Sincronización de sistemas caóticos y el recontra espionaje

Zablotsky, Amir Nicolás
Instituto Balseiro, UNCuyo, CNEA, Argentina

15 de octubre de 2020

Resumen

Una aplicación de las dinámicas caóticas consiste en la posibilidad de encriptar y desencriptar señales enmascarando el mensaje con una variable caótica generada por el sistema del emisor, y luego mediante el forzado del sistema del receptor con la señal recibida obtener la misma máscara para así desencriptar el mensaje. De esta manera, si la señal fuera interceptada en el medio por un miembro de la organización criminal KAOS, solo vería una señal caótica [1]. En este informe se detalla la implementación de los sistemas del emisor y receptor, se realiza un estudio de algunos aspectos de su funcionamiento y se enseña el encriptado de una señal junto a algunas sugerencias.

1. Introducción

Una forma de encriptar señales consiste en enmascarar el mensaje mediante una variable de un sistema caótico con propiedades de auto-sincronización como lo es el sistema de Lorentz [2]. Esta propiedad permite forzar una o mas de las variables del sistema para hacerlo tender asintóticamente a la misma trayectoria que el sistema con el cual se lo fuerza independientemente de las condiciones iniciales (lo cual resulta de mucho interés, ya que la alta sensibilidad a las condiciones iniciales es característica de los sistemas caóticos). El método consiste en sumarle a la señal que se quiere enviar una variable caótica del sistema, y luego el receptor puede utilizar esto para forzar la variable correspondiente de su sistema y de esta manera, debido a la sincronización, obtener la misma variable caótica para restársela a la señal recibida y obtener el mensaje desencriptado.

En la sección Métodos se explica el funcionamiento e implementación por separado de los sistemas de emisor y receptor en C++ con el fin de estudiar la sincronización de ambos sistemas caóticos mediante el forzado de una de las variables y enviar un mensaje, y en Resultados se analizan algunas características del sistema como las trayectorias de los atractores caóticos, las variables que permiten sincronizar al emisor y el receptor, la independencia de la sincronización con las condiciones iniciales de ambas partes, la dependencia del error en el desencriptado en función de la frecuencia de la señal enviada y un ejemplo de encriptado de un mensaje de audio.

2. Método

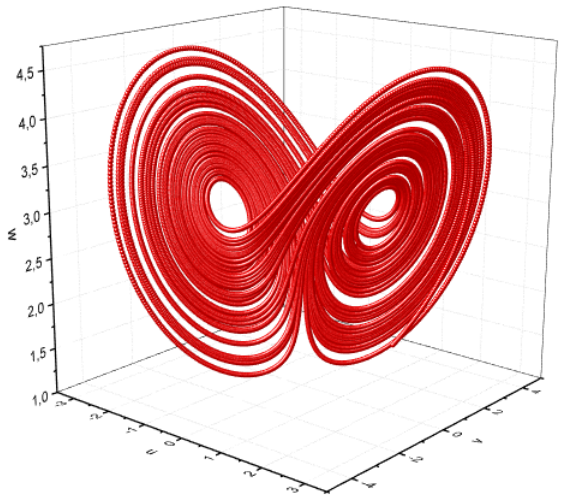

Figura 1: Atractor de Lorentz, correspondiente al conjunto de soluciones caóticas del sistema del mismo nombre.

El sistema caótico utilizado en esta forma de encriptado debido a sus propiedades de auto-sincronización es el llamado sistema de Lorentz, propuesto originalmente para modelar el fenómeno de convección atmosférica [3], que está dado por el siguiente conjunto de ecuaciones diferenciales:

$$\begin{cases} \dot{u} = \sigma(v - u) \\ \dot{v} = \rho\, u - v - 20uw \\ \dot{w} = 5uv - \beta w. \end{cases}$$

Para implementar el sistema de encriptado y desencriptado se tomaron $\sigma = 10$, $\rho = 60$ y $\beta = \frac{8}{3}$ que corresponden al regimen caótico del sistema (Fig. 1), y se calculó la evolución temporal de las variables de los sistemas mediante un algoritmo Runge-Kutta de orden cuatro con paso fijo $h = 0,0001$.

El sistema del emisor consiste en el sistema mencionado previamente, a partir del cual se utiliza $u(t)$ para enmascarar un mensaje $m(t)$ y así obtener el mensaje encriptado $s(t)$ mediante la operación

$$s(t) = u(t) + \epsilon\, m(t),$$

donde ϵ es una constante con el propósito de reescalear el mensaje de manera que punto a punto sea pequeño en comparación a $u(t)$, obteniendo así la variable caótica perturbada s.

