(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 724 598**

(21) Número de solicitud: 201930480

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN B2

(22) Fecha de presentación:

30.05.2019

(43) Fecha de publicación de la solicitud:

12.09.2019

Fecha de concesión:

12.03.2020

(45) Fecha de publicación de la concesión:

19.03.2020

(73) Titular/es:

UNIVERSIDAD POLITÉCNICA DE MADRID (50.0%)
Avda. Ramiro de Maeztu, nº 7
28040 MADRID (Madrid) ES y
UNIVERSIDAD DE GUADALAJARA (50.0%)

(72) Inventor/es:

PISARCHIK, Alexander;
REÁTEGUI JAMES, Rider;
RODRIGUEZ FLORES, César y
GARCIA LOPEZ, Juan Hugo

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

(54) Título: **SISTEMA DE COMUNICACIÓN SEGURA BASADO EN MULTI-ESTABILIDAD**

(57) Resumen:

Sistema de comunicación segura basado en multi-estabilidad.

Se divulga un sistema de comunicación segura basado en multi-estabilidad conformado por emisor/receptor basados en osciladores caóticos multi-estables y dos canales de comunicación público/privado. El privado permite sincronizar los osciladores de emisor y receptor. Conmutadores caóticos idénticos en emisor y receptor cambian las condiciones iniciales de los osciladores discretamente con intervalos más cortos que el tiempo de sincronización, funcionando como llaves secretas permitiendo el cambio de los atractores caóticos simultáneamente en los osciladores de emisor y receptor. La información se transmite por el canal público, adhiriendo un número muy grande de paquetes de señal de información en forma escalonada a un número muy grande de señales de enmascaramiento caótico multi-estable dentro de una misma serie temporal. El cambio de los atractores caóticos más rápido que el tiempo de sincronización hace imposible el ataque de sincronización, y además la sincronización de señales caóticas entre el emisor y receptor en cada atractor permite recuperar la señal de información con una alta estabilidad.

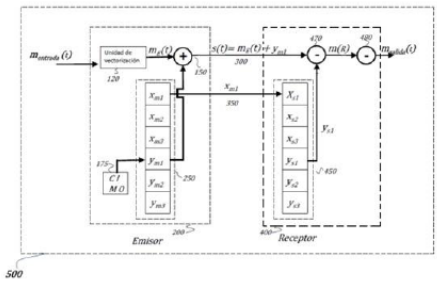

FIG. 5

ES 2 724 598 B2

DESCRIPCIÓN

SISTEMA DE COMUNICACIÓN SEGURA BASADO EN MULTI-ESTABILIDAD

OBJETO DE LA INVENCIÓN.

La presente invención está dirigida a un sistema de comunicación segura basado en multi-estabilidad.

La presente invención está relacionada con el campo de los sistemas de comunicación segura, métodos, dispositivos electrónicos digitales y programas de computador, más específicamente se refiere a un sistema para comunicaciones altamente seguras basado en sistemas dinámicos con coexistencia de múltiples atractores caóticos.

ANTECEDENTES DE LA INVENCIÓN.

Cada vez que se usa una contraseña se está usando criptografía. Cada vez que se realiza una transacción financiera por internet se está usando criptografía. Si se desea tener una llamada segura de voz o video, donde “segura” significa que nadie más que los participantes pueden atender asistir, entonces tienes que usar criptografía. Si se desea escribir un mensaje que solo su destinatario sea capaz de leer y nadie más, es necesario que se mantenga una contraseña entre los participantes de la transmisión de información.

Para mantener alguna información secreta, se usa criptografía. En criptografía se usan mecanismos de codificación o encriptación, por el cual se toma un mensaje inicial, llamado texto-plano y se codifica. Es decir, se cambia el mensaje a alguna cosa que por sí misma no puede ser leída, llamado texto-cifrado. Para leer el texto cifrado, es necesario decodificar este mensaje. Este proceso es llamado decodificación. Este solo debe ser realizado por alguien autorizado. De lo contrario se dice que la codificación ha sido quebrantada. Codificación y decodificación trabajan usando alguna llave de seguridad que es un instrumento para esconder y revelar la información que se desea proteger.

Utilizar tecnologías de cifrado, autenticación y control de acceso a los sistemas de comunicación segura es una solución adecuada para evitar intentos de espionaje y robo de transmisión de datos. Una contribución para resolver este problema es usar señales generadas por componentes que funcionan en el régimen no lineal, tales como osciladores caóticos multi-estables.

En general, los sistemas caóticos muestran repentinos y dramáticos cambios que dan lugar a un complejo comportamiento llamado “caos”. Este comportamiento describe la evolución temporal aperiódico de un sistema. Es decir, nunca se repite y aparentemente es aleatorio, pero completamente determinístico, con una fuerte dependencia a las condiciones iniciales. Un sistema se dice que es determinístico si se conoce la ecuación de evolución temporal, los parámetros que describen al sistema y las condiciones iniciales.

En el estado del arte de sistemas de comunicaciones que usan sistemas caóticos para codificar información se requiere la transmisión de la llave para decodificación de información. Entre las patentes que usan estos métodos podemos mencionar: U.S. Pat. No. 5,048,086 y Weiss U.S. Pat. No. 5,479,512, el cual consiste, en generar una secuencia de números aleatorios en formato digital producidos por un sistema caótico, se le adhiere el mensaje a codificar en formato digital y la señal combinada es transmitida. El receptor extrae el mensaje digital de la señal combinada transmitida usando una llave que genera la misma secuencia de números aleatorios en formato digital, producidos por un sistema caótico. La desventaja de este método es debido a la disminución de la seguridad como resultado de transmisión de la llave o clave.

Una forma de resolver este problema usando sistemas caóticos para seguridad de comunicación donde no se requiere la transmisión de la llave se muestra en las patentes de Carroll U.S. Pat. No. 5,473,694 y Cuomo U.S. Pat. No. 5,291,555. En resumen, este método consiste en modular un parámetro de una señal caótica con una señal que transporta la información o se agrega una señal que lleva información a una señal caótica. La señal caótica resultante se transmite usando tecnologías convencionales de transmisión desde un transmisor que contiene un codificador a un receptor que contiene un decodificador. El decodificador en el receptor sincroniza la señal caótica del receptor con la señal caótica original sin la necesidad de intercambio de llaves. La comparación de la señal caótica resultante con la señal sincronizada permite extraer la información original. Sin embargo, estos sistemas de comunicación

segura que usan sincronización presentan una deficiencia, es decir, si se intercepta la transmisión, es posible reconstruir el espacio de fase para extraer la dinámica subyacente del codificador de transmisión permitiendo extraer la señal de información utilizando otro sistema no lineal generador de caos u otra tecnología.

Por lo que respecta a tecnología patentada en este campo basado en sistemas caóticos, se han localizado innumerables documentos de patentes, por ejemplo, US 7490246 B2, US 2010/007445A1, US 2018/0032475A1, WO 2010/034728 A1, WO 2011/105972 A1, EP1129542B1, US8340295 B2, US 2009/0285395 A1, EP2359519A1, CN103957098B, CN1852089B, CN202362970U, CN106130713A, CN105827393A, CN105744294A, CN104618091A, CN104320241A, CN103532696A, CN103220127A, CN103297221B, CN101345615A, KR198150B1, KR2000009822A, CN107437266A, CN105704500A, CN105634723A, CN105429706A, CN103415009A, US20110002460A1, US20100074445A1.

No obstante, cada una de las referencias tecnológicas encontradas en el estado de la técnica resuelve problemas específicos relacionadas con los puntos antes mencionados en las patentes Carroll U.S. Pat. No. 5473694 y Cuomo U.S. Pat. No. 5291555. Estos sistemas de comunicación segura basados en sincronización de señales caóticas presentan una debilidad contra ataque por sincronización. Sistemas de comunicación segura basados en sincronización usan sistemas no lineales caóticos acoplados en configuración maestro – esclavo, donde el maestro representa un emisor y el esclavo un receptor, la señal de salida del emisor es usada para codificar o enmascarar la señal de información.

El ataque de fuerza bruta por sincronización de estos sistemas de comunicación incluye la intercepción del canal de comunicación y la simulación del receptor por un modelo virtual que ajuste todos los parámetros hasta que se alcance la mejor sincronización o el menor error de sincronización. Cuando el emisor y el receptor virtual alcanzan los mismos valores de parámetros, es cuando se tiene sincronización completa entre estos dos sistemas y la extracción de la señal de información se obtiene comparando la señal sincronizada del receptor virtual con la señal del emisor.

La sensibilidad de sincronización a cambios de parámetros de los sistemas caóticos es muy crucial para la seguridad de la comunicación. Una pequeña variación en uno de estos parámetros puede producir el error de sincronización tan grande que la

recuperación de la señal información sea imposible. A sí mismo, podemos considerar dos tipos de parámetros: grupo de parámetros relacionados con los sistemas no lineales caóticos (emisor-receptor) y el parámetro subyacente al tiempo de sincronización. Siendo el valor umbral este último parámetro primordial para alcanzar sincronización completa. Para valores inferiores a este tiempo de sincronización, no se alcanza la sincronización completa y la recuperación de la información es imposible.

Cuando se implementa el esquema tradicional de comunicación con caos, el oscilador caótico maestro y el oscilador caótico esclavo deben de ser idéntico o uno la contra-parte del otro. Cuando se suma una señal de información pequeña $\boldsymbol{m_E(t)}$ con la señal del oscilador caótico maestro del $\boldsymbol{y_{Emisor}(t)}$ se produce $\boldsymbol{s(t)}$ como $\boldsymbol{s(t) = m_E(t) + y_{Emisor}(t)}$, la cual luego se trasmite al receptor. En el receptor, la señal $\boldsymbol{s(t)}$ se usa para sincronizar el oscilador caótico esclavo con el oscilador caótico maestro, la generación de la señal caótica esclavo $\boldsymbol{y_{Emisor}(t)}$ se dificulta debido a que existe una sincronización incompleta o intermitente la que imposibilita la recuperación de la señal de información $\boldsymbol{m_R}$. Lo anterior es consecuencia del proceso de sumar la información $\boldsymbol{m_E(t)}$ a la señal del oscilador caótica maestro $\boldsymbol{y_{Emisor}(t)}$, convirtiéndolo a este último oscilador no idéntico al oscilador caótico esclavo, y como resultado la dificultad de recuperar la señal de información $\boldsymbol{m_R}$.

Además, los sistemas de comunicación segura basados en sincronización de señales caóticas presentan debilidad contra ataque de sincronización. El ataque de sincronización de estos sistemas de comunicación incluye la intercepción del canal de comunicación y la simulación del receptor por un modelo virtual que ajuste todos los parámetros hasta que se alcanza la mejor sincronización o el menor error de sincronización es alcanzada. El error de sincronización se logra cuando el tiempo de sincronización entre el receptor virtual y el emisor supera un tiempo umbral $\boldsymbol{\tau_k}$ donde el error de sincronización es mínimo. Más concretamente, ataques de sincronización en sistemas de comunicación seguros basados en señales caóticas se describe en los siguientes artículos: *Zanin, M., Sevilla-Escoboza, J. R., Jaimes-Reátegui, R., Garcıa-López, J. H., Huerta-Cuellar, G., & Pisarchik, A. N. (2013). Synchronization attack to chaotic communication systems. Discontinuity, Nonlinearity, and Complexity 2(4) (2013) 333–34; García-López, J. H., Jaimes-Reategui, R., Chiu-Zarate, R., Lopez-Mancilla, D., Jimenez, R., & Pisarchik, A. N. (2008). Secure computer communication based on chaotic Rössler oscillators. Open Electrical & Electronic Engineering Journal, 2, 41-44.*

DESCRIPCIÓN DE LA INVENCION

Para evitar estos inconvenientes, se propone en la presente invención un nuevo sistema de comunicación que usa una llave privada dinámica cambiante que opera en un canal privado y otro llave estática. El canal privado es realizado por una de las variables de estado del emisor que comunica o acopla adecuadamente con el receptor y produce una sincronización completa dinámicamente cambiante entre el receptor con el emisor.

Además, la presente invención resuelve el inconveniente de ataque de sincronización, al implementar en el canal de comunicación privada un método novedoso de sincronización dinámicamente cambiante entre el receptor y el emisor por medio de los atractores múltiples caóticos coexistentes en el oscilador maestro. Lo anterior, se materializa usando diferentes variaciones o cambios en forma caótica de las condiciones iniciales de las variables del mismo oscilador caótico maestro y que funcionan como llaves secretas dinámicas permitiendo el cambio de los atractores en el receptor y en el emisor en forma caótica. El cambio caótico de los atractores caóticos con los intervalos mas cortos que el tiempo de sincronización hace el ataque de sincronización imposible de romper la seguridad de este sistema de comunicación.

Por tanto, el objetivo principal de la presente invención es proponer un sistema de comunicación altamente segura, cuya seguridad se logra con un esquema conformado por un emisor y un receptor basados en sistemas caóticos multi-estables. La “multi-estabilidad” de un sistema dinámico significa que el sistema tiene la coexistencia de un número grande de atractores. Un “atractor” es un conjunto de valores numéricos hacia los cuales un sistema tiende a evolucionar, dada una gran variedad de condiciones iniciales de las variables del estado del sistema. Un “estado de un sistema” dinámico es una solución que permanece confinada en una zona de su espacio de estados o atractor. La sincronización completa es solo posible cuando sistemas dinámicos acoplados son idénticos y se encuentran en el mismo atractor.

En un aspecto de la presente invención se divulga un sistema de comunicación segura basado en multi-estabilidad que comprende un emisor y un receptor que se comunican entre sí a través de un canal público y de un canal privado. De esta forma el emisor recibe una señal de información a transmitir $\boldsymbol{m_E(t)}$, la cual envía codificada ***s(t)***,

mediante atractores coexistentes de enmascaramiento caótico, al receptor por el canal público, y donde el emisor envía una llave dinámica al receptor por el canal privado para la sincronización entre el emisor y el receptor y la decodificación de la señal codificada ***s(t)*** obteniéndose una señal $\boldsymbol{m_{salida}(t)}$ en el receptor igual a la señal $\boldsymbol{m_E(t)}$ de entrada en el emisor.

En una forma de realización, el emisor comprendido en el sistema de comunicación segura basado en multi-estabilidad comprende:

- una unidad de vectorización configurada para recibir una señal de información a transmitir $\boldsymbol{m_E(t)}$, la cual es vectorizada y divida en ***d*** paquetes de información $\boldsymbol{m_E^i(t)}$;
- una unidad generadora de condiciones iniciales donde las condiciones iniciales $\boldsymbol{y_{m1}^i}$ están situadas en el intervalo $\boldsymbol{[y_{m1\_inicial}, y_{m1\_final}]}$;
- un sistema dinámico caótico maestro multi-estable que genera ***d*** atractores caóticos coexistentes de enmascaramiento caótico que varían caóticamente cambiando las condiciones iniciales $\boldsymbol{y_{m1}^i}$ de la variable $\boldsymbol{y_{m1}}$ en las ecuaciones [3] a [6] a través de la unidad generadora de condiciones iniciales y resolviendo las siguientes ecuaciones diferenciales:

$$\frac{dx_{m1}}{dt} = -x_{m2} - x_{m3} \qquad [1]$$

$$\frac{dx_{m2}}{dt} = x_{m2} + ay_{m2} \qquad [2]$$

$$\frac{dx_{m3}}{dt} = b - cx_{m3} + y_{m1}y_{m3} \qquad [3]$$

$$\frac{dy_{m1}}{dt} = x_{m1} - y_{m1} - x_{m2} - x_{m3} \qquad [4]$$

$$\frac{dy_{m2}}{dt} = y_{m1} + ay_{m2} \qquad [5]$$

$$\frac{dy_{m3}}{dt} = b + y_{m3}(y_{m1} - c) \qquad [6]$$

con $\boldsymbol{a = 0.2, b = 0.2}$ y $\boldsymbol{c = 5.7;}$

- una unidad de encriptación configurada para combinar los ***d*** paquetes de información $\boldsymbol{m_E^i(t)}$ con los ***d*** atractores caóticos coexistentes de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$ obteniéndose una señal ***s(t)*** tal que $\boldsymbol{s(t) = y_{m1}(t) + m_E(t)}$, donde la señal ***s(t)*** es enviada a través de un canal público a

un receptor y donde la señal $\boldsymbol{x_{m1}(t)}$ de la ecuación [1] es enviada al receptor mediante un canal privado.

En una forma de realización del emisor de comunicación segura basado en multi-estabilidad, el sistema dinámico caótico maestro multi-estable comprende dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado, donde el comportamiento del primer oscilador queda definido por las ecuaciones diferenciales anteriormente descritas [1] a [3] y el comportamiento del segundo oscilador queda definido por las ecuaciones diferenciales anteriormente descritas [4] a [6].

En una forma de realización del emisor de comunicación segura basado en multi-estabilidad, la unidad generadora de condiciones iniciales modula caóticamente el intervalo $\left[\boldsymbol{y_{m1\_inicial}}, \boldsymbol{y_{m1\_final}}\right]$ a través de un mapa logístico caótico definido por la siguiente ecuación:

$$\boldsymbol{x_{(n+1)}} = \boldsymbol{\mu x_n}(\mathbf{1} + \boldsymbol{x_n}), \qquad [L1]$$

donde $\boldsymbol{x_n}$ está definido en el intervalo $[0, 1]$ y $\boldsymbol{\mu}$ en el intervalo $[0, 4]$, y la modulación de las condiciones iniciales $\boldsymbol{y_{m1\_0}}$ en el intervalo $\left[\boldsymbol{y_{m1\_inicial}}, \boldsymbol{y_{m1\_final}}\right]$ es definido por la siguiente ecuación:

$$\boldsymbol{y_{m1\_0}} = \boldsymbol{y_{m1\_inicial}} + \boldsymbol{x_{n+1}}\left(\boldsymbol{y_{m1\_final}} - \boldsymbol{y_{m1\_inicial}}\right), \qquad [L2]$$

donde $\boldsymbol{x_{n+1}}$ representa la serie temporal del mapa logístico (L1) en el régimen caótico y $\boldsymbol{n + 1}$ son las iteraciones.

En una forma de realización del emisor de comunicación segura basado en multi-estabilidad, se selecciona las ultimas ***d* = 751** iteraciones de la serie temporal $\boldsymbol{x_{n+1}}$, después de transcurridas las 100 primeras iteraciones transitorias.

En una forma de realización del emisor de comunicación segura basado en multi-estabilidad, cada paquete de información ***d*** tiene un tamaño $\boldsymbol{v_p}$ igual a 90 iteraciones y un tiempo de duración $\boldsymbol{t_{me}(t)}$ de 18 segundos.

En una forma de realización, el receptor de comunicación segura basado en multi-estabilidad, comprende:

- una primera unidad de decodificación con una entrada conectada a un canal público para recibir una señal ***s(t)*** procedente del emisor;
- una segunda unidad de decodificación conectada a una salida de la primera unidad de decodificación;
- un sistema dinámico caótico esclavo multi-estable que genera una señal de enmascaramiento caótico esclavo $y_{s1}(t)$ a partir de una señal $x_{m1}(t)$ recibida de un emisor mediante un canal privado, y resolviendo las siguientes ecuaciones diferenciales:

$$\frac{dx_{s1}}{dt} = -x_{s2} - x_{s3} + k(x_{m1} - x_{s1}) \qquad [7]$$

$$\frac{dx_{s2}}{dt} = x_{s2} + ay_{s2} \qquad [8]$$

$$\frac{dx_{s3}}{dt} = b - cx_{s3} + y_{s1}y_{s3} \qquad [9]$$

$$\frac{dy_{s1}}{dt} = x_{s1} - y_{s1} - x_{s2} - x_{s3} \qquad [10]$$

$$\frac{dy_{s2}}{dt} = y_{s1} + ay_{s2} \qquad [11]$$

$$\frac{dy_{s3}}{dt} = b + y_{s3}(y_{s1} - c) \qquad [12]$$

siendo ***k*** el factor de acoplamiento entre el emisor y el receptor;

donde la primera unidad de decodificación sustrae la señal de enmascaramiento caótico esclavo $y_{s1}(t)$ a la señal ***s(t)*** procedente del emisor, obteniéndose una señal de mensaje recuperado $m_R(t)$ que alcanza a la segunda unidad de decodificación que sustrae un error de sincronización $e^i(t)$ a la señal de mensaje recuperado $m_R(t)$ para obtener la señal $m_{salida}(t)$. La señal $m_{salida}(t)$ a la salida del receptor coincide con la señal a la entrada $m_E(t)$ del emisor que se deseaba transmitir entre emisor y receptor de manera codificada.

En una forma de realización del receptor de comunicación segura basado en multi-estabilidad, el sistema dinámico caótico esclavo multi-estable comprende dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado, donde el comportamiento del primer oscilador queda definido por las ecuaciones diferenciales anteriormente descritas [7] a [9] y el comportamiento del segundo oscilador queda definido por las ecuaciones diferenciales anteriormente descritas [10] a [12].

BREVE DESCRIPCION DE LAS FIGURAS

Figura 1 muestra el sistema de comunicación segura usando señales caóticas.

Figura 2 muestra los máximos locales de la variable x_{m1} en función de las condiciones iniciales y_{m1_0}. Cada estado de la variable x_{m1} pertenece a diferente atractor caótico coexistente.

Figura 3(a) muestra el estado de enmascaramiento caótico de la variable $y_{m1}(t)$ en función del tiempo para un atractor caótico.

Figura 3(b) muestra el estado de enmascaramiento caótico de la variable $y_{m1}(t)$ en función del tiempo para otro atractor caótico, usando diferente condición inicial y_{m1_0}.

Figura 4 muestra la variación caótica de las condiciones iniciales y_{m1_0} moduladas por el mapa logístico, ecuación (***L1***).

Figura 5 representa esquemáticamente un sistema de comunicación segura basado en multi-estabilidad ***500*** de acuerdo con la presente invención basada en sistemas caóticos multi estables.

Figura 6 representa la esquemática para cualquier dispositivo electrónico digital de un sistema de comunicación segura basado en multi-estabilidad ***500a*** de acuerdo con la presente invención.

