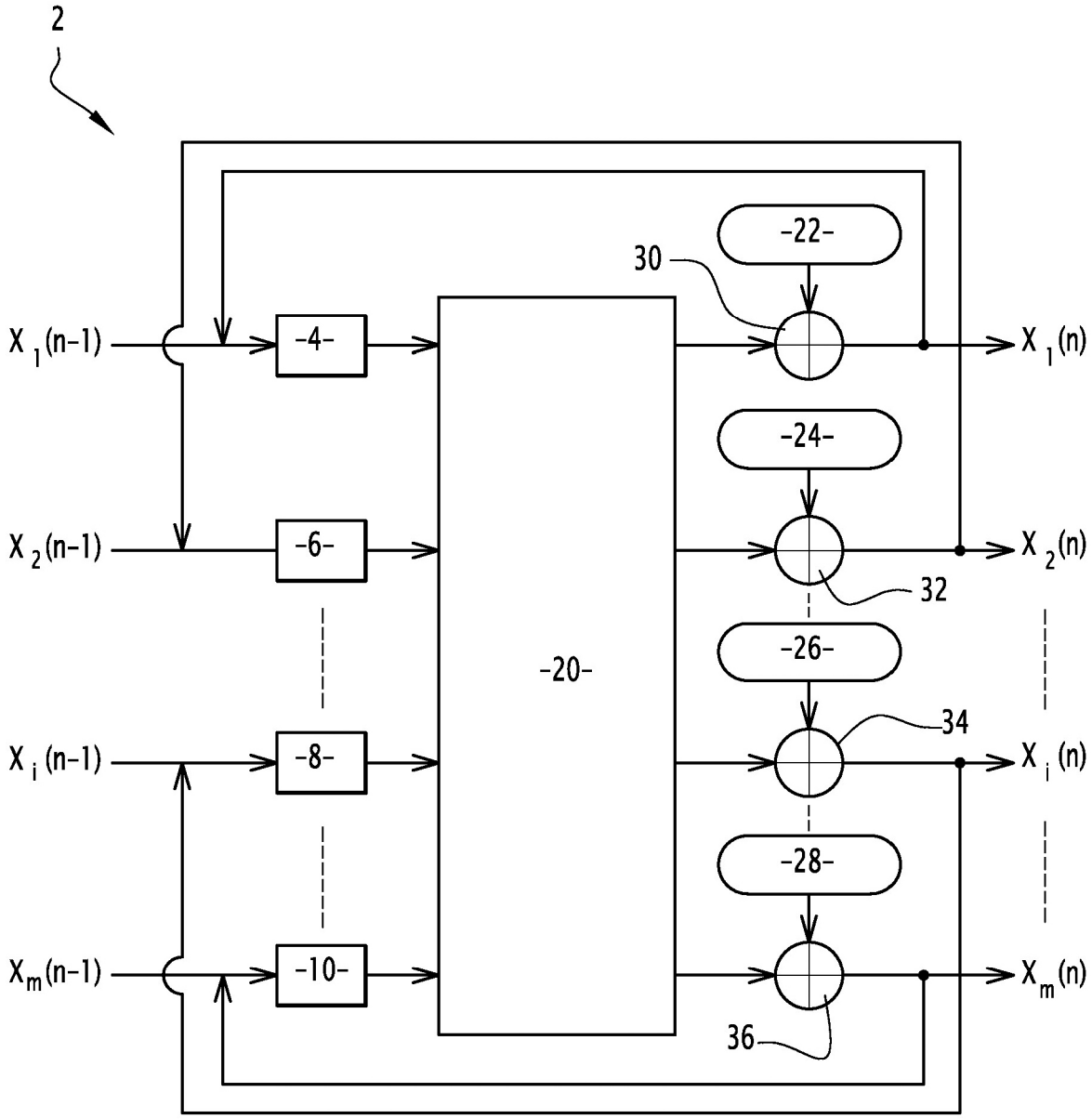
2
-22-
30
X 1(n-1)
-4-
X 1(n)
-24-
X 2(n-1)
-6-
X 2(n)
32
-26-
-20-
34
X i(n-1)
-8-
X i(n)
-28-
Xm(n-1)
-10-
Xm(n)
36