El sistema del receptor consiste en el mismo sistema de ecuaciones diferenciales (y parámetros de control) pero en lugar de dejarlo evolucionar como en el caso anterior se fuerza la variable u para sincronizarlo con el sistema del emisor. De esta manera, el sistema del receptor queda dado por:

$$\begin{cases} \dot{u}_r = \sigma(v_r - u_r) \\ \dot{v}_r = \rho\, u(t) - v_r - 20u(t)w_r \\ \dot{w}_r = 5u(t)v_r - \beta w_r. \end{cases}$$

Si se fuerza el sistema del receptor con $s(t)$ el sistema converge asintóticamente a la trayectoria del emisor (en particular $u_r(t)$ tiende a $u(t)$), por lo que mediante

$$m'(t) = s(t) - u_r(t)$$

es posible recuperar el mensaje encriptado a menos de un factor de escala.

3. Resultados

3.1. Propiedades del sistema

En primera instancia se observaron las trayectorias del sistema de Lorentz para distintas condiciones iniciales (Figs. 2 y 3). Se utilizaron las condiciones iniciales $(0.5, 0.5, 0.5)$, $(1.5, 1.5, 1.5)$ y $(3, 3, 3)$, y se graficaron las proyecciones en los planos u-v y u-w para simplificar su visualización.

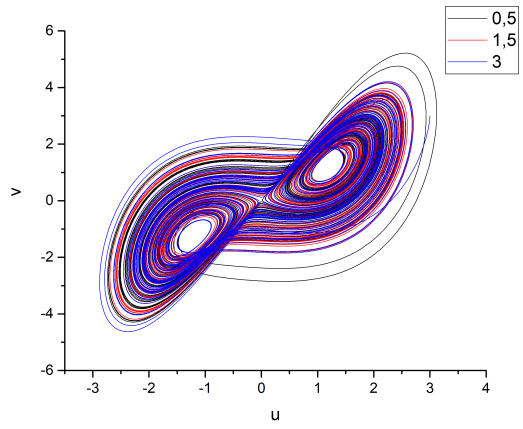

Figura 2: Proyección de las trayectorias en el plano u-v para distintas condiciones iniciales del tipo $u_0 = v_0 = w_0$.

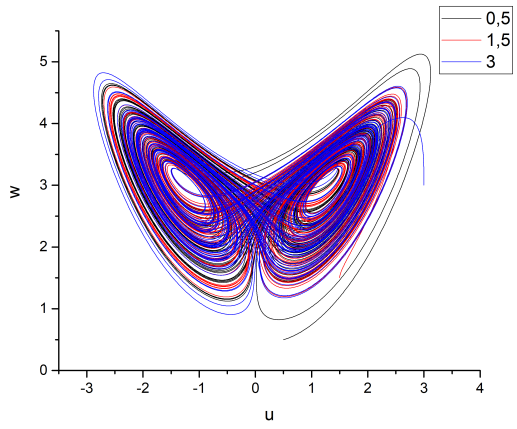

Figura 3: Proyección de las trayectorias en el plano u-w correspondientes a las mismas condiciones iniciales que en la Fig. 2.

Como se puede ver, las trayectorias atractoras del sistema tienen la misma forma (cortes de la Fig. 1) independientemente de las condiciones iniciales, lo cual permite que el sistema forzado converja asintóticamente y con alta precisión a la misma trayectoria del sistema que lo fuerza.

Para verificar que esta sincronización se da independientemente de las condiciones iniciales, incluso si el sistema del receptor y el emisor parten de condiciones iniciales diferentes, se observó en el mismo gráfico las trayectorias del emisor y el receptor con distintas condiciones iniciales (Figs. 4 y 5) donde se puede notar que estas se superponen salvo por un tramo inicial (a causa de la diferencia en las condiciones iniciales), lo cual indica que el receptor se sincroniza con el emisor. Para verlo de manera mas detallada, se graficó la distancia $d = \sqrt{(u-u_r)^2 + (v-v_r)^2 + (w-w_r)^2}$ en función del tiempo para tres condiciones iniciales distintas (Fig. 6).