Figura 7(a) muestra una gráfica de una imagen plana.

Figura 7(b) muestra un paquete de señal de información $m_E^i(t)$ versus el tiempo.

Figura 7(c) muestra una porción de la señal de información $m_{Entrada}(t)$ versus el tiempo.

Figura 8(a) muestra un estado de enmascaramiento caótico $y_{m1}^i(t)$ en función del tiempo generada por el sistema caótico maestro ***250a***.

Figura 8(b) muestra la señal de transmisión $s^i(t) = y_{m1}^i(t) + m_E^i(t)$ que es la combinación de un estado de enmascaramiento caótico $y_{m1}^i(t)$ con un paquete de información $m_E^i(t)$ realizada por la unidad de enmascaramiento caótico **150a.**

Figura 8(c) muestra la grafica $s^i(t)$ versus el tiempo, donde se incluye; el tiempo de sincronización τ_s, tiempo requerido para que el sistema caótico esclavo se sincronice con el sistema caótico maestro y el tiempo de transmisión τ_t, tiempo requerido para transmitir cada paquete de información $m_E^i(t)$ enmascarado en cada estado caótico multi estable $y_{m1}^i(t)$.

Figura 8(d) muestra una porción de la señal transmitida $s(t) = y_m(t) + m_E(t)$, correspondiente a un número muy grande de estado de enmascaramiento caótico $y_{m1}(t)$ y a un número muy grande de señales de información $m_E(t)$.

Figura 9(a) muestra un estado de enmascaramiento caótico $\boldsymbol{x_{m1}^{i}(t)}$ versus el tiempo**,** generado por el sistema caótico maestro, ecuaciones ***250a***.

Figura 9(b) muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus el tiempo.

Figura 9(c) muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus la señal $\boldsymbol{y_{m1}^{i}(t)}$**.**

Figura 10(a) muestra la señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ versus el tiempo.

Figura 10(b) representa una porción del mensaje recuperado $m_R(\boldsymbol{t}) = \boldsymbol{e(t)} + \boldsymbol{m_E(t)}$ versus el tiempo.

Figura 11(a) muestra un paquete de señal de mensaje recuperada satisfactoriamente $\boldsymbol{m_{salida}^{i}(t)}$ versus el tiempo.

Figura 11(b) muestra una porción de la señal del mensaje recuperado satisfactoriamente $\boldsymbol{m_{salidd}(t)}$ correspondiente a un número muy grande de señales recuperadas $\boldsymbol{m_{salida}^{i}(t)}$**.**

Figura 12 gráfica una porción de la señal recuperada satisfactoriamente $\boldsymbol{m_{salidad}(t)}$ versus una porción de la señal original $\boldsymbol{m_{entrada}(t)}$**.**

Figura 13 muestra imagen plana recuperada satisfactoriamente.

Figura 14(a) muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus el tiempo, para ejemplo representativo 2.

Figura 14(b) muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus la señal $\boldsymbol{y_{m1}^{i}(t)}$ **,** para ejemplo representativo 2.

Figura 15(a) muestra la señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ versus el tiempo, para ejemplo representativo 2.

Figura 15(b) representa una porción del mensaje recuperado $\boldsymbol{m_R(t)}$ versus el tiempo, para ejemplo representativo 2.

Figura 16(a) muestra un paquete de señal de mensaje recuperada incorrectamente $\boldsymbol{m_{salida}^{i}(t)}$ versus el tiempo, para ejemplo representativo 2.

Figura 16(b) muestra una porción de la señal del mensaje recuperado incorrectamente $\boldsymbol{m_{salidd}(t)}$**,** para ejemplo representativo 2.

Figura 16(c) representa una porción de la señal recuperada incorrectamente $\boldsymbol{m_{salidad}(t)}$ versus una porción de la señal original $\boldsymbol{m_{entrada}(t)}$ **,** para ejemplo representativo 2**.**

Figura 17 muestra una imagen plana recuperada incorrectamente, para ejemplo representativo 2.

Figura 18 representa un sistema de comunicación segura ***500b*** que puede ser implementada en cualquier sistema electrónico digital, para ejemplo representativo 3.

Figura 19(a) muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus el tiempo, para ejemplo representativo 3.

Figura 19(b) muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus la señal $\boldsymbol{y_{m1}^{i}(t)}$ **,** para ejemplo representativo 3.

Figura 20(a) muestra la señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ versus el tiempo, para ejemplo representativo 3.

Figura 20(b) representa una porción del mensaje recuperado $\boldsymbol{m_{R}(t)}$ versus el tiempo, para ejemplo representativo 3.

Figura 21(a) muestra un paquete de señal de mensaje recuperada incorrectamente $\boldsymbol{m_{salida}^{i}(t)}$ versus el tiempo, para ejemplo representativo 3.

Figura 21(b) muestra una porción de la señal del mensaje recuperado incorrectamente $\boldsymbol{m_{salidd}(t)}$**,** para ejemplo representativo 3.

Figura 21(c) grafica una porción de la señal recuperada incorrectamente $\boldsymbol{m_{salidad}(t)}$ versus una porción de la señal original $\boldsymbol{m_{entrada}(t)}$**,** para ejemplo representativo 3.

Figura 22 muestra una imagen plana recuperada incorrectamente.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

La implementación de la presente invención está directamente relacionada con el campo de los sistemas de comunicación segura, método, dispositivos electrónicos digitales y programas de computador, más específicamente se refiere a un sistema de comunicación altamente segura basada en sistemas caóticos multi-estables. Adicionalmente, la presente invención puede ser implementada en circuitos electrónicos digitales como en sistemas de comunicación inalámbricas.

Una descripción detallada de la presente invención se presentada a continuación. La presente invención es un sistema de comunicación altamente segura basado en multi-estabilidad, cuya seguridad se logra con un esquema conformado por un emisor y un receptor basados en sistemas caóticos multi-estables. Adicionalmente, la variación caótica de las condiciones iniciales en cualquiera de las variables de estado en el sistema multi-estable sirve como una llave dinámica. La comunicación entre el emisor y el receptor se logra a través de un canal privado y otro canal público. El canal privado se realiza por la variable de estado $\boldsymbol{x_{m1}}$ donde las llaves dinámicas son implementadas y a la vez es usado para sincronización el emisor con el receptor, mientras la señal de información se transmite del emisor al receptor por el canal público, a través de la variable de estado $\boldsymbol{y_{m1}}$.

En general, en concordancia con la presente invención sistemas de comunicación segura usando caos incluye un emisor y un receptor. El emisor incluye al menos un oscilador caótico maestro. Así mismo, el receptor incluye un oscilador caótico esclavo. Además, los osciladores caóticos maestro y esclavo son idénticos o unos es contraparte del otro.

Tanto el emisor como el receptor están comprendidos por dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado. Variando las condiciones iniciales en cualquiera de las variables de estado, el sistema muestra una dinámica multi-estable, desde regímenes (atractores) periódicos y/o caóticos coexistentes. La comunicación entre el emisor y el receptor se logra a través de dos canales: un canal privado y otro público. El canal privado se realiza por la variable de estado $\boldsymbol{x_{m1}}$ y es usado para sincronizar el emisor con el receptor, a la vez sirve como primera llave dinámica, mientras la señal de información es transmitida del emisor al receptor por el canal público, a través de la variable de estado $\boldsymbol{y_{m1}}$. La transmisión de información se realiza adhiriendo un número muy grande de paquetes de señal de información en forma escalonada a un número muy grande de señales de enmascaramiento caótico con los cambios entre los atractores caóticos dentro de una misma serie temporal de la variable de estado $\boldsymbol{y_{m1}}$.

En particular, el emisor comprende un “sistema caótico maestro” correspondiente a dos osciladores caóticos Rössler con acoplamiento no lineal entre sus variables de estado, que genera múltiples atractores caóticos coexistentes. Este “sistema caótico maestro” tiene dos salidas. Una “primera salida” configurada para enviar un numero grande de paquetes de señal de información y transmitirla juntamente con un numero grande de señal enmascaramiento caótico a través de las interrupciones entre atractores caóticos coexistentes por un canal público y una “segunda salida” configurada para transmitir una señal caótica por un canal privado, que funciona como primera llave dinámica y sirve para sincronizar el emisor con el receptor. El emisor tiene una unidad configurada para sumar un número muy grande de señal de enmascaramiento caótico de la primera salida del sistema dinámico caótico con un número muy grande de paquetes de señal de información.

Por su parte, el receptor es estructuralmente la contra-parte del emisor y tiene dos entradas: una “primera entrada” que comunica o acopla a través del canal público el emisor con el receptor y una “segunda entrada” que comunica o acopla a través del

canal privado el emisor con el receptor. El receptor comprende un “sistema caótico esclavo” que es la contra-parte del sistema dinámico maestro del emisor y consiste de dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado. Este sistema dinámico caótico esclavo tiene una entrada que comunica o acopla el emisor y el receptor por el canal privado a través de la segunda señal de salida del sistema caótico maestro, la cual, está configurada para generar un número muy grande de atractores caóticos y sirve para sincronizar el receptor con el emisor.

El sistema caótico maestro y el sistema caótico esclavo pueden operar de una manera sincronizada solo cuando se encuentran en el mismo atractor. Este sistema caótico esclavo tiene una salida configurada para generar una versión de un número muy grande de señales de enmascaramiento caótico a través de interrupciones entre atractores caóticos coexistentes equivalente al número muy grande de señales de enmascaramiento caótico del sistema caótico maestro. Este sistema caótico esclavo tiene una unidad de extracción de un número muy grande de paquetes de señales de información, la cual se realiza restando la versión de número muy grande de paquetes de señales de enmascaramiento caótico del sistema esclavo de la señal transmitida por el canal público.

El emisor comprende un sistema caótico maestro correspondiente a dos osciladores caóticos Rössler con acoplamiento no lineal entre sus variables de estado, que genera señales caóticas multi-estables y que matemáticamente se corresponde con el siguiente conjunto de ecuaciones diferenciales acopladas:

$$\frac{dx_{m1}}{dt} = -x_{m2} - x_{m3} \qquad [1]$$

$$\frac{dx_{m2}}{dt} = x_{m2} + ay_{m2} \qquad [2]$$

$$\frac{dx_{m3}}{dt} = b - cx_{m3} + y_{m1}y_{m3} \qquad [3]$$

$$\frac{dy_{m1}}{dt} = x_{m1} - y_{m1} - x_{m2} - x_{m3} \qquad [4]$$

$$\frac{dy_{m2}}{dt} = y_{m1} + ay_{m2} \qquad [5]$$

$$\frac{dy_{m3}}{dt} = b + y_{m3}(y_{m1} - c) \qquad [6]$$

donde las ecuaciones del [1]-[3] corresponden al primer oscilador caótico maestro Rössler y las ecuaciones [4]-[6] corresponden al segundo oscilador caótico maestro Rössler.

El receptor es estructuralmente la contra-parte del emisor y comprende un sistema caótico esclavo correspondiente a dos osciladores caóticos Rössler con acoplamiento no lineal entre sus variables de estado, que genera la coexistencia de múltiples atractores caóticos y matemáticamente corresponde al siguiente conjunto de ecuaciones diferencias acoplados:

$$\frac{dx_{s1}}{dt} = -x_{s2} - x_{s3} + k(x_{m1} - x_{s1}) \qquad [7]$$

$$\frac{dx_{s2}}{dt} = x_{s2} + ay_{s2} \qquad [8]$$

$$\frac{dx_{s3}}{dt} = b - cx_{s3} + y_{s1}y_{s3} \qquad [9]$$

$$\frac{dy_{s1}}{dt} = x_{s1} - y_{s1} - x_{s2} - x_{s3} \qquad [10]$$

$$\frac{dy_{s2}}{dt} = y_{s1} + ay_{s2} \qquad [11]$$

$$\frac{dy_{s3}}{dt} = b + y_{s3}(y_{s1} - c), \qquad [12]$$

donde las ecuaciones del [7] a [9] corresponden al primer oscilador caótico esclavo Rössler y las ecuaciones [10] a [12] corresponden al segundo oscilador caótico esclavo Rössler.

El primer oscilador caótico esclavo Rössler está configurado para recibir un conjunto de llaves dinámicas secretas a través del término $k(x_{m1} - x_{s1})$ en la ecuación [7], donde k factor de acoplamiento del entre el emisor y el receptor y funciona como llave estática.

Como primer previo proceso, se realiza la generación de atractores múltiples en el intervalo de condiciones iniciales $[y_{m1\_inicial}, y_{m1\_final}]$ correspondiente a la variable de estado y_{m1} del segundo oscilador caótico maestro.

Como segundo previo proceso, se determina en el canal privado $\boldsymbol{k}(\boldsymbol{x_{m1}} - \boldsymbol{x_{s1}})$ en la ecuación [7] el factor de acoplamiento $\boldsymbol{k}$ y el tiempo de sincronización $\boldsymbol{\tau_k}$, donde el receptor se sincroniza completamente con el emisor en cada atractor coexistente.

Como tercer previo proceso, se modula caóticamente el intervalo de condiciones iniciales $[\boldsymbol{y_{m1\_inicial}}, \boldsymbol{y_{m1\_final}}]$ a través de mapa logístico caótico.

Como cuarto previo proceso, se vectoriza la señal de información en paquetes de información equivalente al número de los atractores caóticos.

Cuando los osciladores caóticos maestro-esclavo están comunicados o acoplados por una señal común, estos osciladores pueden operar de una manera sincronizada e incluso cuando inicialmente ambos osciladores están operando en condiciones iniciales diferentes.

En un sistema tradicional de comunicación con caos ***Figura 1***, una pequeña señal de información $\boldsymbol{m_E(t)}$ es combinada con una señal caótica $\boldsymbol{y_{Emisor}(t)}$ para enmascarar, esconder, cifrar, codificar ó encubrir la señal de información $\boldsymbol{m_E(t)}$. En el emisor ó sistema caótico maestro la señal de información $\boldsymbol{m_E(t)}$ y la señal caótica ó señal de enmascaramiento $\boldsymbol{y_{Emisor}(t)}$ son sumadas para producir la señal de transmisión $\boldsymbol{s(t) = m_E(t) + y_{Emisor}(t)}$. La señal $\boldsymbol{s(t)}$ es conocida como señal de información caóticamente enmascarada.

En el receptor o sistema caótico esclavo se recibe la señal $\boldsymbol{s(t)}$ y usa esta señal para generar la señal caótica $\boldsymbol{y_{Receptor}(t)}$ del receptor por sincronización entre el emisor y el receptor. En el receptor se sustrae la señal $\boldsymbol{y_{Receptor}(t)}$ de la señal $\boldsymbol{s(t)}$ para desenmascarar, decodificar, descifrar, extraer o recuperar la señal la señal $\boldsymbol{m_R}$. Matemáticamente es representada como $\boldsymbol{m_R = s(t) - y_{Receptor}}$ o $\boldsymbol{m_R = m_E(t) + y_{Emisor} - y_{Receptor}}$, la cual produce $\boldsymbol{m_R = m_E}$ cuando $\boldsymbol{y_{Emisor}}$ e $\boldsymbol{y_{Receptor}}$ son idénticas.

En los sistemas dinámicos Rössler multi-estables con acoplamiento no lineal, tanto el emisor como el receptor comprenden dos osciladores caóticos Rössler con acoplamiento no lineal entre sus variables de estado. Estos osciladores caóticos son expresados por el siguiente conjunto de ecuaciones diferenciales:

$$\frac{dx_1}{dt} = -x_2 - x_3 \qquad [1]$$

$$\frac{dx_2}{dt} = x_2 + ay_2 \qquad [2]$$

$$\frac{dx_3}{dt} = b - cx_3 + y_1 y_3 \qquad [3]$$

$$\frac{dy_1}{dt} = x_1 - y_1 - x_2 - x_3 \qquad [4]$$

$$\frac{dy_2}{dt} = y_1 + ay_2 \qquad [5]$$

$$\frac{dy_3}{dt} = b + y_3(y_1 - c) \qquad [6]$$

donde $x_1, x_2, x_3, y_1, y_2, y_3$ son variables de estado, con $a = 0.2, b = 0.2$ y $c = 5.7$ son parámetros del sistema funcionando en el régimen caótico cuando los osciladores Rössler están desacoplados y a la vez sirven como llaves estáticas, en la presente invención.

Para demostrar un número grande de atractores coexistentes o multi estabilidad, se varia la condición inicial de una singular variable y_{m1_0} y se encuentra el estado final resolviendo numéricamente el sistema de ecuaciones [1] a [6]. Este proceso se puede implementar electrónicamente o numéricamente.

En la ***Figura 2***, se muestra los máximos locales de la variable x_{m1} en función de las condiciones iniciales y_{m1_0}, que pertenecen a diferentes atractores coexistentes. En esta ***Figura 2,*** se observa regímenes tales como periodo-3, periodo-4, periodo-5, periodo-8 y caos. Toda la gráfica párese un diagrama de bifurcación, pero enfatizamos que el eje de las abscisas no es un parámetro de control pero son condiciones iniciales de la variable de estado y_{m1} de los osciladores acoplados. En ***Figura 2*** se puede distinguir dos etiquetas $y_{m1\_inicial}$ y y_{m1_final}, los cuales representan condición inicial y final, donde el sistema de ecuaciones diferenciales [1] a [6] muestra la coexistencia de múltiples atractores caóticos o multi-estabilidad.

El emisor basado en sistemas caóticos multi-estables comprende un sistema caótico maestro basado en dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado y es descrito por el siguiente sistema de ecuaciones diferenciales [1] – [6]:

$$\frac{dx_{m1}}{dt} = -x_{m2} - x_{m3} \qquad [1]$$

$$\frac{dx_{m2}}{dt} = x_{m2} + ay_{m2} \qquad [2]$$

$$\frac{dx_{m3}}{dt} = b - cx_{m3} + y_{m1}y_{m3} \qquad [3]$$

$$\frac{dy_{m1}}{dt} = x_{m1} - y_{m1} - x_{m2} - x_{m3} \qquad [4]$$

$$\frac{dy_{m2}}{dt} = y_{m1} + ay_{m2} \qquad [5]$$

$$\frac{dy_{m3}}{dt} = b + y_{m3}(y_{m1} - c), \qquad [6]$$

donde x_{m1}, x_{m2}, x_{m3} son variables de estado del primer oscilador caótico maestro y y_{m1}, y_{m2}, y_{m3} son variables de estado del segundo oscilador caótico maestro, con $a = 0.2, b = 0.2$ y $c = 5.7$ son parámetros del sistemas funcionando en el régimen caótico cuando los osciladores Rössler están desacoplados y a la vez sirven como llaves estáticas, en la presente invención.

La señal $x_{m1}(t)$ de la ecuación [1] se usa para comunicar, acoplar o sincronizar el receptor con el emisor y se lleva a cabo mediante el canal privado, que a la vez sirve como primera llave dinámica. Mientras que la señal de enmascaramiento caótico $y_{m1}(t)$ de la ecuación [4], es usada para cifrar, codifica, ocultar o esconder la señal de información $m_E(t)$**.** La señal de trasmisión $s(t)$ resulta de la combinación de la señal información $m_E(t)$ y la señal de enmascaramiento caótico $y_{m1}(t)$. La señal transmitida del emisor al receptor es

$$s(t) = y_{m1}(t) + m_E(t).$$

El emisor incluye un proceso de generación y modulación caótica de las condiciones iniciales y_{m1_0} de la variable de estado y_{m1} de la ecuación [4]. El cambio de las condiciones iniciales y_{m1_0} en el intervalo $[y_{m1\_inicial}, y_{m1\_final}]$ en forma caótica resulta en interrupciones entre los múltiples atractores caóticos coexistentes $y_{m1}(t)$**.** Dos de estos estados son representados en las ***Figuras 3 (a)*** y ***(b).***

El proceso de generación y modulación caótica de las condiciones iniciales y_{m1_0} de la variable de estado y_{m1} se realiza por la unidad generadora de condiciones iniciales **175,** (ver ***Figura 5***), y más concretamente por un mapa logístico que se define la siguiente ecuación en diferencias:

$$x_{(n+1)} = \mu x_n(1 + x_n), \qquad [\mathbf{L1}]$$

donde x_n está definido en el intervalo $[0, 1]$ y μ en el intervalo $[0, 4]$, cuando $\mu = 4$ el mapa logístico muestra un comportamiento caótico.

El cambio de las condiciones iniciales y_{m1_0} en el intervalo $[y_{m1\_inicial}, y_{m1\_final}]$ queda definido por la siguiente ecuación:

$$y_{m1\_0} = y_{m1\_inicial} + x_{n+1}(y_{m1\_final} - y_{m1\_inicial}), \qquad [\mathbf{L2}]$$

donde x_{n+1} representa la serie temporal del mapa logístico [**L1**] en el régimen caótico y $n + 1$ son las iteraciones**.** En la presente invención, se seleccionaron las ultimas $d = 751$ iteraciones de la serie temporal x_{n+1}**,** después de transcurrido las iteraciones transitorias $n_{transitorias} = 100$. Así mismo, en la presente invención está configurada para que las ecuaciones [L1] y [L2] puedan ser implementadas en cualquier sistema electrónico digital. La variación caótica de las condiciones iniciales y_{m1_0} se muestra en la ***Figura 4.***

En la implementación de la presente invención, la ecuación [L2] representa la unidad generadora de condiciones iniciales ***175*** (ver ***Figura 5***). Esta unidad ***175*** (ver ***Figura 5***) genera $d = 751$ condiciones iniciales y_{m1_0}, las cuales son los resultados de modular el intervalo de condiciones iniciales $[y_{m1\_inicial}, y_{m1\_final}]$ por la serie temporal x_{n+1} del mapa logístico caótico [L1]. A su vez, la variable y_{m1} usa estas y_{m1_0} condiciones iniciales para que el sistema dinámico caótico maestro, ecuaciones [1]-[6], generen $d = 751$ señales de enmascaramiento caótico a través de interrupciones entre múltiples atractores caóticos coexistentes; $y_{m1}(t)$ y $x_{m1}(t)$ son transmitidas del emisor al receptor por el canal público y privado respectivamente.