FIG.1

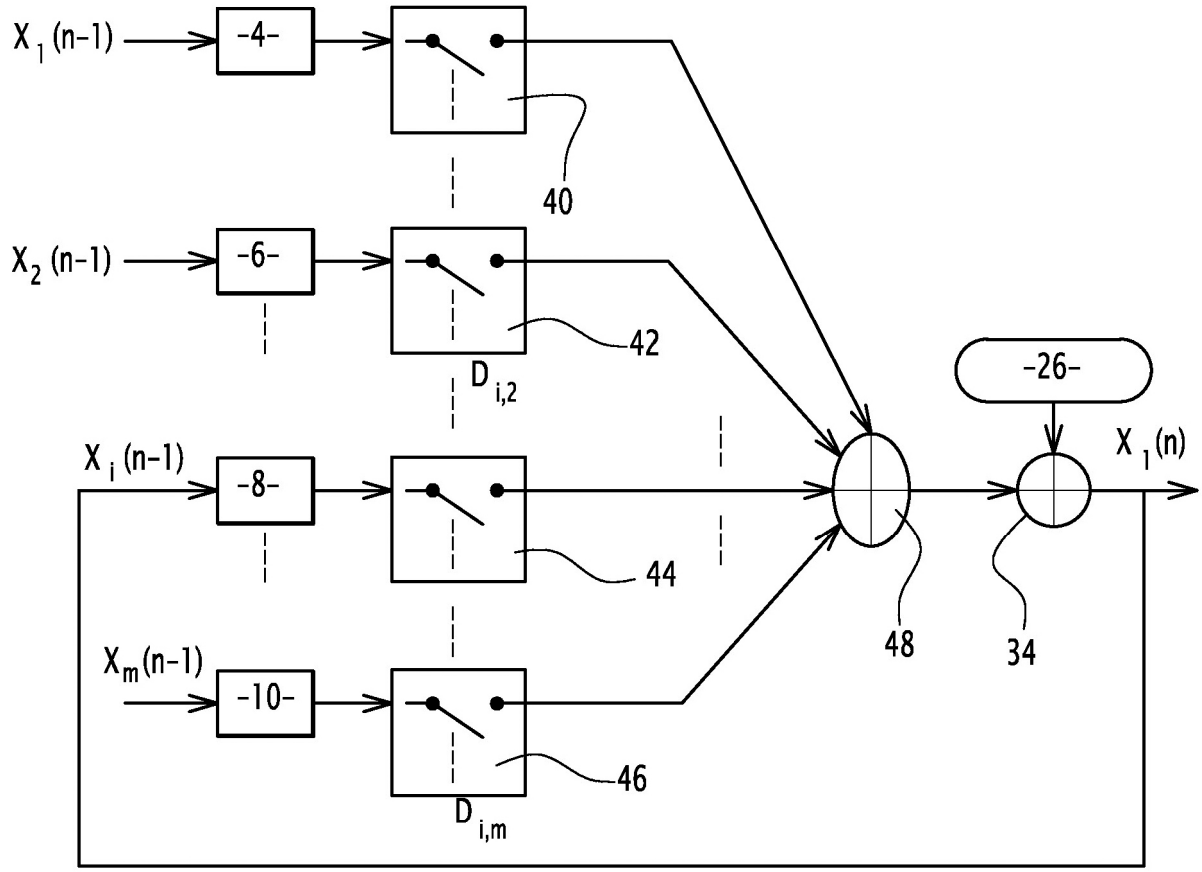

FIG.2

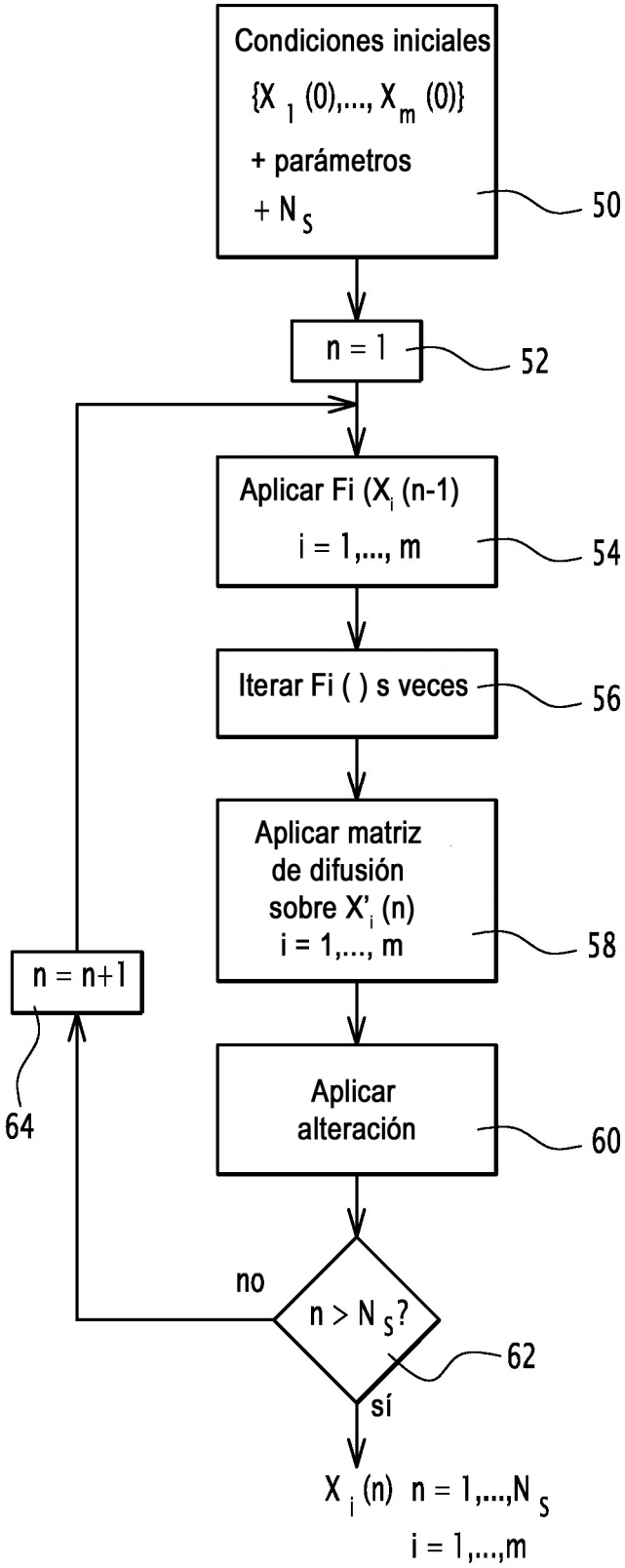
Condiciones iniciales
{X 1 (0),..., X m (0)}
+ parámetros
+ N S
50
n = 1
52
Aplicar Fi (X i (n-1)
i = 1,..., m
54
Iterar Fi ( ) s veces
56
Aplicar matriz
de difusión
sobre X'i (n)
i = 1,..., m
58
Aplicar
alteración
60
n > N S?
62
no
sí
n = n+1
64
X i (n) n = 1,...,N S
i = 1,...,m

FIG.3