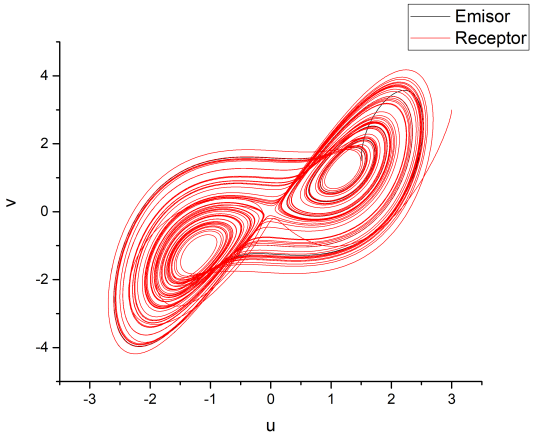

Figura 4: Proyección de las trayectorias del emisor con condición inicial $(1.5, 1.5, 1.5)$ y el receptor con condición inicial $(3, 3, 3)$ en el plano u-v.

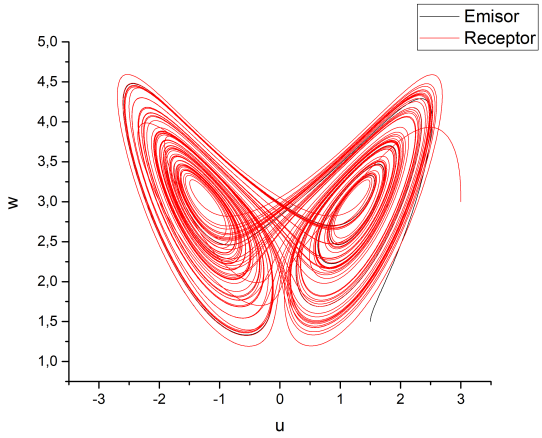

Figura 5: Proyección de las trayectorias del emisor con condición inicial $(1.5, 1.5, 1.5)$ y el receptor con condición inicial $(3, 3, 3)$ en el plano u-w.

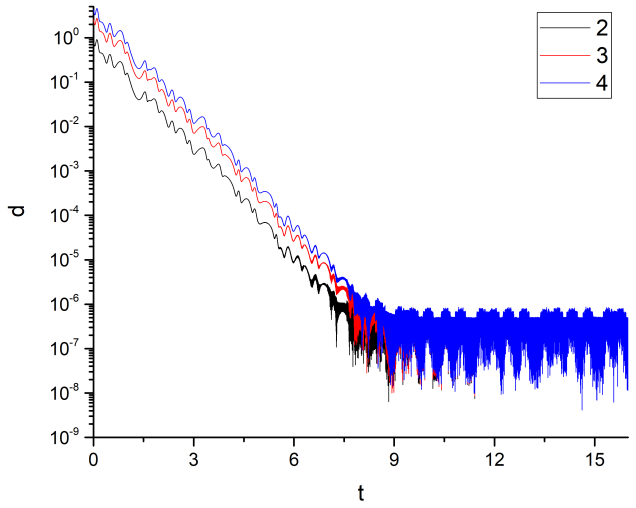

Figura 6: Gráfico $d(t)$ en escala logarítmica. Se puede notar que las trayectorias tienden a juntarse, a menos de un error de baja frecuencia inducido por el método de encriptado. Para el sistema del receptor se utilizaron condiciones iniciales del tipo $u_0 = v_0 = w_0$ indicadas en el gráfico por colores.

Como se puede ver en la Fig. 6, la trayectoria del receptor tiende asintóticamente a la trayectoria del emisor ($d = 0$) a menos de un error inducido por el encriptado en el orden de 10^{-6}, y en los primeros tiempos en los que las trayectorias aún no coinciden notamos que la distancia entre ellas decae de manera exponencial con el tiempo. A partir de esto, podemos concluir que si se fuerza la variable u del sistema es posible sincronizar al receptor con el emisor independientemente de las condiciones iniciales.

A raíz de esto surge la inquietud de si cualquier variable del sistema permite forzar al receptor para que su trayectoria tienda asintóticamente a la del emisor. Para esto se forzó el sistema del receptor mediante la variable caótica $w(t)$ en lugar de $u(t)$, y se graficaron las proyecciones de sus trayectorias (Figs. 7 y 8) donde se puede ver que no coinciden con los cortes del atractor de Lorentz (Fig. 1) por lo que el sistema no se sincronizará. Para que esto quede en evidencia también se graficó la distancia entre las trayectorias del emisor y el receptor forzándolo con $w(t)$ (Fig. 9).