El receptor basado en sistemas caóticos multi-estables de la presente invención comprende un sistema caótico esclavo y es estructuralmente la contra-parte del sistema caótico maestro. Este sistema caótico esclavo está basado en dos osciladores caóticos Rössler con acoplamiento no lineal entre sus variables de estado, que genera multi-estabilidad y matemáticamente queda definido por el siguiente conjunto de ecuaciones diferenciales acopladas:

$$\frac{dx_{s1}}{dt} = -x_{s2} - x_{s3} + k(x_{m1} - x_{s1}) \qquad [\mathbf{7}]$$

$$\frac{dx_{s2}}{dt} = x_{s2} + ay_{s2} \qquad [8]$$

$$\frac{dx_{s3}}{dt} = b - cx_{s3} + y_{s1}y_{s3} \qquad [9]$$

$$\frac{dy_{s1}}{dt} = x_{s1} - y_{s1} - x_{s2} - x_{s3} \qquad [10]$$

$$\frac{dy_{s2}}{dt} = y_{s1} + ay_{s2} \qquad [11]$$

$$\frac{dy_{s3}}{dt} = b + y_{s3}(y_{s1} - c), \qquad [12]$$

donde x_{s1}, x_{s2}, x_{s3} son variables de estado del primer oscilador caótico esclavo y y_{s1}, y_{s2}, y_{s3} son variables de estado del segundo oscilador caótico esclavo, con $a = 0.2, b = 0.2$ y $c = 5.75$ parámetros del sistemas funcionando en el régimen caótico cuando los osciladores Rössler están desacoplados y a la vez sirven como llaves estáticas en la presente invención.

El sistema caótico esclavo del receptor ***450*** (ver ***Figura 5***) comprende un primer oscilador Rössler, el cual está configurado para recibir por el canal privado, la señal $x_{m1}(t)$ del emisor a través del término $k(x_{m1}(t) - x_{s1}(t))$ en la ecuación [7], donde k factor de acoplamiento entre el emisor y el receptor. Es decir, el sistema caótico esclavo del receptor usa la señal $x_{m1}(t)$ de enmascaramiento caótico del maestro para generar la versión de la señal de enmascaramiento caótico esclavo $y_{s1}(t)$ por sincronización entre el emisor y el receptor. Adicionalmente, en el receptor se sustrae $y_{s1}(t)$ de la señal de información $s(t)$ para desenmascarar, decodificar, descifrar, extraer o recuperar la señal $m_R(t)$. Matemáticamente se expresa como:

$$m_R(t) = s(t) - y_{s1} \quad \text{o} \quad m_R(t) = m_E(t) + y_{m1}(t) - y_{s1}(t)$$

la cual produce

$$m_R(t) = e(t) + m_E(t)$$

cuando $y_{m1}(t)$ y y_{s1} son idénticas, siendo $e(t)$ la señal del error de sincronización.

La ***Figura 5*** es una representación esquemática del sistema de comunicación segura basado en multi-estabilidad ***500*** en concordancia con la presente invención basada en sistemas caóticos multi-estables. El sistema ***500*** comprende un emisor ***200*** y un receptor ***400*** que están configurados para transmitir y recuperar por un canal público ***300*** un número muy grande de paquetes de información enmascarados con un número muy grande de atractores caóticos coexistentes, y además trasmite llaves

dinámicas por un canal privado ***350*** diferente al canal público ***300***. El emisor ***200*** está configurado para recibir una señal de información $\boldsymbol{m_{Entrada}(t) = m_E(t)}$, y el receptor ***400*** está configurada para recuperar una señal de información $\boldsymbol{m_{Salidad}(t)}$**.** Además, el emisor ***200*** comprende: un sistema dinámico caótico maestro multi-estable ***250***, una unidad vectorizadora-divisora de información ***120*** y una unidad generadora de condiciones iniciales ***175***. A sí mismo, el receptor **400** comprende un sistema dinámico caótico esclavo ***450*** que es la contra-parte del sistema dinámico caótico maestro multi-estable ***250***. Adicionalmente, el receptor comprende una primera unidad de decodificación o desenmascaramiento ***470*** y una segunda unidad de decodificación o desenmascaramiento ***480***.

En la implementación de la presente invención, el sistema dinámico caótico maestro multi-estable ***250*** del emisor ***200,*** genera un número muy grande de señales de enmascaramiento caótico multi-estables $\boldsymbol{y_{m1}(t)}$ que opera en concordancia con el sistema de ecuaciones [1]-[6]. Además, el sistema dinámico caótico esclavo multi-estable ***450*** del emisor ***400*** esta acoplado por un canal privado con la señal $\boldsymbol{x_{m1}(t)}$ del sistema dinámico maestro ***250*** a través de la expresión $\boldsymbol{k(x_{m1} - x_{s1})}$ ecuación [7] y que por sincronización entre estos dos sistemas esclavo-***450*** y maestro-***250***, genera en lado del sistema esclavo ***450*** un número muy grande de señales de enmascaramiento caótico $\boldsymbol{y_{s1}(t)}$. A sí mismo, el sistema caótico esclavo ***450*** está en concordancia con las ecuaciones [7] a [12].

En la implementación de la presente invención, el emisor ***200*** comprende una unidad de vectorización de información ***120***, la cual vectoriza y divide la señal de información $\boldsymbol{m_E(t)}$, en ***d* = 751** paquetes de información $\boldsymbol{m_E^i(t)}$ y cada paquete comprende un tamaño de $\boldsymbol{v_p}$ **= 90** iteraciones y un tiempo de duración $\boldsymbol{t_{me}(t)}$ **= 18 s**.

El emisor ***200*** está configurado para enmascarar caóticamente cada paquete de información $\boldsymbol{m_E^i(t)}$, usando la señal de cada estado de cada atractor de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$ del sistema caótico maestro ***250***. Además, el emisor ***200*** combina cada paquete de información $\boldsymbol{m_E^i(t)}$, con cada estado de cada atractor de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$ para producir la señal de trasmisión $\boldsymbol{s^i(t) = y_{m1}^i(t) + m_E^i(t)}$ de cada paquete de información.

El sistema caótico maestro ***250*** del emisor ***200*** genera $\boldsymbol{d = 751}$ estados de atractores coexistentes de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ variando caóticamente las condiciones iniciales de la variable $\boldsymbol{y_{m1}^{i}(t)}$ ecuación [4] a través de la unidad generadora de condiciones iniciales ***175***. Cada uno de estos estados de diferentes atractores $\boldsymbol{y_{m1}^{i}(t)}$ comprenden un tiempo de duración de $\boldsymbol{t_{estado} = 70\ s}$, y este a su vez tiene un tamaño de $\boldsymbol{M_{estaado} = 360}$ iteraciones. A sí mismo, cada uno de los atractores $\boldsymbol{y_{m1}^{i}(t)}$ tiene dos tramos; **a)** primer tramo corresponde a un tiempo $\boldsymbol{\tau_s = 52\ s}$ equivalente a $\boldsymbol{t_{mx} = 270}$ iteraciones, siendo $\boldsymbol{\tau_s}$ el tiempo requerido por el sistema caótico esclavo ***450*** del receptor ***400*** para que se sincronice con el sistema caótico maestro ***250*** del emisor ***200***, **b)** segundo tramo o tramo subsecuente al primero, le corresponde a un tiempo $\boldsymbol{\tau_t = 18\ s}$ equivalente a $\boldsymbol{v_p = 90}$ iteraciones, siendo $\boldsymbol{\tau_t}$ el tiempo de transmisión de cada paquete de información $\boldsymbol{m_E^i(t)}$.

La unidad generadora de condiciones iniciales ***175*** del emisor ***200***, genera ***d* = 751** condiciones iniciales y que sirven como llaves dinámicas. Estas condiciones iniciales o llaves dinámicas son usadas en la variable $\boldsymbol{y_{m1}}$ ecuación [4] del sistema caótico maestro ***250***. Estas condiciones iniciales son seleccionadas caóticamente por el mapa logístico operadas por la ecuación [L1]. Esta cantidad de condiciones iniciales ***d* = 751** permite generar ***d* = 751** estados de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ diferentes.

El emisor ***200*** comprende una unidad de encriptación o enmascaramiento ***150*** que está configurada para combinar cada paquete de información $\boldsymbol{m_E^i(t)}$ con cada señal del atractor coexistente de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$. Es decir, una condición inicial es generada por la unidad generadora de condiciones iniciales ***175*** y es utilizada por el sistema caótico maestro ***250*** para generar una señal del enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ en un atractor coexistente. La unidad de enmascaramiento ***150*** combina la señal de información $\boldsymbol{m_E^i(t)}$ con la señal de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ de la siguiente forma. La señal de información $\boldsymbol{m_E^i(t)}$ que tiene $\boldsymbol{v_p = 90}$ iteraciones o un tiempo de duración de $\boldsymbol{\tau_t = 18\ s}$, es sumada al *segundo tramo* de la señal de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ que tiene también $\boldsymbol{v_p = 90}$ iteraciones y un tiempo de duración de $\boldsymbol{\tau_t = 18\ s}$. Subsecuentemente este proceso se vuelve a repetir. Es decir, se genera una nueva condición inicial por la unidad ***175*** y esta nueva condición inicial es utilizada por el sistema caótico maestro ***250*** para generar una nueva señal de enmascaramiento caótico $\boldsymbol{y_{m1}^{i+1}(t)}$ en otro atractor coexistente y luego la unidad de enmascaramiento ***150*** combina la nueva señal de información $\boldsymbol{m_E^{i+1}(t)}$

con la nueva señal de enmascaramiento caótico $\boldsymbol{y_{m1}^{i+1}(t)}$**,** así sucesivamente. La señal combinada $\boldsymbol{s(t) = y_{m1}(t) + m_E(t)}$ es transmitida del emisor ***200*** al receptor ***400*** por el canal público ***300***.

La combinación o suma de cada señal de información $\boldsymbol{m_E^i(t)}$ con la señal de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$, siempre es al segundo tramo de la señal de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$, es decir, después que transcurrió el tiempo de sincronización $\boldsymbol{\tau_s = 52\ s}$ equivalente a $\boldsymbol{t_{mx} = 270}$ iteraciones.

El cambio de cada condición inicial en la unidad ***175*** se realiza después de que cada señal de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$ haya completado $\boldsymbol{M_{estado} = 360}$ iteraciones o $\boldsymbol{t_{estado} = 70\ s}$.

El cambio de las condiciones iniciales o llaves dinámicas se transmie del emisor ***200*** al receptor ***400*** por una segunda señal de enmascaramiento caótico $\boldsymbol{x_{m1}(t)}$ a través del canal privado ***350***. El sistema dinámico caótico esclavo ***450*** del receptor ***400*** usa esta señal $\boldsymbol{x_{m1}(t)}$ para generar la señal de enmascaramiento caótico esclavo $\boldsymbol{y_{s1}(t)}$ por sincronización entre el receptor ***400*** y el emisor ***200***.

El sistema caótico maestro ***250*** y el sistema caótico esclavo ***450*** están configurados en regímenes de sincronización completa, basados en los valores de sus parámetros ***a* = 0.2, *b* = 0.2** y ***c* = 5.7** que operan como llaves estáticas y facilitan la recuperación de la señales de información transmitida $\boldsymbol{m_E(t)}$.

El receptor ***400*** está configurado para recibir la señal transmitida ***s(t)*** por el canal público ***300*** además, está adicionalmente configurado para recibir las condiciones iniciales o llaves dinámicas por una segunda señal de enmascaramiento caótico $\boldsymbol{x_{m1}(t)}$ a través del canal privado ***350***. El receptor ***400*** utiliza el sistema caótico esclavo ***450*** para generar la versión de la señal de enmascaramiento caótico esclavo $\boldsymbol{y_{s1}(t)}$ y elimina las condiciones iniciales o llaves dinámicas desde la señal transmitida ***s(t)*** sustrayendo $\boldsymbol{y_{s1}(t)}$ de ***s(t)*** a través de la primera unidad de desenmascaramiento o desencriptación ***470***. Para una adecuada supresión de las condiciones iniciales o llaves dinámicas, el sistema caótico esclavo ***450*** y el sistema caótico maestro ***250*** deben de estar sincronizados completamente por medio de las llaves estáticas, basados en los valores de sus parámetros ***a* = 0.2, *b* = 0.2** y ***c* = 5.7**. Como resultado de la sustracción de $\boldsymbol{y_{s1}(t)}$ a ***s(t)*** por medio de la primera unidad de

desenmascaramiento o decodificación ***470***, la señal de mensaje enmascarado caótico transmitida ***s(t)*** es transformado en la señal del mensaje recuperado $\boldsymbol{m_R(t)}$.

Específicamente, cada señal del mensaje recuperada $\boldsymbol{m_R^i}$ está conformada por dos tramos: a) Primer tramo corresponde al error de sincronización $\boldsymbol{e^i(t)}$ equivalente al tiempo $\boldsymbol{\tau_s = 52\ s}$ o $\boldsymbol{t_{mx} = 270}$ iteraciones. b) Segundo tramo subsiguiente al primero, le correspondiente una señal de transmisión $\boldsymbol{m_E^i(t)}$, es decir, $\boldsymbol{m_R^i(t) = e^i(t) + m_E^i(t)}$.

En resumen, la operación del emisor ***250*** y del receptor ***450*** pueden ser representados por las siguientes ecuaciones matemáticas:

- $\boldsymbol{s(t) = y_{m1}(t) + m_E(t)}$,
- $\boldsymbol{x_{m1}(t)}$: señal de sincronización del emisor ***250*** y el receptor ***450***,
- $\boldsymbol{m_R(t) = m_E(t) + y_{m1}(t) - y_{s1}(t)}$, donde $\boldsymbol{m_R(t) = e(t) + m_E(t)}$ cuando $\boldsymbol{y_{m1}(t) = y_{s1}(t)}$,

donde:

- $\boldsymbol{s(t)}$: señal de mensaje enmascarado caótico, transmitida por el canal público ***300***,
- $\boldsymbol{x_{m1}(t)}$: señal de condiciones iniciales o llave dinámica transmitida por el canal privado ***350***,
- $\boldsymbol{m_R(t)}$: señal recuperada,
- $\boldsymbol{e(t)}$: error de sincronización.

Adicionalmente, el receptor ***400*** incluye una segunda unidad desenmascaramiento o decodificación ***480***, que está configurada para recuperar la señal de información $\boldsymbol{m_{Salida}(t)}$, por la sustracción $\boldsymbol{e(t)}$ de $\boldsymbol{m_R(t)}$, es decir,

$\boldsymbol{m_{Salidad}(t) = m_R(t) - e(t)}$,

$\boldsymbol{m_{Salidad}(t) = e(t) + m_E(t) - e(t)}$, donde $\boldsymbol{m_{salidad}(t) = m_E(t)}$ o $\boldsymbol{m_{Salidad}(t) = m_{Entrada}(t)}$.

La ***Figura 6*** es una representación esquemática de un dispositivo electrónico digital que implemente el sistema de la presente invención. En términos generales, el dispositivo electrónico digital ***500a*** comprende un emisor ***200a*** y un receptor ***400a*** que están configurados para transmitir y recuperar por un canal público ***300a*** un número muy grande de paquetes de información enmascarados con un número muy grande de atractores caóticos coexistentes, y además trasmite las llaves dinámicas por un canal

privado ***350a*** diferente al canal público ***300a***. El emisor ***200a*** está configurado para recibir una señal de información $\boldsymbol{m_{Entrada}(t)}$, y el receptor ***400a*** está configurado para recuperar una señal de información $\boldsymbol{m_{Salida}(t)}$. Además, el emisor ***200a*** comprende: un sistema caótico maestro multi-estable ***250a***, una unidad vectorizadora-divisora de información ***100a*** y una unidad generadora de condiciones iniciales ***175a***. A sí mismo, el receptor ***400a*** comprende un sistema caótico esclavo ***450a*** que es la contra-parte del sistema dinámico caótico maestro multi-estable ***250a.*** Además, el receptor ***400a*** incorpora la primera unidad de desenmascaramiento o decodificación ***470a,*** que está configurada para suprimir las condiciones iniciales o llaves dinámicas. Al mismo tiempo, el receptor ***400a*** comprende la segunda unidad desenmascaramiento o decodificación ***480a***, que está configurada para recuperar la señal de información $\boldsymbol{m_{salida}(t)}$.

Ejemplos representativos del sistema de codificación-decodificación caótico de señal de información basada en sistemas multi-estables

La ***Figura 7(a)*** es una gráfica de una imagen plana y por técnicas convencionales, los pixeles de esta imagen son convertidos a una señal de información $\boldsymbol{m_{Entrada}(t) = m_E(t)}$ o señal vectorizada. La ***Figura 7(b)*** muestra un paquete de señal de información $\boldsymbol{m_E^i(t)}$ versus el tiempo, realizada por la unidad vectorizadora-divisora de información ***120a.*** La ***Figura 7(c)*** muestra una porción de la señal de información $\boldsymbol{m_{Entrada}(t)}$ versus el tiempo, correspondiente a un número muy grande paquete de señal de información $\boldsymbol{m_E^i(t)}$**.**

A continuación se describen ejemplos representativos que ilustran particulares casos, bajo los cuales, se tienen correctas e incorrectos recuperaciones de la señal de información $\boldsymbol{m_{Entrada}(t)}$. Estos ejemplos representativos corresponden al sistema de comunicación segura basado en multi-estabilidad ***500a*** en concordancia con la presente invención.

Ejemplo representativo 1: mensaje $\boldsymbol{m_{Entrada}(t)}$, recuperado correctamente

Proceso de enmascaramiento o encriptación

En este ejemplo representativo, el sistema caótico maestro ***250a*** del emisor ***200a*** y el sistema caótico esclavo ***450a*** del receptor ***400a*** están configurados para ser idénticos

o similares. Las respectivas llaves estáticas del emisor ***200a*** y el receptor ***400a*** son mostradas en la ***Tabla I.***

Llaves estáticas					
Emisor ***200a***			Receptor ***400a***		
Sistema caótico maestro ***250a***			Sistema caótico esclavo ***450a***		
a	***b***	***c***	***a***	***b***	***c***
0.2	**0.2**	**5.7**	**0.2**	**0.2**	**5.7**

Tabal I: Llaves estáticas del emisor ***200a*** y el receptor ***400a***, correspondientes a los parámetros de los sistemas de ecuaciones [1]-[6] y [7]-[12], para ejemplo, representativo 1: mensaje $\boldsymbol{m_{Entrada}(t)}$, recuperada correctamente.

La ***Figura 8(a)*** muestra un estado de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ en función del tiempo generada por el sistema caótico maestro ***250a***, debido al cambio de una condición inicial producida en la unidad generadora de condiciones iniciales ***175a.*** La ***Figura 8(b)*** muestra la combinación de un estado de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ con un paquete de información $\boldsymbol{m_E^i(t)}$ realizada por la unidad de enmascaramiento caótico ***150a,*** para producir una señal de trasmisión $\boldsymbol{s^i(t) = y_{m1}^{i}(t) + m_E^i(t)}$, la cual es transmitida del emisor ***200a*** al receptor ***400a*** por el canal público ***300a.***

Para esclarecer como es el proceso de encriptación de información con atractores caóticos coexistentes, en la ***Figura 8(c)*** se muestra $\boldsymbol{s^i(t)}$ versus el tiempo. La señal $\boldsymbol{s^i(t)}$ incluye dos tramos: a) Primer tramo: señal $\boldsymbol{s^i(t)}$, el cual corresponde a un tiempo $\boldsymbol{\tau_s = 52\ s}$ equivalente al tiempo requerido por el sistema caótico esclavo para que se sincronice con el sistema caótico maestro**.** b) Segundo tramo: señal $\boldsymbol{s^i(t)}$, el corresponde a un tiempo $\boldsymbol{\tau_t = 18\ s}$ equivalente al tiempo de transmisión de cada paquete de información $\boldsymbol{m_E^i(t)}$ es enmascarado, encriptado en cada atractor caótico coexistente $\boldsymbol{y_{m1}^{i}(t)}$. En esta ***Figura 8(c)*** también se observa el tiempo total $\boldsymbol{t_{estado} = 70\ s}$ de cada atractor caótico coexistente $\boldsymbol{y_{m1}^{i}(t)}$, equivalente a $\boldsymbol{t_{estado} = \tau_s + \tau_t}$**.**

La ***Figura 8(d)*** muestra una porción de la señal transmitida $\boldsymbol{s(t) = y_m(t) + m_E(t)}$**,** correspondiente a un número muy grande de atractores caóticos coexistentes de enmascaramiento caótico $\boldsymbol{y_{m1}(t)}$ y a un número muy grande de señales de información $\boldsymbol{m_E(t)}$**,** que son trasmitidos del emisor ***200a*** al receptor ***400a.***

Proceso de recuperación o de desencriptación

La ***Figura 9(a)*** muestra un estado de enmascaramiento caótico $\boldsymbol{x_{m1}^{i}(t)}$ versus el tiempo**,** generado por el sistema caótico maestro, ecuaciones ***250a***, debido al cambio de una condición inicial producida en la unidad generadora de condiciones iniciales ***175a.*** La señal $\boldsymbol{x_{m1}^{i}(t)}$ es transmitida del emisor ***200a*** al receptor ***400a*** por el canal privado ***350a*** y el sistema caótico esclavo ***450a*** usa la $\boldsymbol{x_{m1}^{i}(t)}$ por sincronización para generar la señal $\boldsymbol{y_{s1}^{i}(t)}$**.** La ***Figura 9(b)*** muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus el tiempo**.** Mientras que la ***Figura 9(c)*** muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus la señal $\boldsymbol{y_{m1}^{i}(t)}$ y en la cual se puede observar una fuerte sincronización completa entre estas señales después de transcurrido el tiempo de sincronización $\boldsymbol{\tau_s}$.

La ***Figura 10(a)*** muestra la señal del mensaje recuperado $\boldsymbol{m_R^i(t)}$ versus el tiempo, como resultado de la sustracción de $\boldsymbol{y_{s1}^{i}(t)}$ de $\boldsymbol{s^i(t)}$ por medio de la primera unidad de desenmascaramiento o decodificación ***470a.*** La señal del mensaje recuperado $\boldsymbol{m_R^i(t)}$ está conformada por un primer tramo correspondiente al error de sincronización $\boldsymbol{e^i(t)}$ y un segundo tramo correspondiente a un paquete de señal de información $\boldsymbol{m_E^i(t)}$**,** es decir $\boldsymbol{m_R^i(t) = e^i(t) + m_E^i(t)}$**.** La ***Figura 10(b)*** representa una porción del mensaje recuperado $\boldsymbol{m_R(t) = e(t) + m_E(t)}$ versus el tiempo, correspondiente a un número muy grande de señales de error de sincronización $\boldsymbol{e^i(t)}$ y a un número muy grande de paquetes de información $\boldsymbol{m_E^i(t)}$**.**

La ***Figura 11(a)*** muestra un paquete de señal de mensaje recuperado satisfactoriamente $\boldsymbol{m_{salida}^i(t)}$ versus el tiempo, como resultado de la sustracción $\boldsymbol{e^i(t)}$ de $\boldsymbol{m_R^i(t)}$ por medio de la segunda unidad de desenmascaramiento o decodificación ***480a.*** La ***Figura 11(b)*** muestra una porción de la señal del mensaje recuperado satisfactoriamente $\boldsymbol{m_{salidd}(t)}$ correspondiente a un número muy grande de señales recuperadas $\boldsymbol{m_{salida}^i(t)}$.

La ***Figura 12*** representa una porción de la señal recuperada satisfactoriamente $\boldsymbol{m_{salidad}(t)}$ versus una porción de la señal original $\boldsymbol{m_{entrada}(t)}$. Esta gráfica muestra en el espacio de estado la sincronización completa entre la señal recuperada y la señal original. La conversión de la señal recuperada satisfactoriamente $\boldsymbol{m_{salidad}(t)}$ a imagen plana es mostrada en la ***Figura 13***.

Las ***Figuras 8 – 13*** muestran una alta correlación entre el proceso de enmascaramiento y recuperación de la señal de información, lo cual le convierte al sistema de comunicación segura ***500a*** de la presente invención en un sistema de comunicación seguro altamente robusto.

Ejemplo representativo 2: mensaje $\boldsymbol{m_{Entrada}(t)}$*, recuperada incorrectamente cuando inadecuadamente las llaves estáticas son implementadas*

Proceso de enmascaramiento o encriptación

En este ejemplo representativo, el sistema caótico maestro ***250a*** del emisor ***200a*** y el sistema caótico esclavo ***450a*** del receptor ***400a*** están configurados para ser completamente diferentes en al menos un parámetro ***a***. Las respectivas llaves estáticas del emisor ***200a*** y el receptor ***400a*** son diferentes y se muestran en la ***Tabla II.***

Llaves estáticas					
Emisor ***200a***			Receptor ***400a***		
Sistema caótico maestro ***250a***			Sistema caótico esclavo ***450a***		
a	***b***	***c***	***a***	***b***	***c***
0.2	**0.2**	**5.7**	**0.3**	**0.2**	**5.7**

Tabal II: Llaves estáticas del emisor ***200a*** y el receptor ***400a***, correspondiente a las parámetros de los sistemas de ecuaciones [1]-[6] y [7]-[12], para el ejemplo representativo 2: mensaje $\boldsymbol{m_{Entrada}(t)}$, recuperada incorrectamente.

La ***Figura 8(a)*** muestra un estado de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}}$ generado por el sistema caótico maestro ***250a***, debido al cambio de una condición inicial producida en la unidad generadora de condiciones iniciales ***175a.*** La ***Figura 8(b)*** muestra la combinación de un atractor de enmascaramiento caótico $\boldsymbol{y_{m1}^{i}(t)}$ con un paquete de información $\boldsymbol{m_{E}^{i}(t)}$ realizada por la unidad de enmascaramiento caótico ***150a*****,** para producir una señal de trasmisión $\boldsymbol{s^{i}(t) = y_{m1}^{i}(t) + m_{E}^{i}(t)}$**,** la cual, es transmitida del emisor ***200a*** al receptor ***400a*** por el canal público ***300a***. La ***Figura 8 (d)*** muestra una porción de la señal transmitida $\boldsymbol{s(t) = y_{m}(t) + m_{E}(t)}$**,** correspondiente a un número muy grande de atractores de enmascaramiento caótico $\boldsymbol{y_{m1}(t)}$ y a un número muy grande de señales de información $\boldsymbol{m_{E}(t)}$**,** que son trasmitidos del emisor ***200a*** al receptor ***400a.***

Proceso de recuperación o de desencriptación

La ***Figura 9(a)*** muestra un estado de enmascaramiento caótico $\boldsymbol{x_{m1}^{i}(t)}$ versus el tiempo**,** generado por el sistema dinámico caótico maestro, ***250a***, debido al cambio de una condición inicial producida en la unidad generadora de condiciones iniciales ***175a.*** La señal $\boldsymbol{x_{m1}^{i}(t)}$ es transmitida del emisor ***200a*** al receptor ***400a*** por el canal privado ***350a*** y el sistema caótico esclavo ***450a*** usa la $\boldsymbol{x_{m1}^{i}(t)}$ por sincronización para generar la señal $\boldsymbol{y_{m1}^{i}(t)}$**.**

La ***Figura 14(a)*** muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus el tiempo**.** Mientras que la ***Figura 14(b)*** muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus la señal $\boldsymbol{y_{m1}^{i}(t)}$ en la cual se puede observar una débil sincronización entre estas señales cuyo espacio de estados $\boldsymbol{y_{s1}^{i}(t)}$ vs $\boldsymbol{y_{m1}^{i}(t)}$ ocupa una amplia región, la cual representa un pobre correlación entre estas señales, es decir, $\boldsymbol{y_{s1}^{i}(t)}$ e $\boldsymbol{y_{m1}^{i}(t)}$ son completamente diferentes. En concordancia con la presente invención, el ejemplo representativo 2 muestra que el sistema de comunicación segura ***500a*** de la presente invención es muy sensible a pequeñas variaciones de sus llaves estáticas; representadas en el sistema dinámico caótico maestro ***250a*** por ***a* = 0.2** y en el sistema caótico esclavo ***450a*** por ***a* = 0.3**. Esta diferencia de las llaves estáticas en el emisor ***200a*** y el receptor ***400a*** dificulta la recuperación de imagen original.

La ***Figura 15(a)*** muestra la señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ versus el tiempo, como resultado de la sustracción de $\boldsymbol{y_{s1}^{i}(t)}$ a $\boldsymbol{s^{i}(t)}$ por medio de la primera unidad de desenmascaramiento o decodificación ***470a.*** La señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ está conformada por un primer tramo correspondiente al error de sincronización $\boldsymbol{e^{i}(t)}$ tiene valores muy grandes y un segundo tramo que es una señal completamente diferente que la señal de información $\boldsymbol{m_{E}^{i}(t)}$**.** La ***Figura 15(b)*** representa una porción del mensaje recuperado $\boldsymbol{m_{R}(t)}$ versus el tiempo, correspondientes un número muy grande de paquetes de información recuperados incorrectamente.

La ***Figura 16(a)*** muestra un paquete de señal de mensaje recuperada incorrectamente $\boldsymbol{m_{salida}^{i}(t)}$ versus el tiempo, como resultado de la sustracción $\boldsymbol{e^{i}(t)}$ de $\boldsymbol{m_{R}^{i}(t)}$ por medio de la segunda unidad de desenmascaramiento o desencriptación ***480a.*** La ***Figura 16(b)*** muestra una porción de la señal del mensaje recuperado incorrectamente $\boldsymbol{m_{salidd}(t)}$ correspondiente a un número muy grande de señales recuperadas incorrectamente $\boldsymbol{m_{salida}^{i}(t)}$.

La ***Figura 16(c)*** muestra una porción de la señal recuperada incorrectamente $\boldsymbol{m_{salidad}(t)}$ versus una porción de la señal original $\boldsymbol{m_{entrada}(t)}$**,** en la cual, se puede observar una débil sincronización entre estas señales y cuyo espacio de estados $\boldsymbol{m_{salidad}(t)}$ vs $\boldsymbol{m_{entrada}(t)}$ ocupa una amplia región, representando un pobre correlación entre estas señales, es decir, $\boldsymbol{m_{salidad}(t)}$ y $\boldsymbol{m_{entrada}(t)}$ son completamente diferentes.

La conversión de la señal recuperada incorrectamente $\boldsymbol{m_{salidad}(t)}$ a imagen plana se muestra en la ***Figura 17,*** la cual es completamente diferente a la imagen plana original ***Figura 7(a)***.

El ejemplo representativo 2 muestra que el sistema de comunicación segura ***500a*** de la presente invención es muy sensible a pequeñas variaciones de sus llaves estáticas. Es decir, una pequeña diferencia de las llaves estáticas en el emisor ***200a*** y el receptor ***400a*** imposibilita la recuperación de imagen original.

Ejemplo representativo 3: mensaje $\boldsymbol{m_{Entrada}(t)}$ *recuperada incorrectamente cuando inadecuadamente se implementan las llaves dinámicas*

En el presente ejemplo representativo 3, las llaves dinámicas son inadecuadamente implementadas. La ***Figura 18*** representa un sistema de comunicación segura ***500b*** que puede ser implementado en cualquier sistema electrónico digital***.*** En este sistema, el canal de comunicación privada que comunica el emisor ***200b*** con el receptor ***400b*** está mal configurado, no es considerado o no existe. En el sistema de comunicación ***500b*** no existe la señal $\boldsymbol{x_{m1}(t)}$ o llaves dinámicas generada por el sistema caótico maestro ***250b*** para ser transmitida por un canal privado que comunique el emisor ***200b*** con el receptor ***400b***, pero a diferencia en el sistema de comunicación segura ***500a*** de la presente invención, este canal privado ***350a*** sí existe o está bien configurado como se ilustra en la ***Figura 6***.

Además, el sistema caótico esclavo ***450b*** del emisor ***400b*** no puede usar la señal $\boldsymbol{x_{m1}(t)}$ del sistema dinámico maestro ***250b*** y por sincronización generar la señal $\boldsymbol{y_{s1}(t)}$. Al no existir sincronización entre el emisor ***200b*** y receptor ***400b***, la señal de enmascaramiento caótico $\boldsymbol{y_{m1}(t)}$ del emisor ***200b*** y la señal de enmascaramiento caótico $\boldsymbol{y_{s1}(t)}$ del receptor **400b** son completamente diferentes, es decir $\boldsymbol{y_{m1}(t) \neq y_{s1}(t)}$.

En el sistema de comunicación segura ***500b***, la señal combinada $\boldsymbol{s(t) = y_{m1}(t) + m_E(t)}$ es transmitida del emisor ***200b*** al receptor ***400b*** por el canal público ***300b***, donde $\boldsymbol{y_{m1}(t)}$ es la señal de enmascaramiento caótico y $\boldsymbol{m_E(t)}$ es la señal de información. Además, en el receptor ***400b*** el mensaje recuperado $\boldsymbol{m_R(t)}$, como resultado de la sustracción de $\boldsymbol{y_{s1}(t)}$ a $\boldsymbol{s(t)}$ por medio de la primera unidad de desenmascaramiento o decodificación ***470a*** es realizada insatisfactoriamente o incorrectamente, esto es debido a que $\boldsymbol{y_{m1}(t) \neq y_{s1}(t)}$ y matemáticamente es representada por

$$\boldsymbol{m_R(t) = s(t) - y_{s1},}$$
$$\boldsymbol{m_R(t) = y_{m1}(t) + m_E(t) - y_{s1},}$$

debido a que $\boldsymbol{y_{m1}(t) \neq y_{s1}(t)}$, la señal recuperada $\boldsymbol{m_R(t)}$ es diferente a la señal $\boldsymbol{m_E(t)}$**.** En este ejemplo representativo 3**,** la omisión de la llave dinámica $\boldsymbol{x_{m1}(t)}$ o carencia del canal de comunicación privada que sincroniza el emisor ***200b*** con el receptor ***400b*** produce que la señal el mensaje original sea insatisfactoriamente recuperada por el receptor ***400b*** del sistema de comunicación segura ***500b.***

Proceso de enmascaramiento o encriptación

En este ejemplo representativo, el sistema caótico maestro ***250b*** del emisor ***200b*** y el sistema dinámico caótico esclavo ***450b*** del receptor **400b** están configurados para ser idénticos. Las respectivas llaves estáticas del emisor ***200b*** y el receptor ***400b*** son semejantes y son mostradas en la ***Tabla I.***

La ***Figura 8(a)*** muestra un estado de enmascaramiento caótico $\boldsymbol{y_{m1}^i}$ generada por el sistema dinámico caótico maestro ***250b***, debido al cambio de una condición inicial-i producida en la unidad generadora de condiciones iniciales ***175a.*** La ***Figura 8(b)*** muestra la combinación de un estado de enmascaramiento caótico-i $\boldsymbol{y_{m1}^i(t)}$ con un paquete de información $\boldsymbol{m_E^i(t)}$ realizada por la unidad de enmascaramiento caótico **150b,** para producir una señal de trasmisión $\boldsymbol{s^i(t) = y_{m1}^i(t) + m_E^i(t)}$**,** la cual, es transmitida del emisor ***200b*** al receptor ***400a*** por el canal público ***300a***. La ***Figura 8 (d)*** muestra una porción de la señal transmitida $\boldsymbol{s(t) = y_m(t) + m_E(t)}$**,** correspondiente a un número muy grande de atractores de enmascaramiento caótico $\boldsymbol{y_{m1}(t)}$ y a un número muy grande de señales de información $\boldsymbol{m_E(t)}$**,** que son trasmitidos del emisor ***200b*** al receptor ***400b.***

Proceso de recuperación o de desencriptación

La ***Figura 19(a)*** muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus el tiempo**.** Mientras que la ***Figura 19(b)*** muestra la señal $\boldsymbol{y_{s1}^{i}(t)}$ versus la señal $\boldsymbol{y_{m1}^{i}(t)}$ en la cual podemos observar una débil sincronización entre estas señales cuyo espacio de estados $\boldsymbol{y_{s1}^{i}(t)}$ vs $\boldsymbol{y_{m1}^{i}(t)}$ ocupa una amplia región, la cual representa un pobre correlación entre estas señales, es decir, $\boldsymbol{y_{s1}^{i}(t)}$ e $\boldsymbol{y_{m1}^{i}(t)}$ son completamente diferentes. En concordancia con la presente invención, el ejemplo representativo 3 muestra que el sistema de comunicación segura ***500b*** es muy sensible a la no existencia de las llaves dinámicas, es decir no existe la señal $\boldsymbol{x_{m1}^{i}(t)}$ o llaves dinámicas del sistema caótico maestro que sincroniza el emisor ***200b*** con el receptor ***400b***. Esta carencia de sincronización del emisor ***200b*** con el receptor ***400b*** realizada por las llaves dinámicas $\boldsymbol{x_{m1}^{i}(t)}$ a través de un canal de comunicación privada dificulta la recuperación de imagen original.

La ***Figura 20(a)*** muestra la señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ versus el tiempo, como resultado de la sustracción de $\boldsymbol{y_{s1}^{i}(t)}$ a $\boldsymbol{s^{i}(t)}$ por medio de la primera unidad de desenmascaramiento o decodificación ***470b.*** La señal del mensaje recuperado $\boldsymbol{m_{R}^{i}(t)}$ está conformada por un primer tramo correspondiente al error de sincronización $\boldsymbol{e^{i}(t)}$ tiene valores muy grandes y un segundo tramo que es una señal completamente diferente que la señal de información $\boldsymbol{m_{E}^{i}(t)}$***.*** La ***Figura 20(b)*** representa una porción del mensaje recuperado $\boldsymbol{m_{R}(t)}$ versus el tiempo, correspondientes un número muy grande de paquetes de información recuperados incorrectamente.

La ***Figura 21(a)*** muestra un paquete de señal de mensaje recuperada incorrectamente $\boldsymbol{m_{salida}^{i}(t)}$ versus el tiempo, como resultado de la sustracción $\boldsymbol{e^{i}(t)}$ de $\boldsymbol{m_{R}^{i}(t)}$ por medio de la segunda unidad de desenmascaramiento o decodificación ***480b.*** La ***Figura 21(b)*** muestra una porción de la señal del mensaje recuperado incorrectamente $\boldsymbol{m_{salidd}(t)}$ correspondiente a un número muy grande de señales recuperadas incorrectamente $\boldsymbol{m_{salida}^{i}(t)}$.

La ***Figura 21(c)*** representa una porción de la señal recuperada incorrectamente $\boldsymbol{m_{salidad}(t)}$ versus una porción de la señal original $\boldsymbol{m_{entrada}(t)}$**,** en la cual podemos observar una débil sincronización entre estas señales y cuyo espacio de estados $\boldsymbol{m_{salidad}(t)}$ vs $\boldsymbol{m_{entrada}(t)}$ ocupa una amplia región, representando un pobre

correlación entre estas señales, es decir, $\boldsymbol{m_{salidad}(t)}$ y $\boldsymbol{m_{entrada}(t)}$ son completamente diferentes.

La conversión de la señal recuperada incorrectamente $\boldsymbol{m_{salidad}(t)}$ a imagen plana se muestra en la ***Figura 22,*** la cual es completamente diferente a la imagen plana original ***Figura 7(a)***.

El ejemplo representativo 3 muestra que el sistema de comunicación segura ***500b*** de la presente invención es muy sensible a la carencia de sus llaves dinámicas, es decir, la no existencia de sincronización entre el emisor ***200b*** y el receptor ***400b*** imposibilita la recuperación de imagen original.

REIVINDICACIONES

1.- Emisor (***200***) de comunicación segura basado en multi-estabilidad, caracterizado porque comprende:

- una unidad de vectorización (***120***) configurada para recibir una señal de información a transmitir $\boldsymbol{m_E(t)}$, la cual es vectorizada y divida en ***d*** paquetes de información $\boldsymbol{m_E^i(t)}$;
- una unidad generadora de condiciones iniciales (***175***) donde las condiciones iniciales $\boldsymbol{y_{m1}^i}$ están situadas en el intervalo $\boldsymbol{[y_{m1\_inicial}, y_{m1\_final}]}$;
- un sistema dinámico maestro multi-estable (***250***) que genera ***d*** atractores caóticos coexistentes de enmascaramiento caótico que varían caóticamente cambiando las condiciones iniciales $\boldsymbol{y_{m1}^i}$ de la variable $\boldsymbol{y_{m1}}$ en las ecuaciones [3]-[6] a través de la unidad generadora de condiciones iniciales (***175***) y resolviendo las siguientes ecuaciones diferenciales:

$$\frac{dx_{m1}}{dt} = -x_{m2} - x_{m3} \qquad [1]$$

$$\frac{dx_{m2}}{dt} = x_{m2} + ay_{m2} \qquad [2]$$

$$\frac{dx_{m3}}{dt} = b - cx_{m3} + y_{m1}y_{m3} \qquad [3]$$

$$\frac{dy_{m1}}{dt} = x_{m1} - y_{m1} - x_{m2} - x_{m3} \qquad [4]$$

$$\frac{dy_{m2}}{dt} = y_{m1} + ay_{m2} \qquad [5]$$

$$\frac{dy_{m3}}{dt} = b + y_{m3}(y_{m1} - c) \qquad [6]$$

con $\boldsymbol{a = 0.2, b = 0.2}$ y $\boldsymbol{c = 5.7}$***;***

- una unidad de encriptación (***150***) configurada para combinar los ***d*** paquetes de información $\boldsymbol{m_E^i(t)}$ con los ***d*** atractores caóticos coexistentes de enmascaramiento caótico $\boldsymbol{y_{m1}^i(t)}$ obteniéndose una señal ***s(t)*** tal que $\boldsymbol{s(t) = y_{m1}(t) + m_E(t)}$**,** donde dicha señal ***s(t)*** es enviada a través de un canal público (***300***) a un receptor (***400***) y donde la señal $\boldsymbol{x_{m1}(t)}$ de la ecuación [1] es enviada al receptor (***400***) mediante un canal privado (***350***).

2.- Emisor (***200***) de comunicación segura basado en multi-estabilidad, según la reivindicación 1, caracterizado porque el sistema dinámico caótico maestro multi-estable (***250***) comprende dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado, donde el comportamiento del primer oscilador queda definido por las ecuaciones [1] a [3] y el comportamiento del segundo oscilador queda definido por las ecuaciones [4] a [6].

3.- Emisor (***200***) de comunicación segura basado en multi-estabilidad, según la reivindicación 1, caracterizado porque la unidad generadora de condiciones iniciales (***175***) modula caóticamente el intervalo $[y_{m1\_inicial}, y_{m1\_final}]$ a través de un mapa logístico caótico definido por la siguiente ecuación:

$$x_{n+1} = \mu x_n(1 + x_n), \qquad [L1]$$

donde x_n está definido en el intervalo $[0, 1]$ y μ en el intervalo $[0, 4]$, y la modulación de las condiciones iniciales y_{m1_0} en el intervalo $[y_{m1\_inicial}, y_{m1\_final}]$ es definido por la siguiente ecuación:

$$y_{m1\_0} = y_{m1\_inicial} + x_{n+1}(y_{m1\_final} - y_{m1\_inicial}), \qquad [L2]$$

donde x_{n+1} representa la serie temporal del mapa logístico (L1) en el régimen caótico y $n + 1$ son las iteraciones.

4.- Emisor (***200***) de comunicación segura basado en multi-estabilidad, según la reivindicación 1, caracterizado porque se selecciona ***d* = 751** iteraciones de la serie temporal x_{n+1}, después de transcurridas las 100 primeras iteraciones transitorias.

5.- Emisor (***200***) de comunicación segura basado en multi-estabilidad, según la reivindicación 1, caracterizado porque cada paquetes de información ***d*** tiene un tamaño v_p igual a 90 iteraciones y un tiempo de duración $t_{me}(t)$ de 18 segundos.

6.- Receptor (***400***) de comunicación segura basado en multi-estabilidad, caracterizado porque comprende:

- una primera unidad de decodificación (***470***) con una entrada conectada a un canal público (***300***) para recibir una señal ***s(t)*** procedente de un emisor (***200***);
- una segunda unidad de decodificación (***480***) conectada a una salida de la primera unidad de decodificación (***470***);

- un sistema dinámico caótico esclavo multi-estable (***450***) que genera una señal de enmascaramiento caótico esclavo $y_{s1}(t)$ a partir de una señal $x_{m1}(t)$ recibida de un emisor (***200***) mediante un canal privado (***350***), y resolviendo las siguientes ecuaciones diferenciales:

$$\frac{dx_{s1}}{dt} = -x_{s2} - x_{s3} + k(x_{m1} - x_{s1}) \qquad [7]$$

$$\frac{dx_{s2}}{dt} = x_{s2} + ay_{s2} \qquad [8]$$

$$\frac{dx_{s3}}{dt} = b - cx_{s3} + y_{s1}y_{s3} \qquad [9]$$

$$\frac{dy_{s1}}{dt} = x_{s1} - y_{s1} - x_{s2} - x_{s3} \qquad [10]$$

$$\frac{dy_{s2}}{dt} = y_{s1} + ay_{s2} \qquad [11]$$

$$\frac{dy_{s3}}{dt} = b + y_{s3}(y_{s1} - c) \qquad [12]$$

siendo ***k*** el factor de acoplamiento entre el emisor (***200***) y el receptor (***400***);
donde la primera unidad de decodificación (***470***) sustrae la señal de enmascaramiento caótico esclavo $y_{s1}(t)$ a la señal ***s(t)*** procedente del emisor (***200***), obteniéndose una señal de mensaje recuperado $m_R(t)$ que alcanza a la segunda unidad de decodificación (***480***) que sustrae un error de sincronización $e^i(t)$ a la señal de mensaje recuperado $m_R(t)$ para obtener la señal $m_{salida}(t)$.

7.- Receptor (***400***) de comunicación segura basado en multi-estabilidad, según la reivindicación 6, caracterizado porque el sistema dinámico caótico esclavo multi-estable (***450***) comprende dos osciladores Rössler con acoplamiento no lineal entre sus variables de estado, donde el comportamiento del primer oscilador queda definido por las ecuaciones [7] a [9] y el comportamiento del segundo oscilador queda definido por las ecuaciones [10] a [12].

8.- Sistema de comunicación segura basado en multi-estabilidad, caracterizado porque comprende un emisor (***200***) definido en una cualquiera de las reivindicaciones 1 a 5, un receptor (***400***) definido en una cualquiera de las reivindicaciones 6 a 8, donde el emisor (***200***) se comunica con el receptor (***400***) a través de un canal público (***300***) y un canal privado (***400***).

9.- Sistema de comunicación segura basado en multi-estabilidad, según la reivindicación 8, caracterizado porque el emisor (***200***) recibe una señal de información a transmitir $\boldsymbol{m_E(t)}$**,** la cual envía codificada ***s(t)***, mediante atractores coexistentes de enmascaramiento caótico, al receptor por el canal público, y donde el emisor envía una llave dinámica al receptor por el canal privado para la sincronización entre el emisor y el receptor y la decodificación de la señal codificada ***s(t)*** obteniéndose una señal $\boldsymbol{m_{salida}(t)}$ igual a $\boldsymbol{m_E(t)}$.

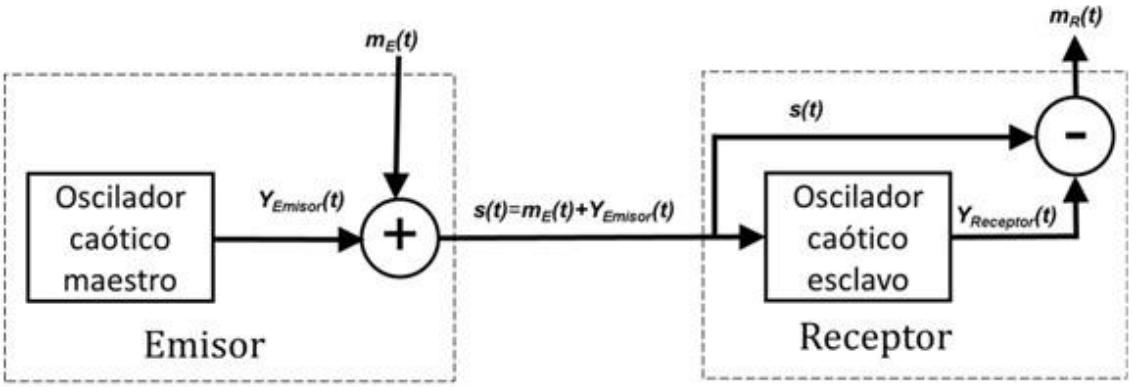
$m_E(t)$
$m_R(t)$
s(t)
Oscilador caótico maestro
$Y_{Emisor}(t)$
$s(t)=m_E(t)+Y_{Emisor}(t)$
Oscilador caótico esclavo
$Y_{Receptor}(t)$
Emisor
Receptor

FIG. 1

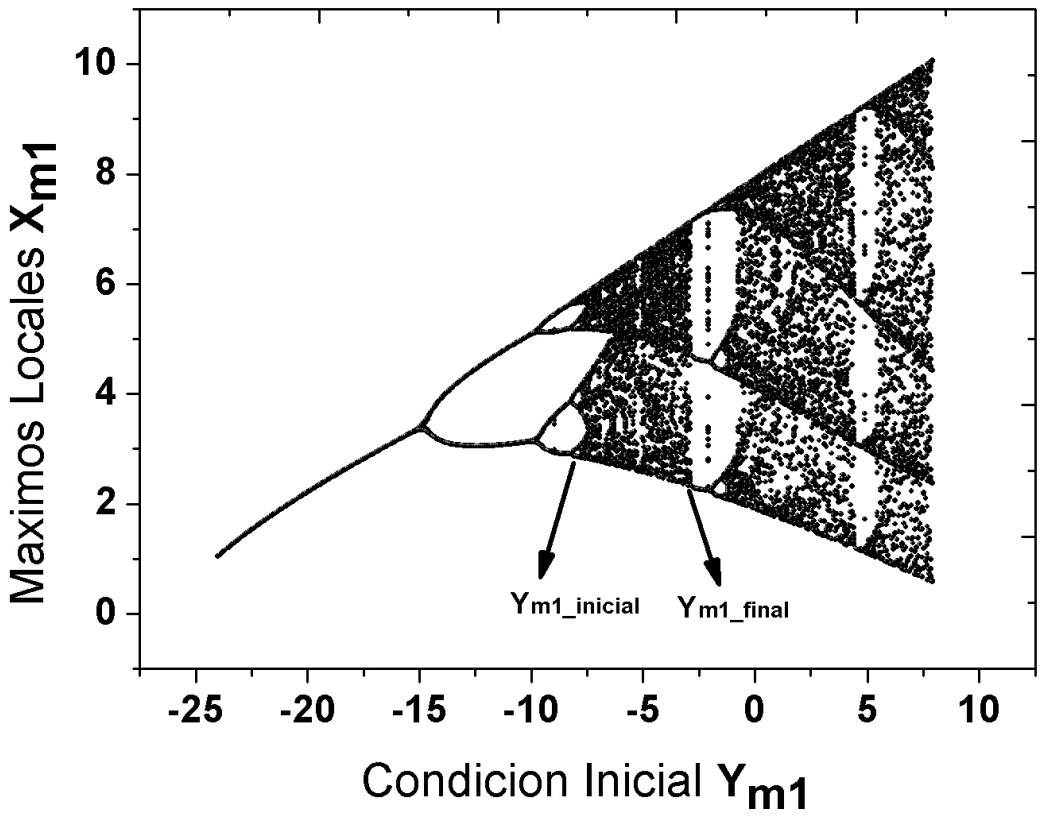
Maximos Locales X_{m1}
Condicion Inicial Y_{m1}
$Y_{m1\_inicial}$
Y_{m1_final}
0
2
4
6
8
10
-25
-20
-15
-10
-5
0
5
10

FIG. 2

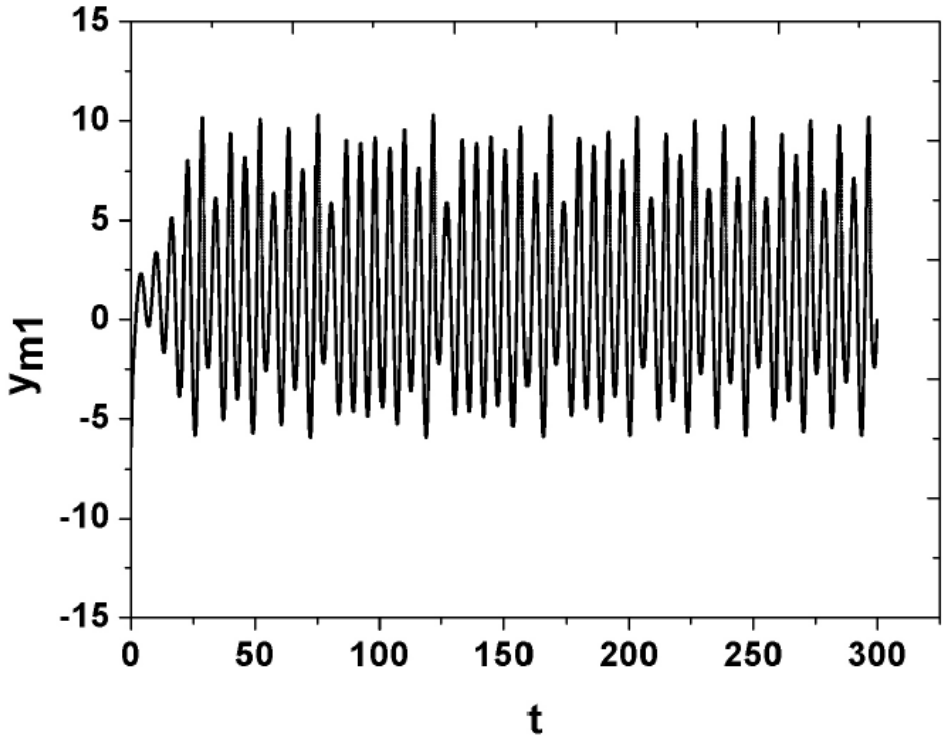
15
10
5
0
-5
-10
-15
ym1
0
50
100
150
200
250
300
t

FIG. 3 (a)

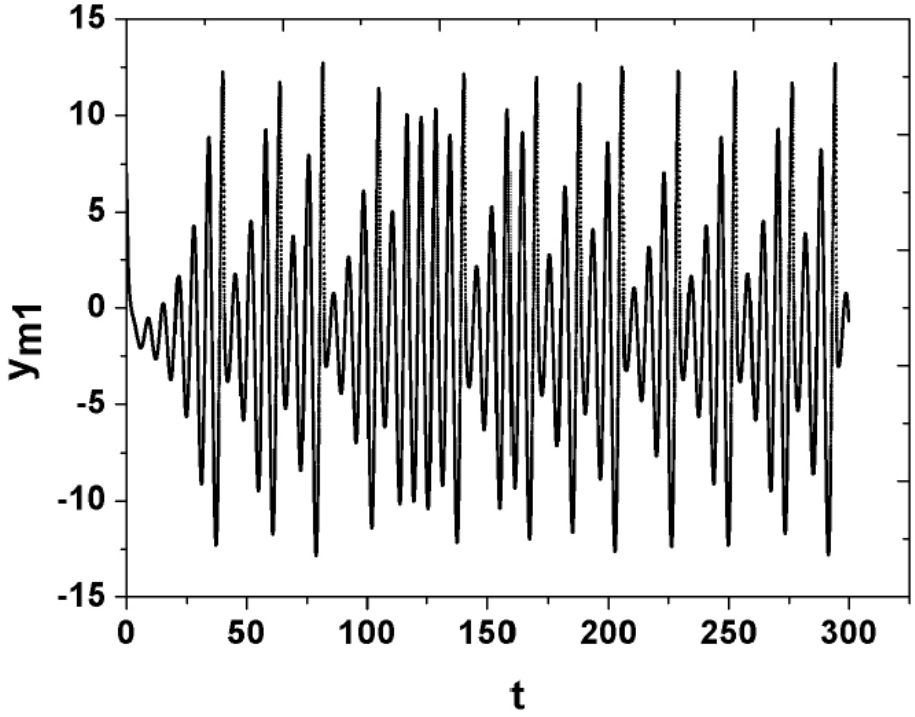
15
10
5
0
-5
-10
-15
ym1
0
50
100
150
200
250
300
t

FIG. 3 (b)

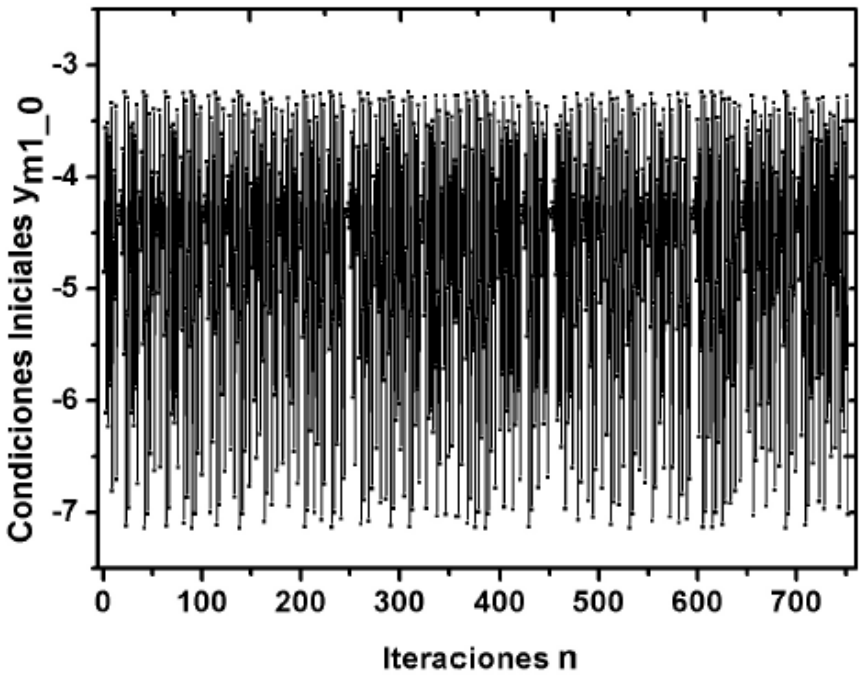
Condiciones Iniciales y_{m1_0}
-3
-4
-5
-6
-7
0
100
200
300
400
500
600
700
Iteraciones n

FIG. 4

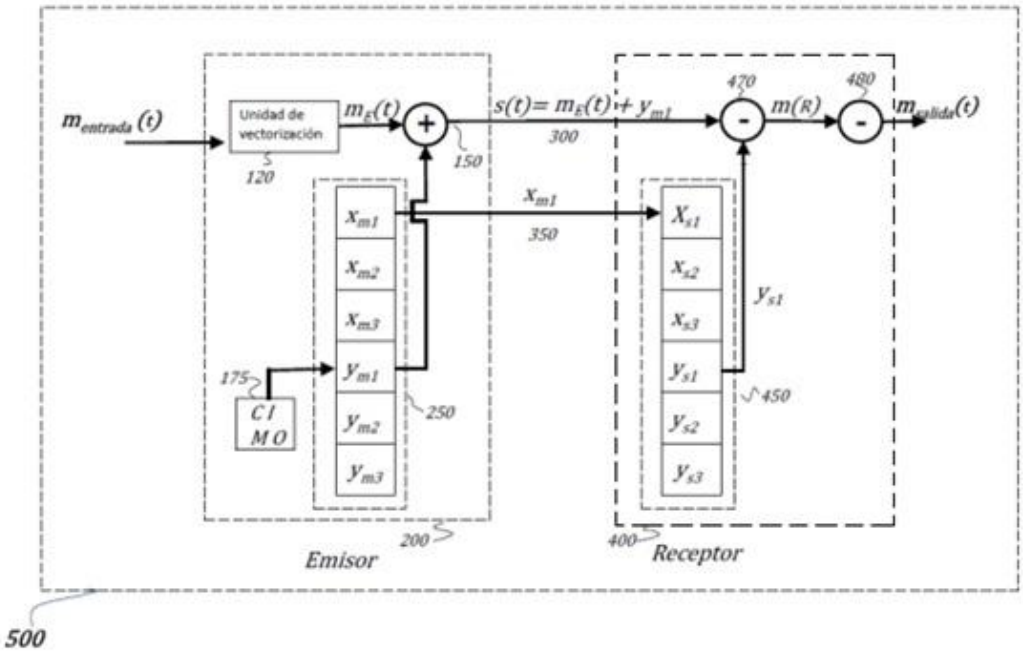
$m_{entrada}(t)$
Unidad de vectorización
120
$m_E(t)$
150
$s(t)= m_E(t)+ y_{m1}$
300
470
$m(R)$
480
$m_{salida}(t)$
x_{m1}
350
x_{m1}
x_{m2}
x_{m3}
y_{m1}
y_{m2}
y_{m3}
175
CI
MO
250
200
Emisor
X_{s1}
x_{s2}
x_{s3}
y_{s1}
y_{s1}
y_{s2}
y_{s3}
450
400
Receptor
500

FIG. 5

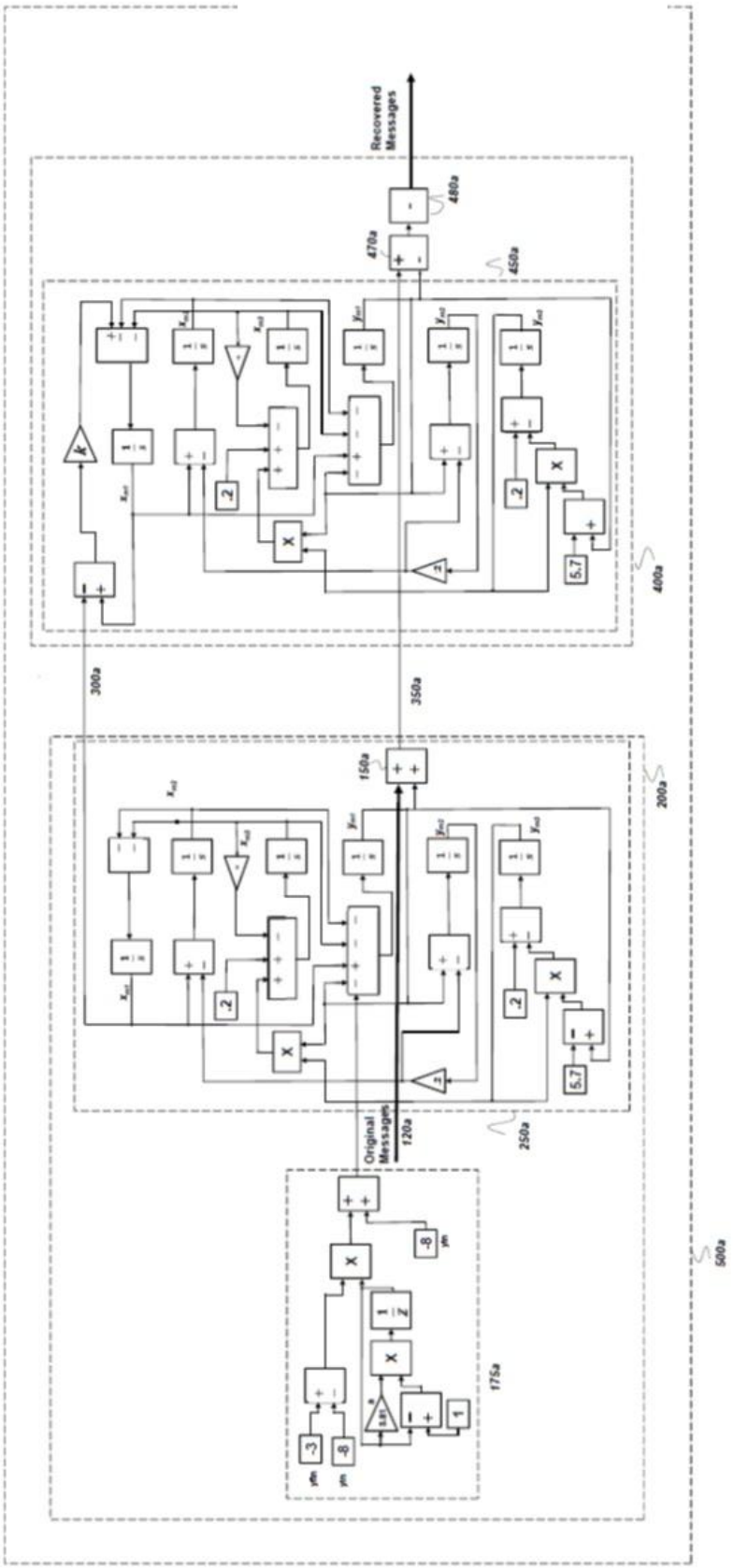
Recovered Messages
480a
470a
450a
400a
300a
350a
150a
200a
Original Messages
120a
250a
500a
175a

FIG. 6

FIG. 7(a)

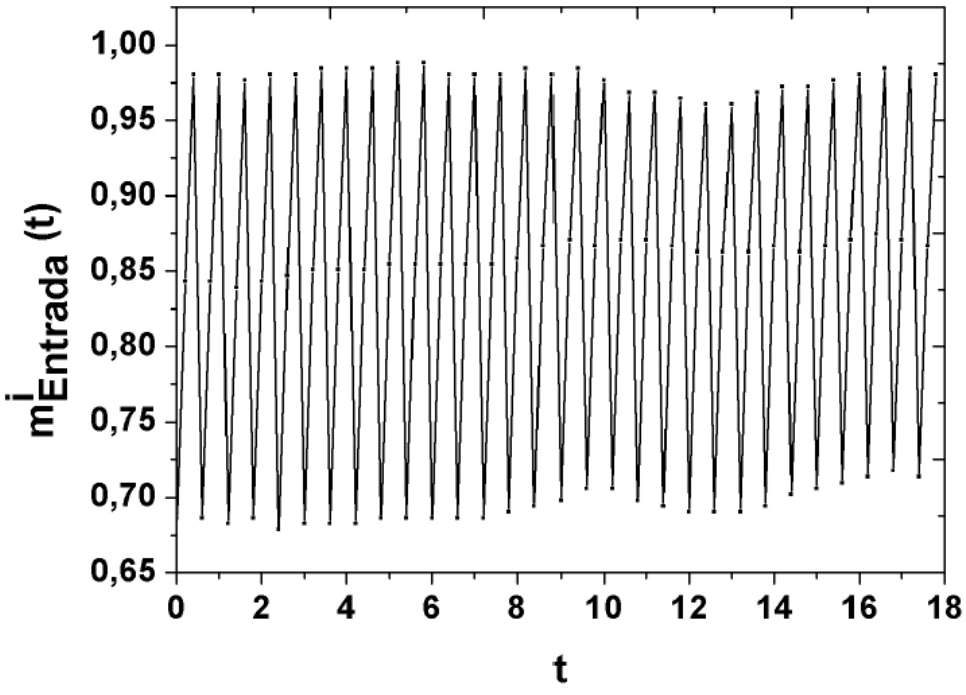
1,00
0,95
0,90
0,85
0,80
0,75
0,70
0,65
$m^i_{Entrada}$ (t)
0
2
4
6
8
10
12
14
16
18
t

FIG. 7(b)

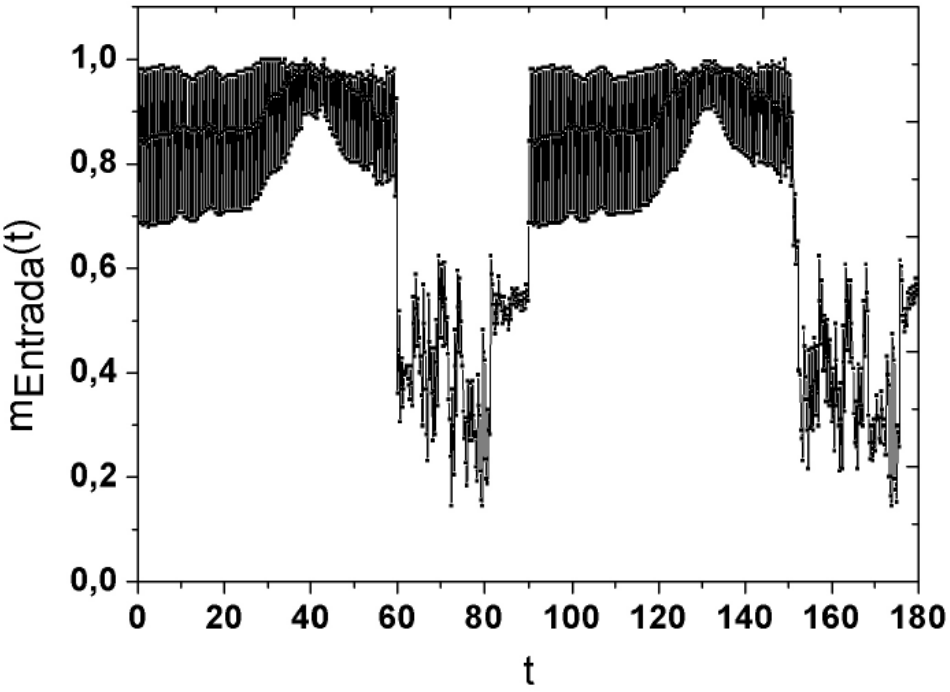
1,0
0,8
0,6
0,4
0,2
0,0
mEntrada(t)
0
20
40
60
80
100
120
140
160
180
t

FIG. 7(c)

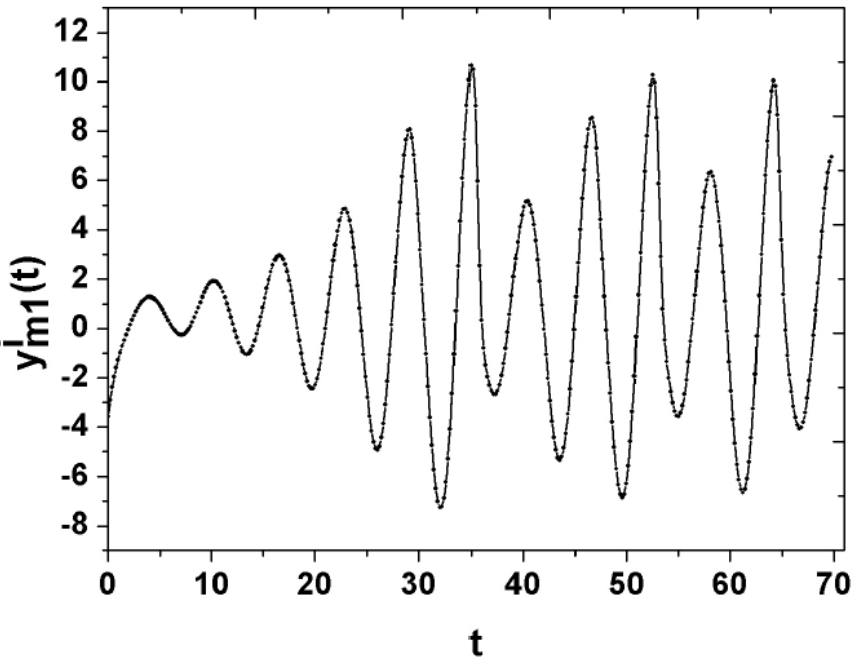
12
10
8
6
4
2
0
-2
-4
-6
-8
$y^i_{m1}(t)$
0
10
20
30
40
50
60
70
t

FIG. 8(a)

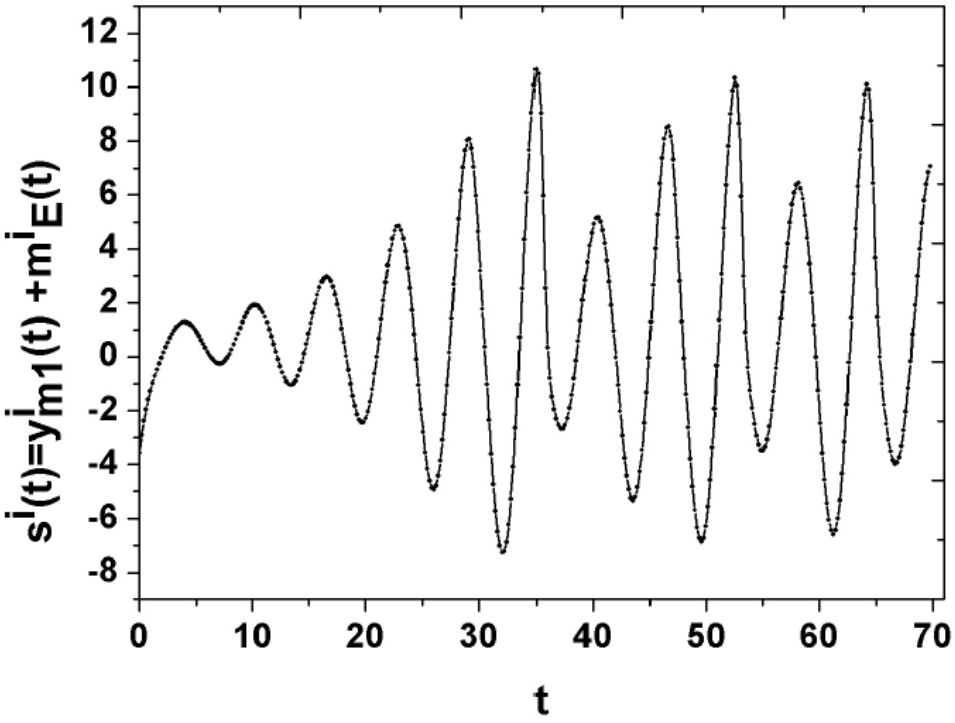

FIG. 8(b)

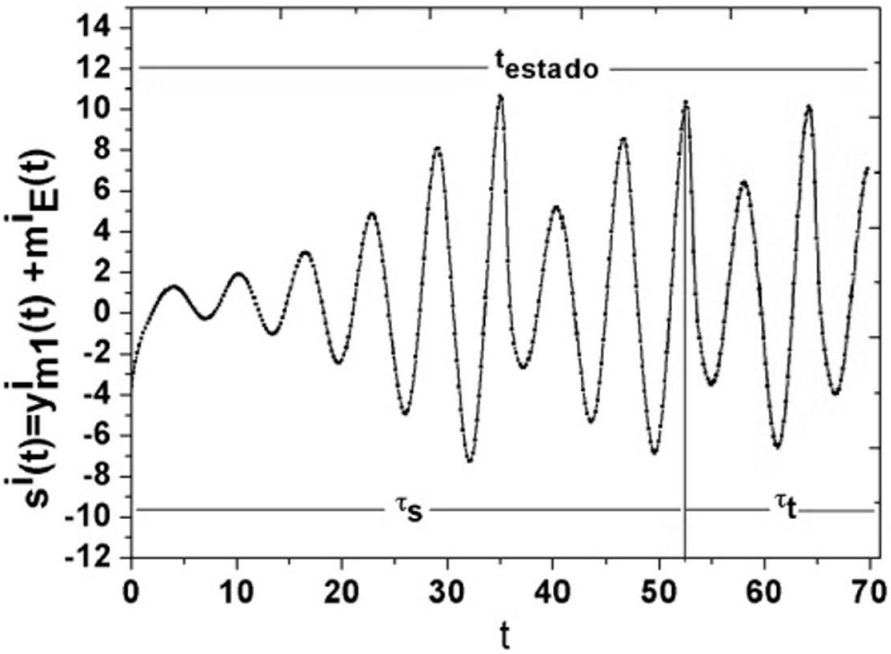

FIG. 8(c)

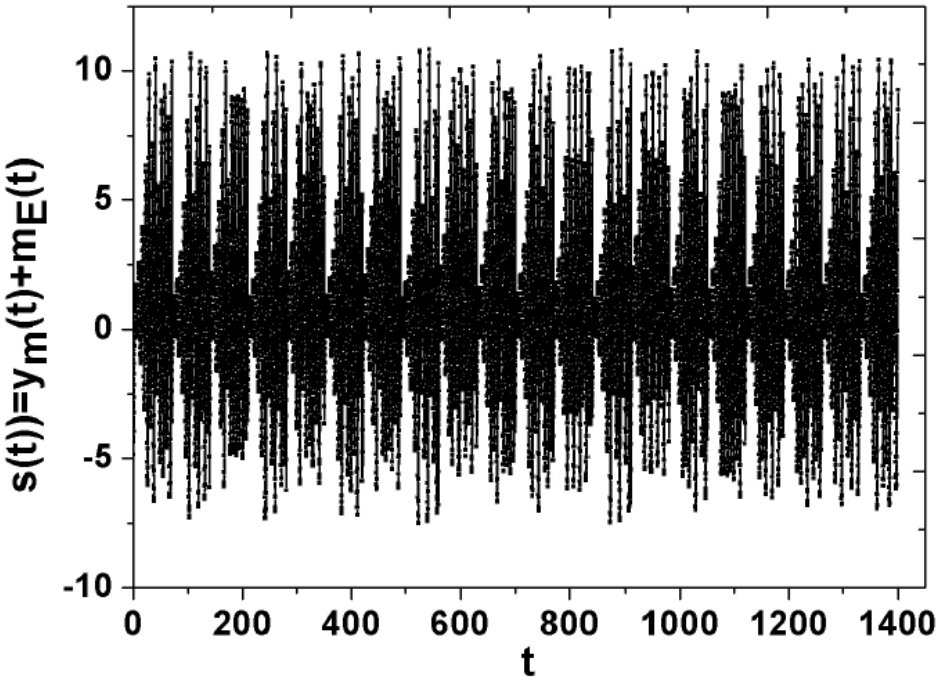
s(t))=y_m(t)+m_E(t)
10
5
0
-5
-10
0
200
400
600
800
1000
1200
1400
t

FIG. 8(d)

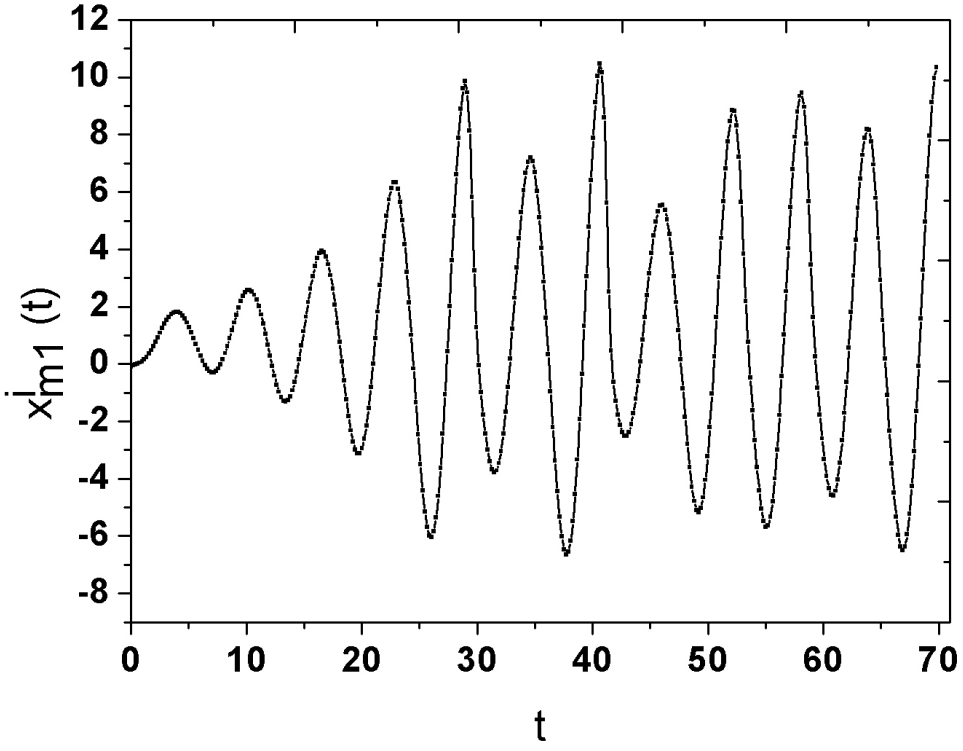
x_m1 (t)
12
10
8
6
4
2
0
-2
-4
-6
-8
0
10
20
30
40
50
60
70
t

FIG. 9(a)

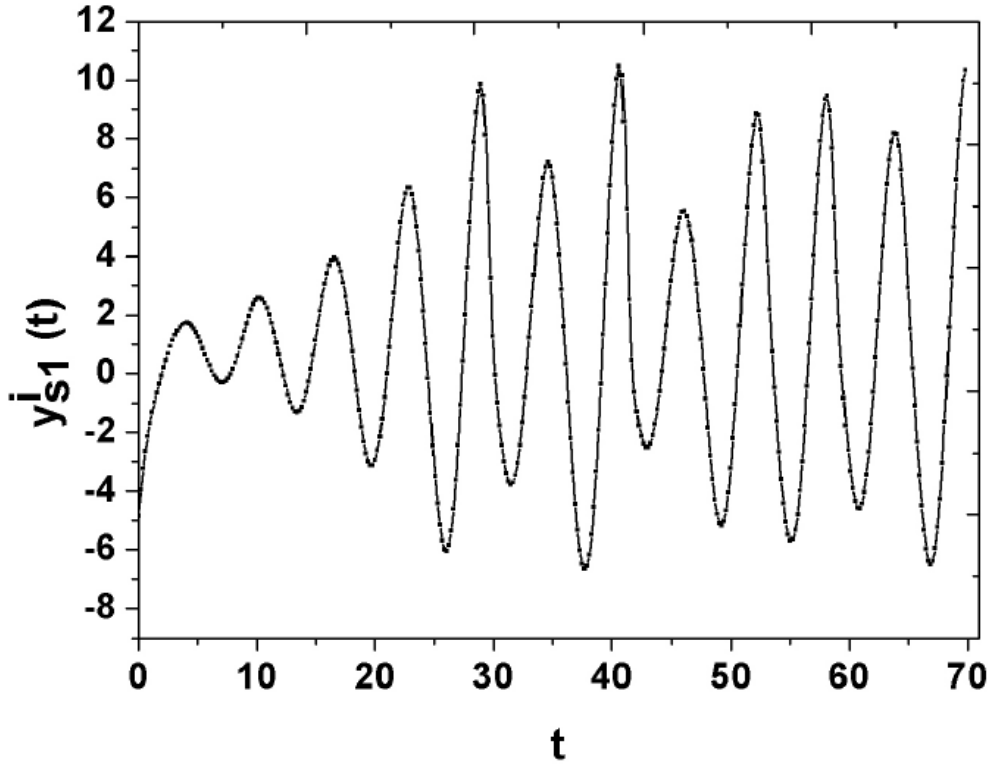
12
10
8
6
4
2
0
-2
-4
-6
-8
0
10
20
30
40
50
60
70
t
y^i_{s1} (t)

FIG. 9(b)

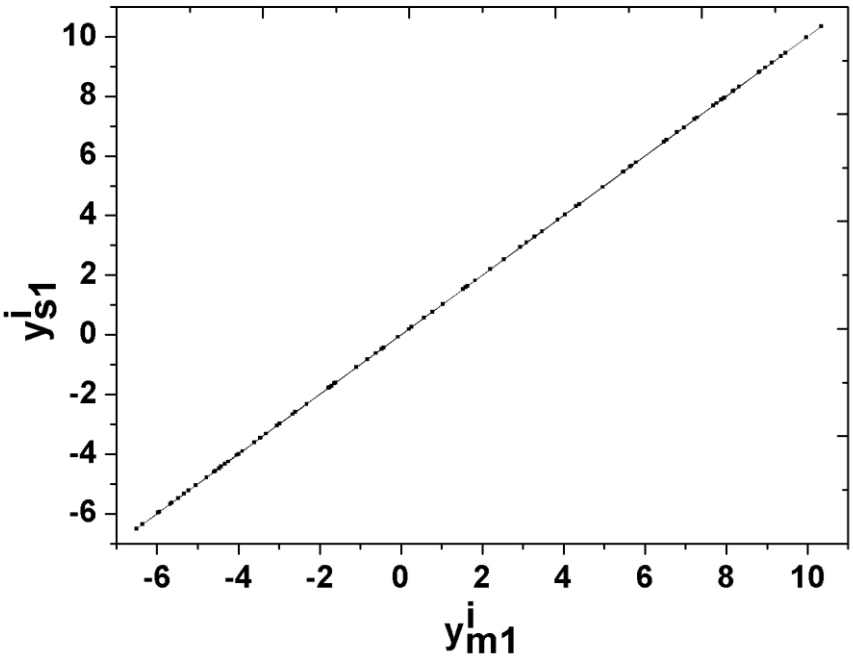
10
8
6
4
2
0
-2
-4
-6
-6
-4
-2
0
2
4
6
8
10
y^i_{m1}
y^i_{s1}

FIG. 9(c)

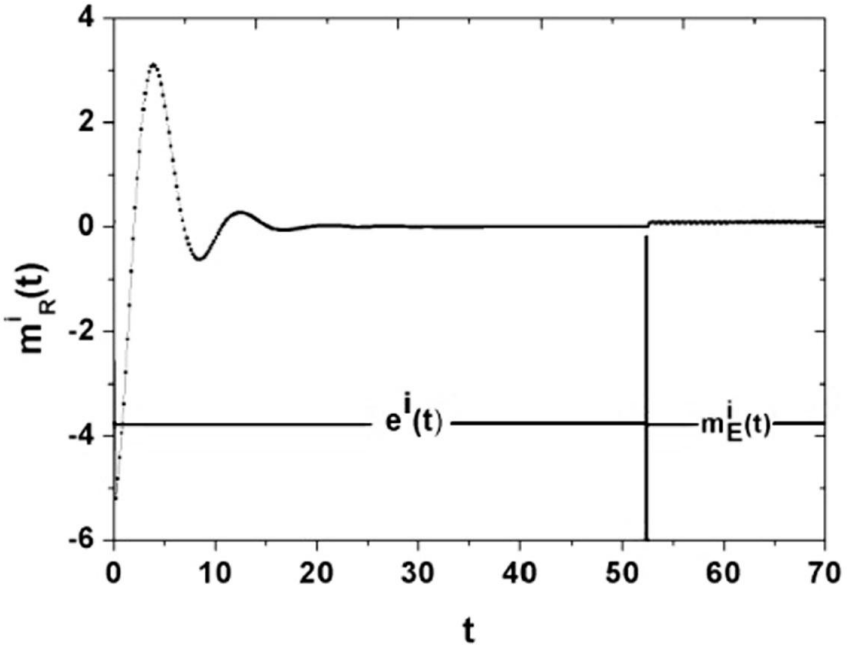

FIG. 10(a)

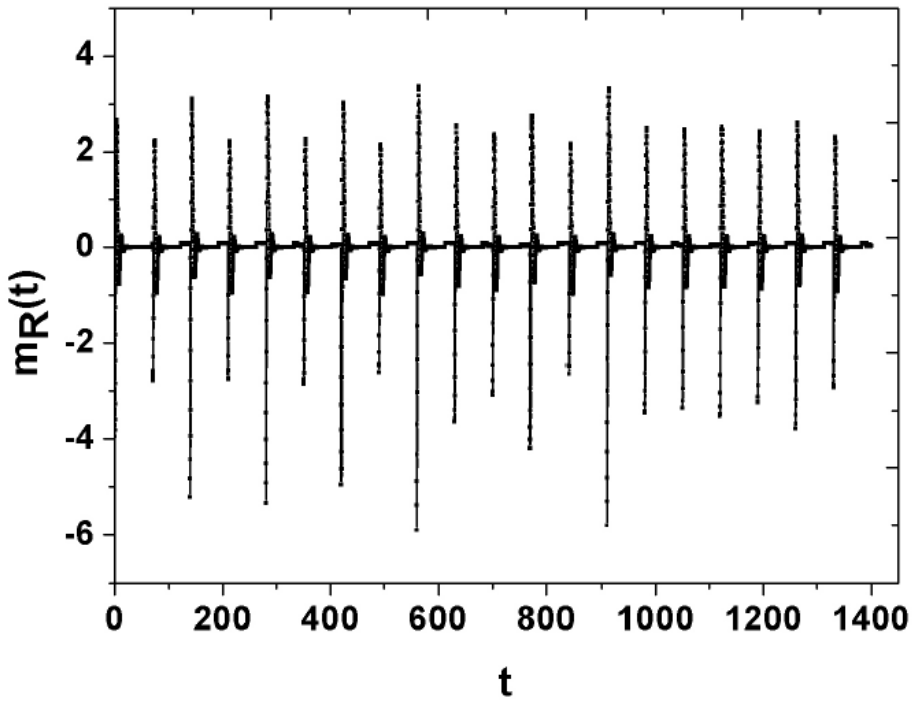

FIG. 10(b)

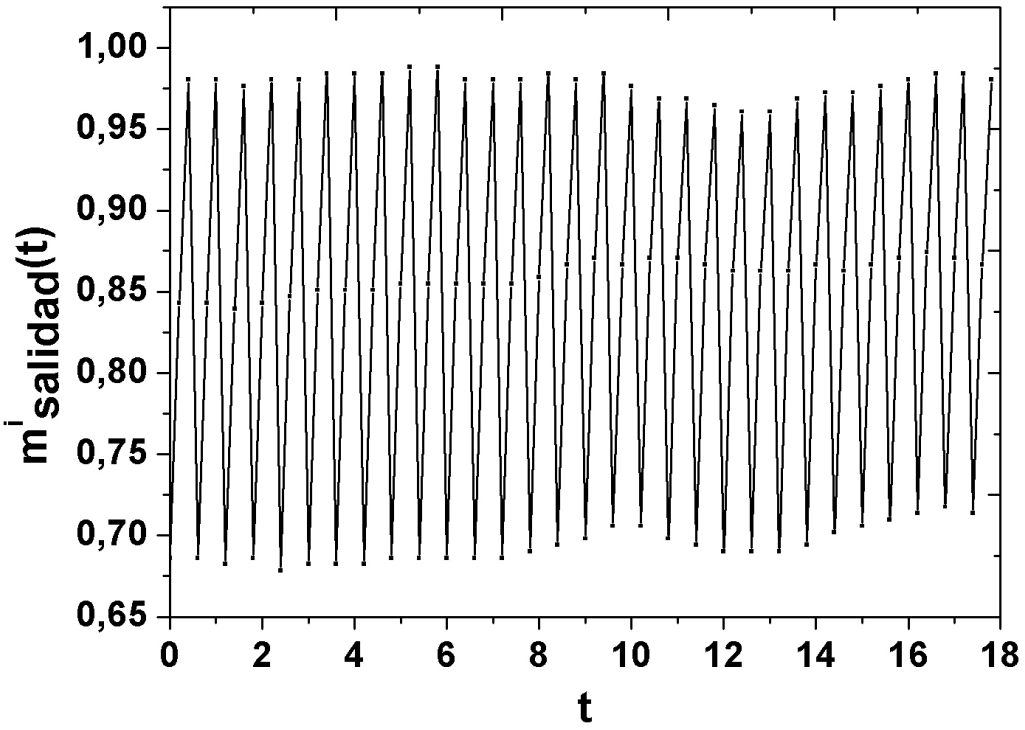

FIG. 11(a)

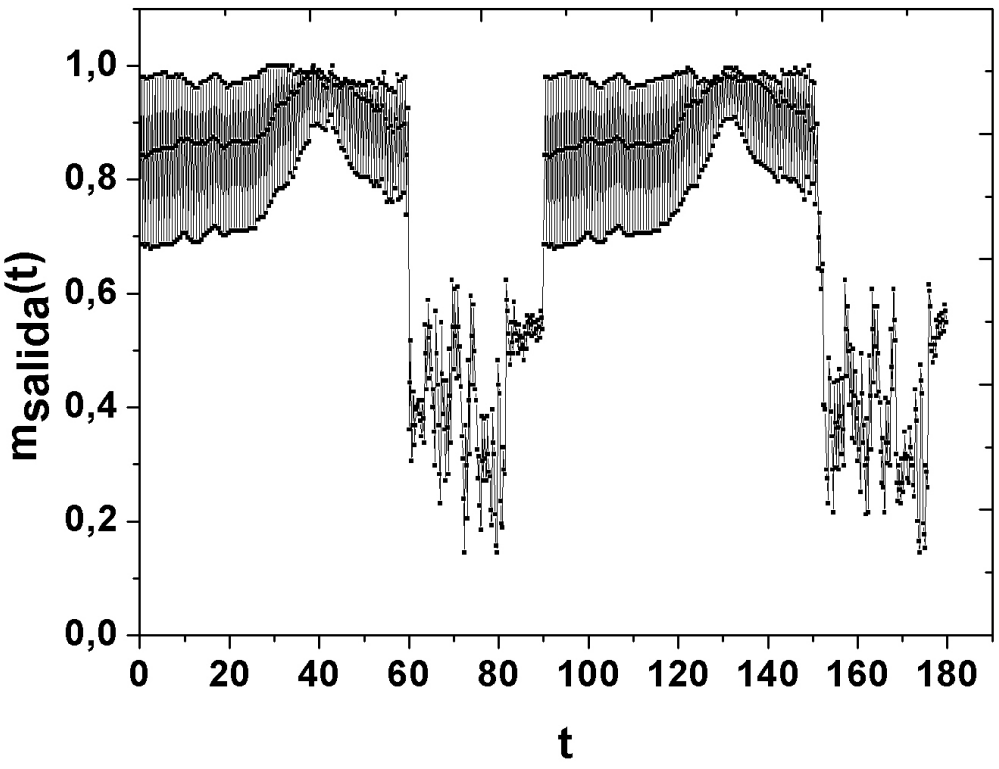

FIG. 11(b)

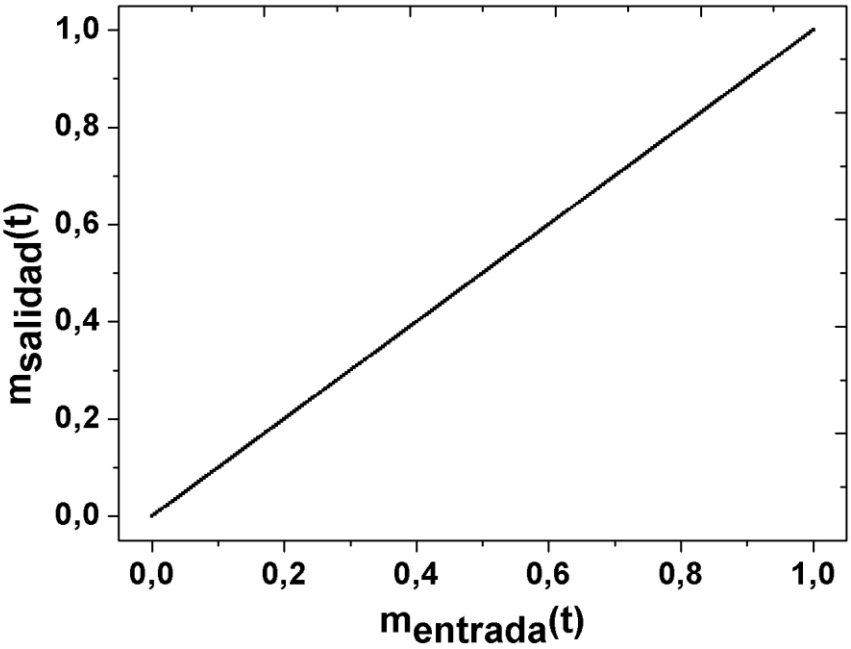

FIG. 12

FIG. 13

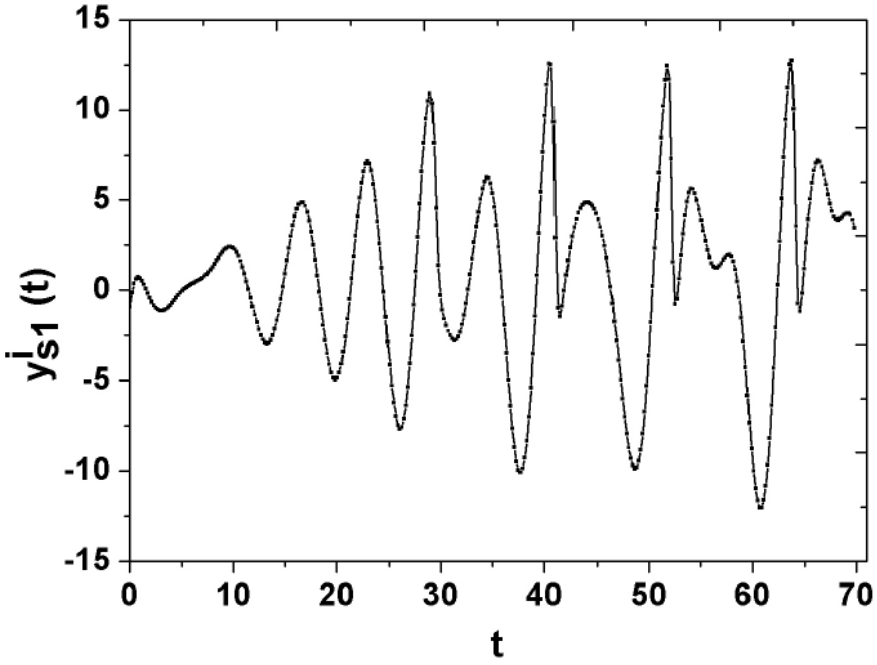

FIG. 14(a)

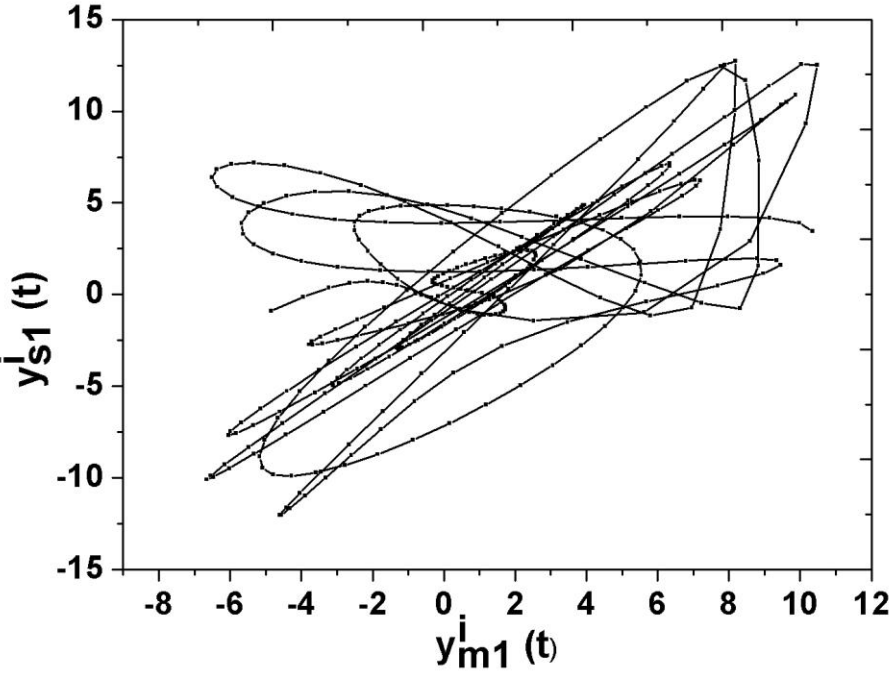

FIG. 14(b)

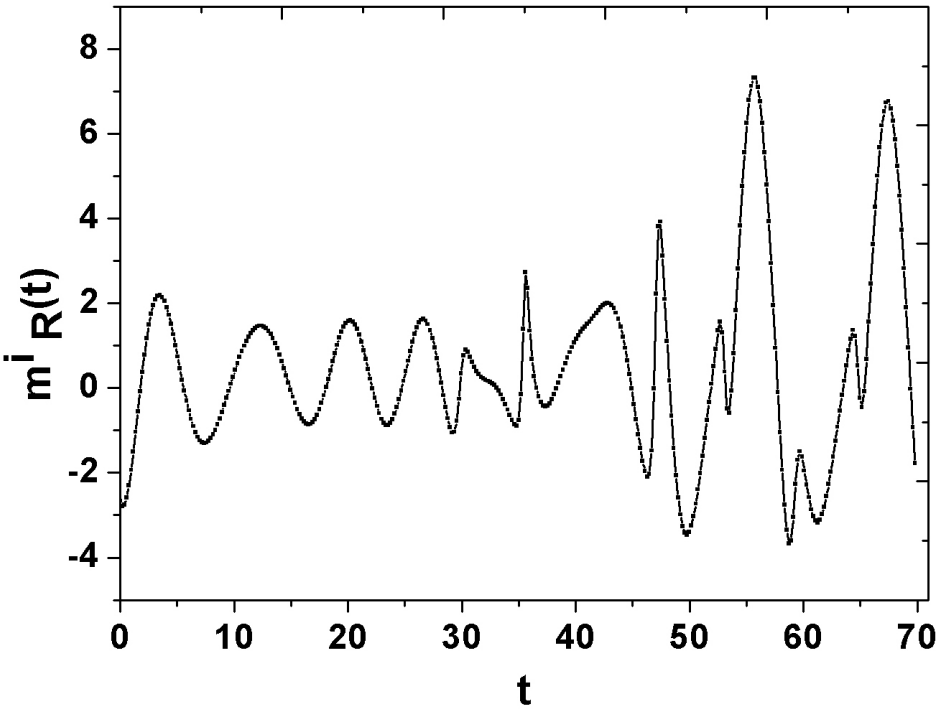

FIG. 15(a)

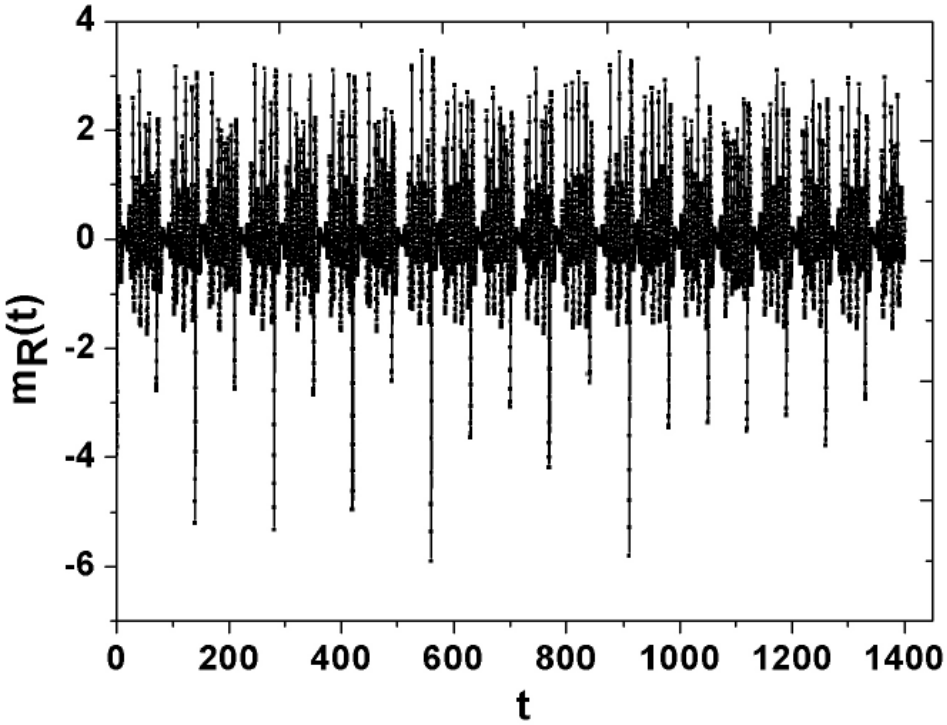

FIG. 15(b)

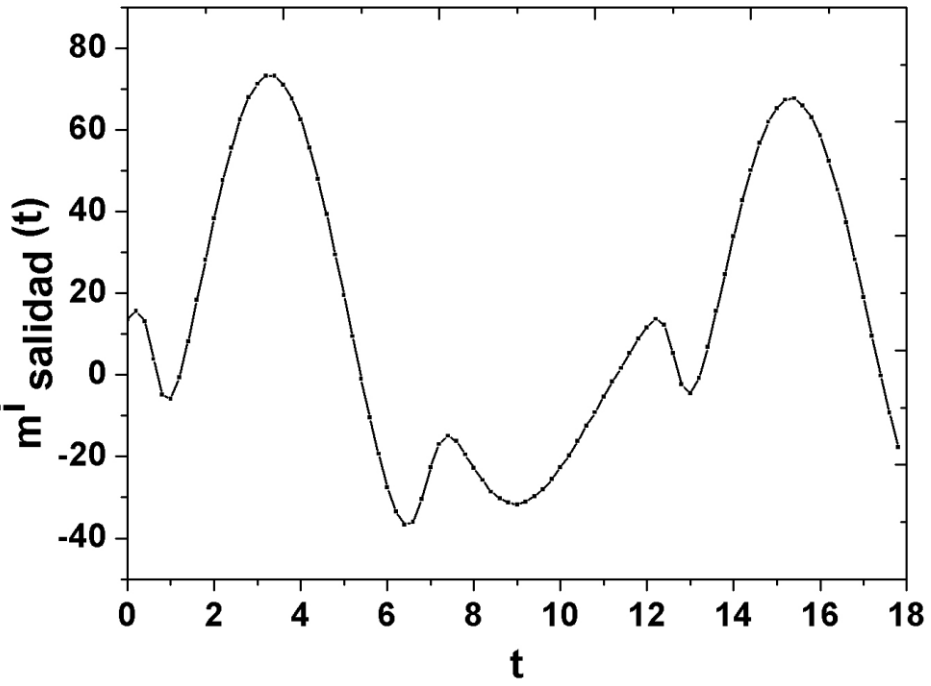

FIG. 16(a)

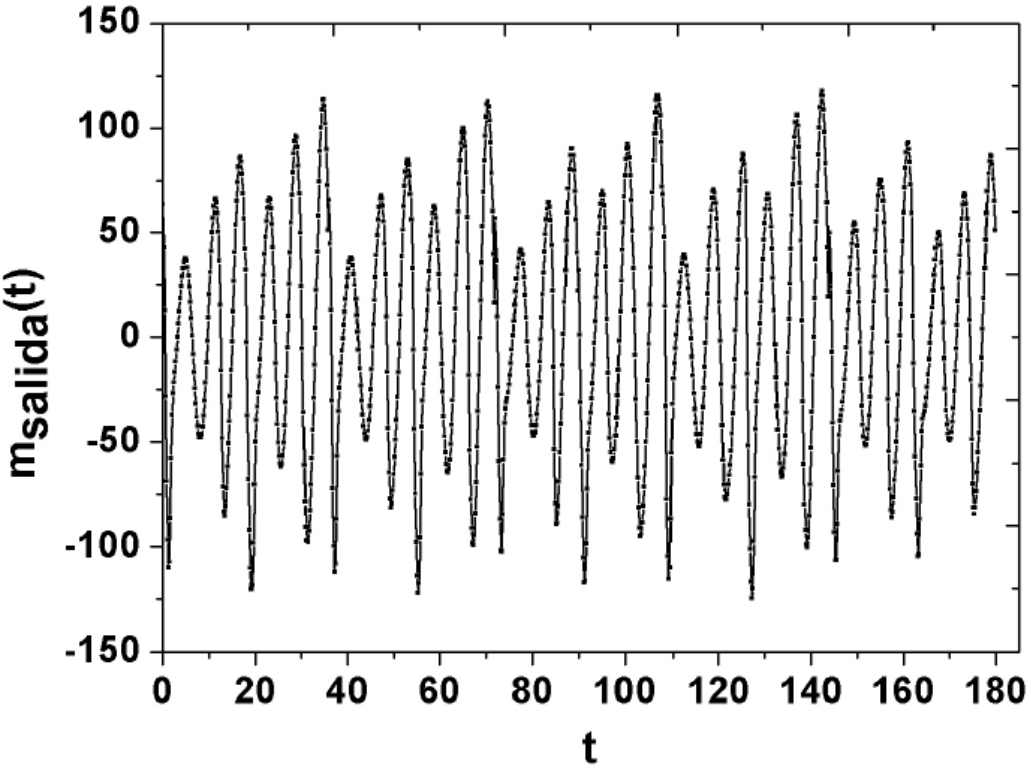

FIG. 16(b)

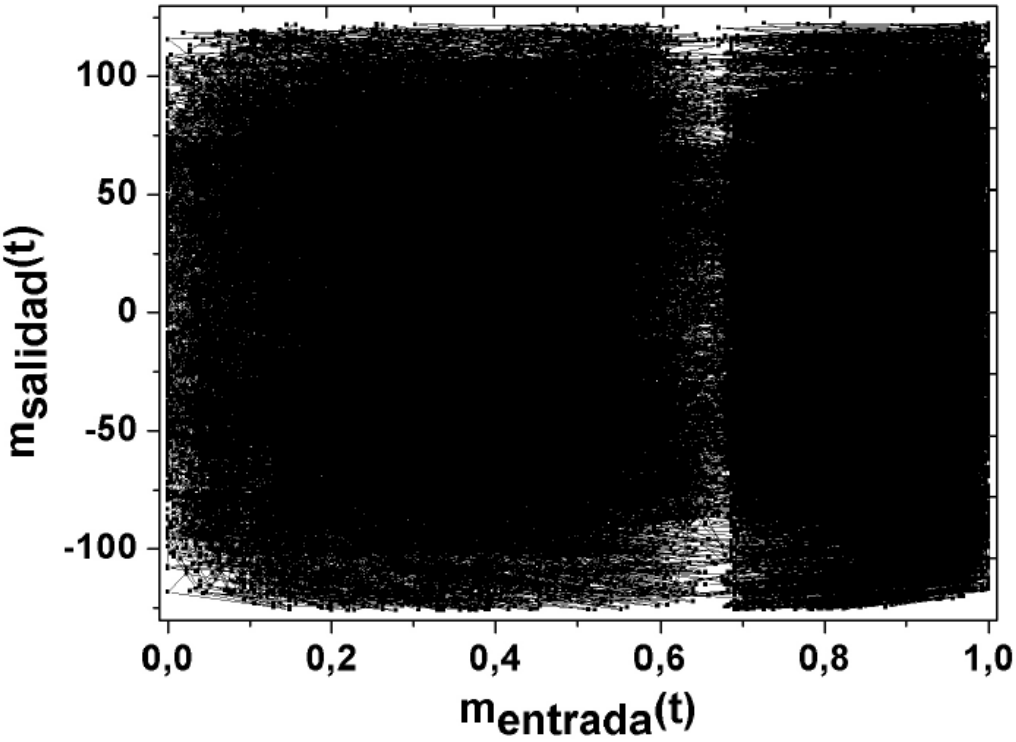

FIG. 16(c)

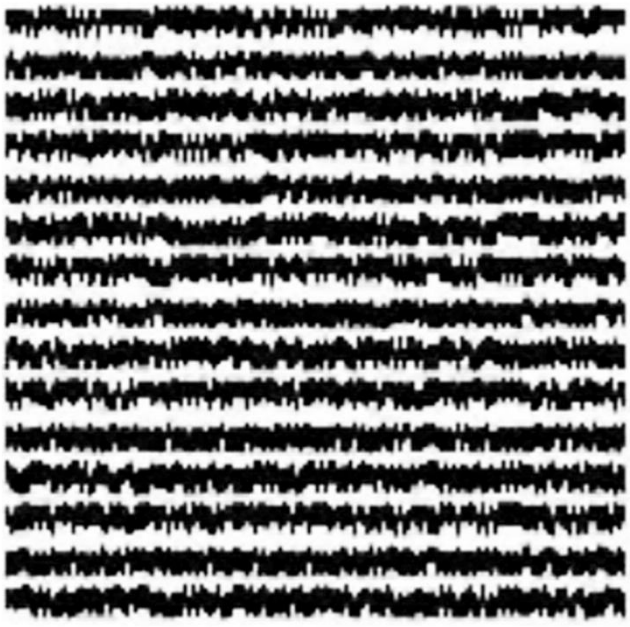

FIG. 17

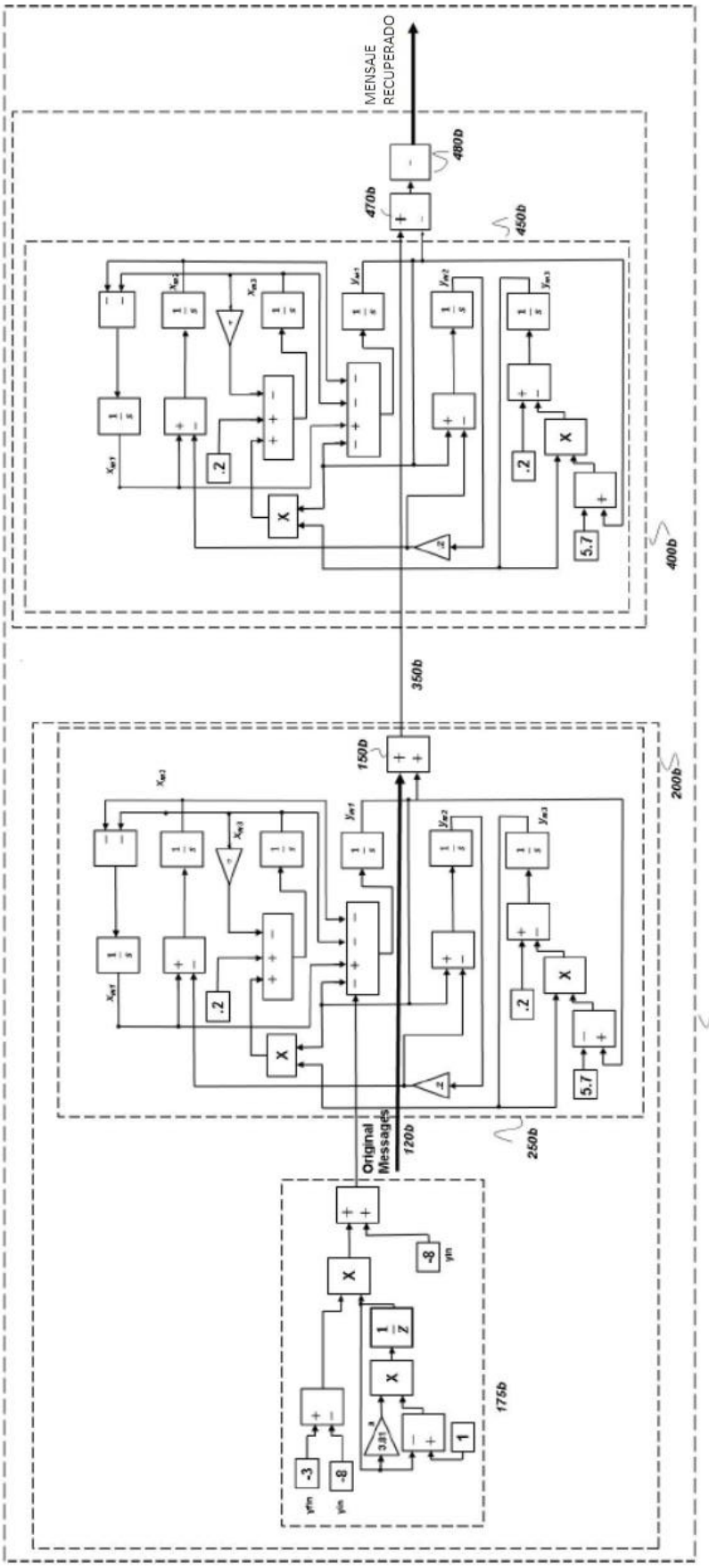
MENSAJE RECUPERADO
480b
470b
450b
400b
350b
150b
200b
500b
Original Messages
120b
250b
175b
.2
5.7
-8
-3
1
3.81

FIG. 18

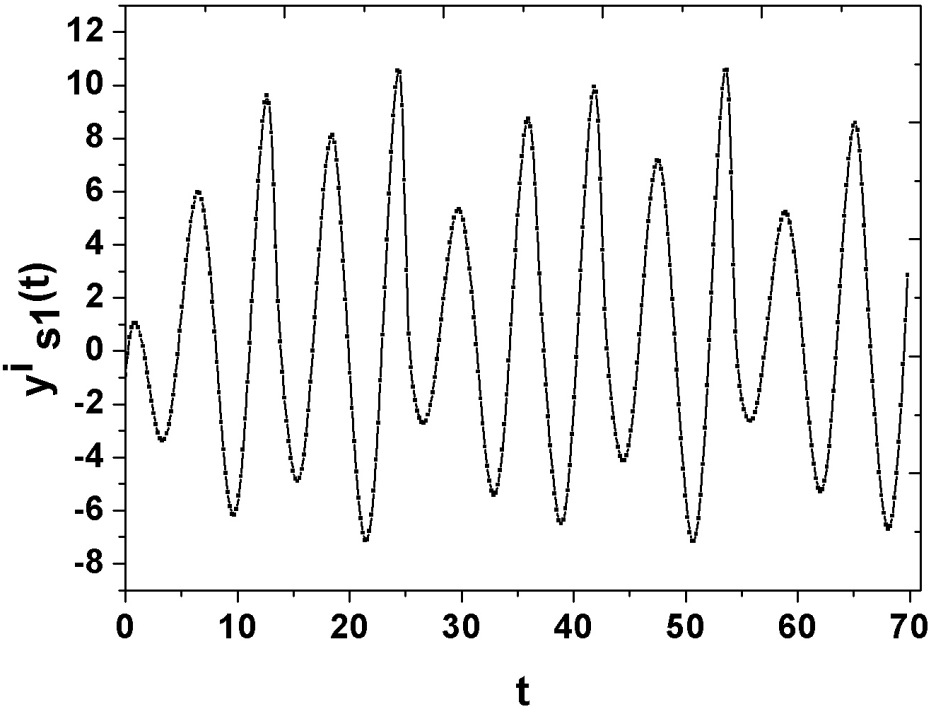

FIG. 19(a)

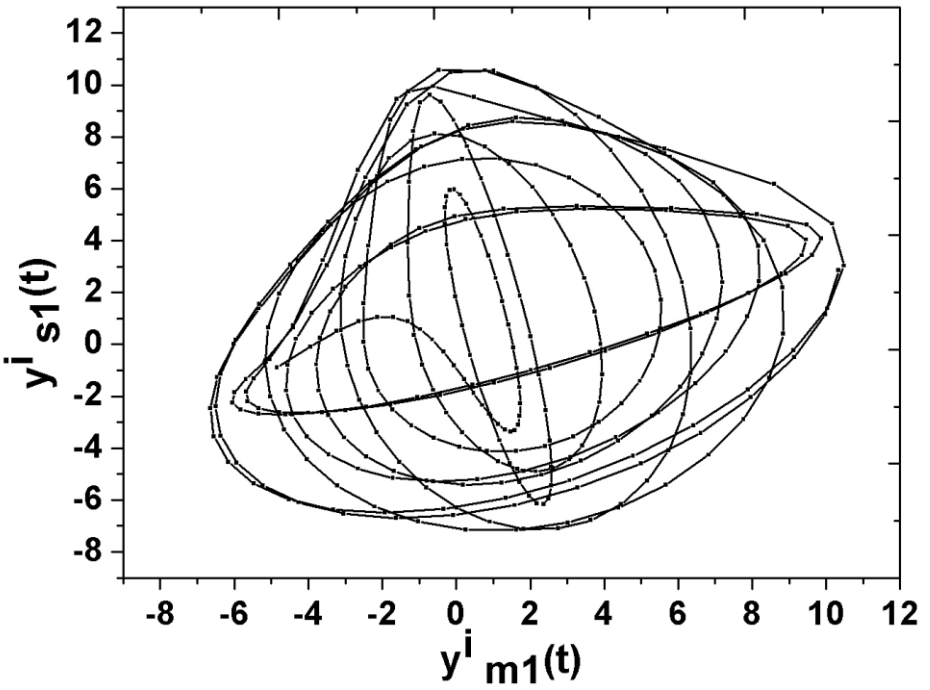

FIG. 19(b)

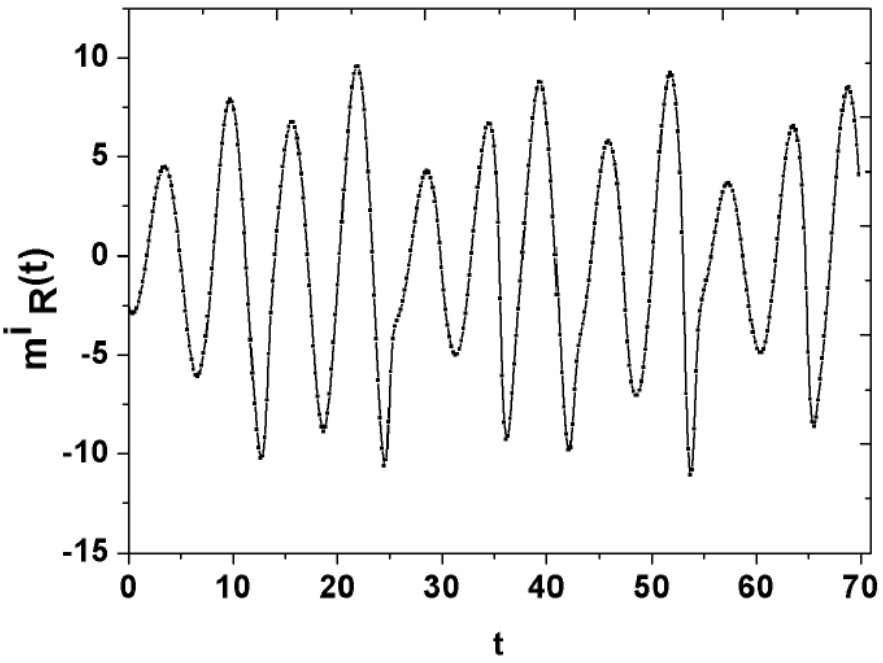

FIG. 20(a)

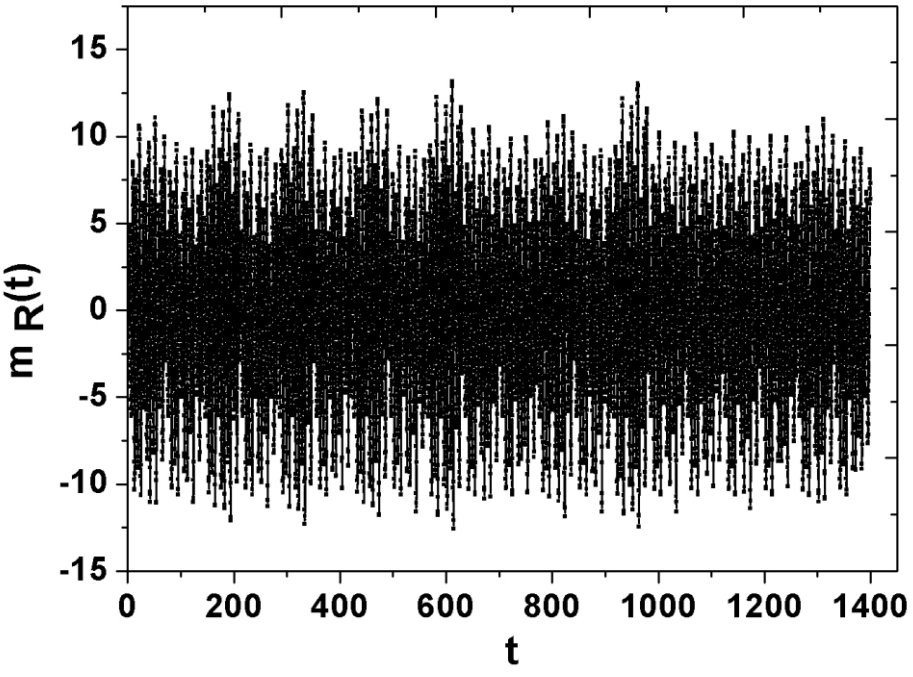

FIG. 20(b)

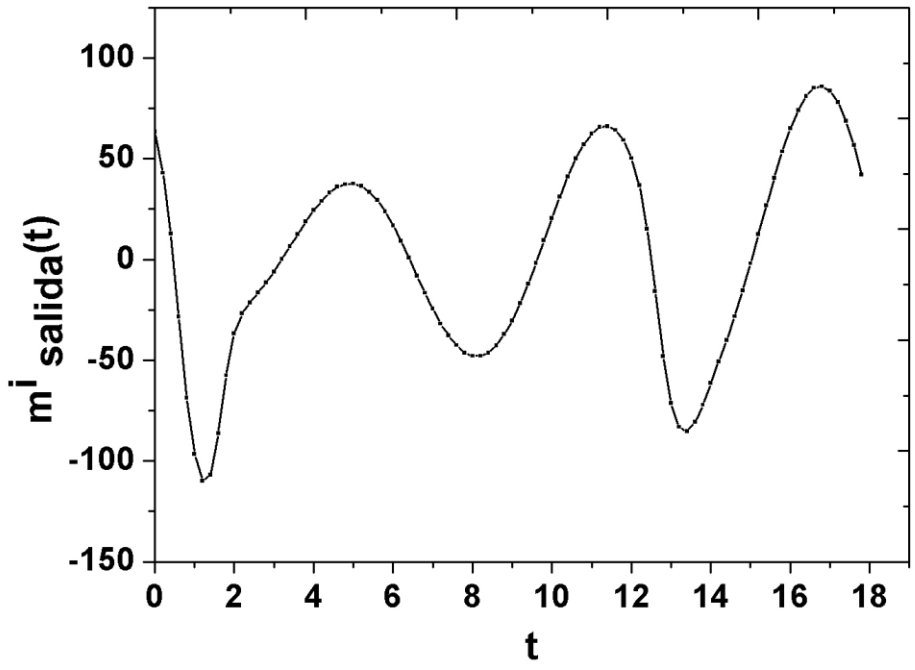

FIG. 21(a)

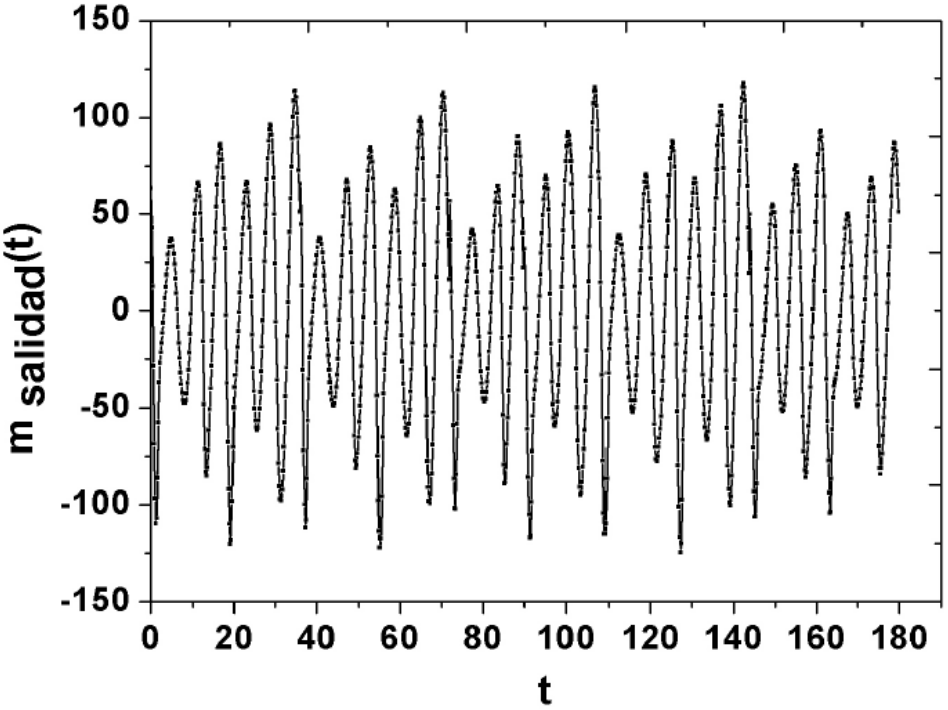

FIG. 21(b)

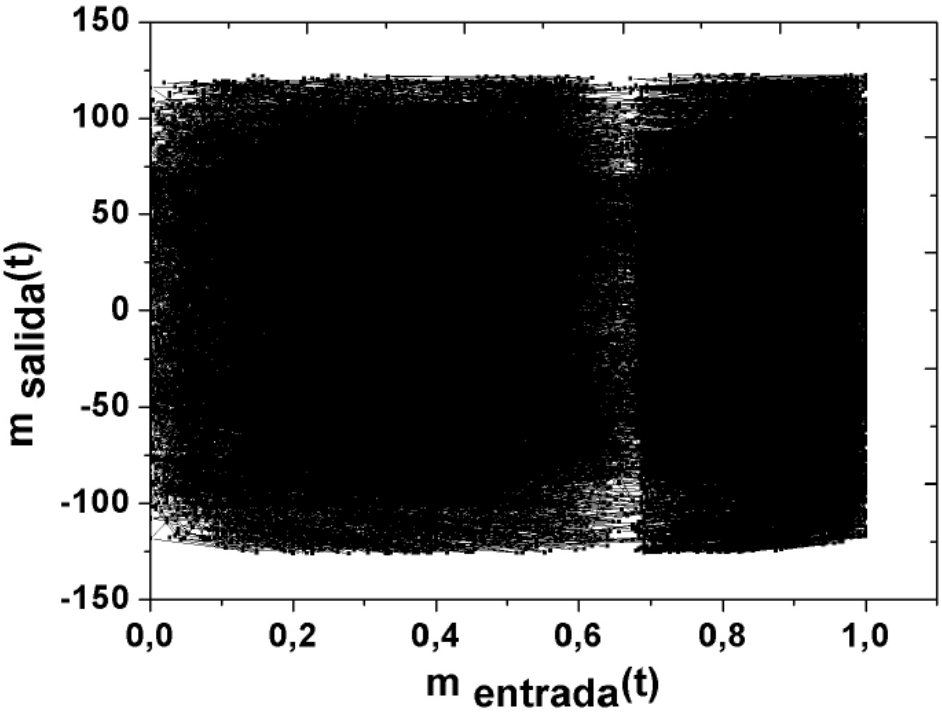

FIG. 21(c)

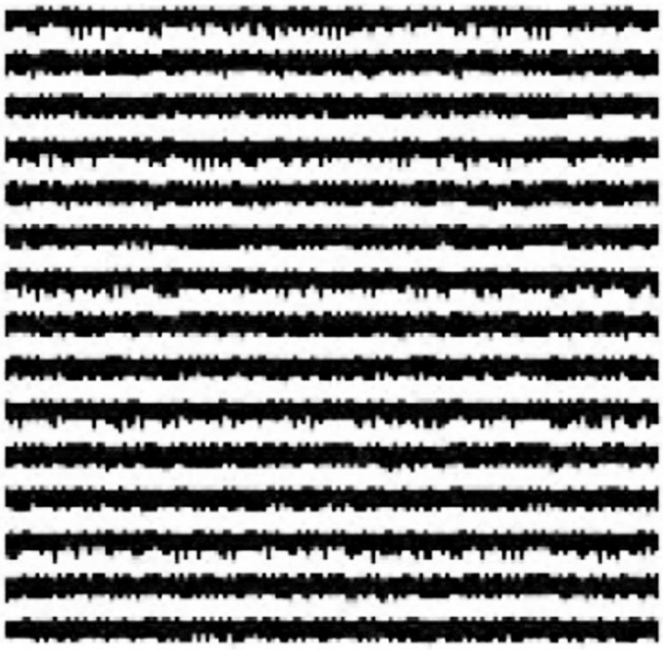

FIG. 22