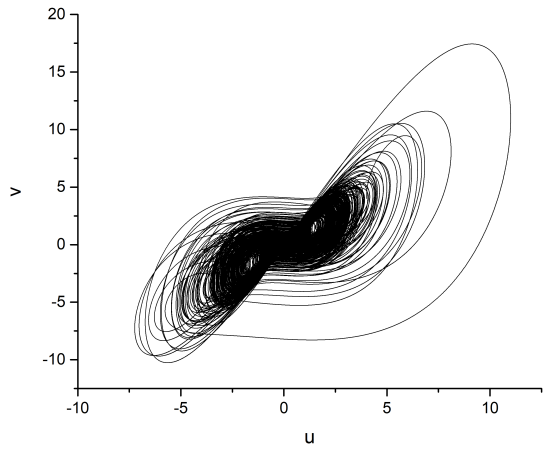

Figura 7: Proyección de la trayectoria del receptor en el plano u-v, forzando la variable w. Se observa como esta difiere respecto a la de la Fig. 2.

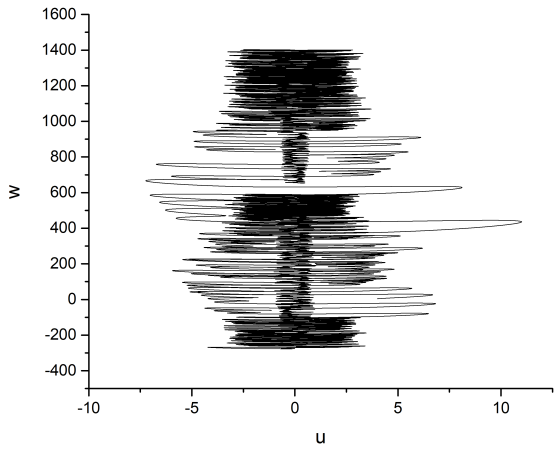

Figura 8: Proyección de la trayectoria del receptor en el plano u-w, forzando la variable w. Se observa como esta difiere respecto a la de la Fig. 3.

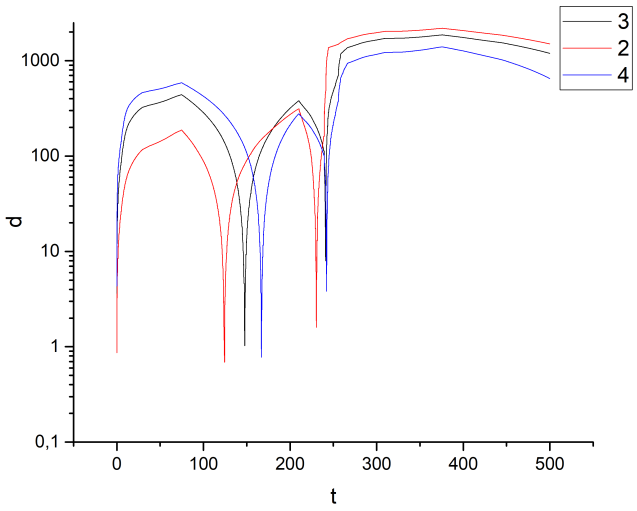

Figura 9: Gráfico $d(t)$ forzando la variable w en lugar de u. Se observa como, a excepción de unas ventanas temporales donde la distancia entre trayectorias disminuye, esta tiende a aumentar con el tiempo.

Como se observa en la Fig. 9 si en lugar de forzar el sistema del receptor con $u(t)$ se lo fuerza con $w(t)$, su trayectoria no converge a la del emisor por lo que podemos afirmar que el sistema no se sincroniza, y por lo tanto no resulta de utilidad para encriptar un mensaje.

Lo último que se estudió fue la dependencia del error de encriptado en función de la frecuencia f del mensaje, y para llevar esto a cabo se encriptó un mensaje $m(t) = \sin(2\pi f\, t)$ y se forzó el sistema del receptor con el mensaje encriptado $s(t) = u(t) + \epsilon\, m(t)$, usando $\epsilon = 0,01$ para que la amplitud del seno sea pequeña en relación a la variable caótica. Luego en el sistema del receptor se reconstruyó el mensaje mediante $m'(t) = s(t) - u_r(t)$ y se graficó el error de desencriptado, definido como $m - m'$, en función de la frecuencia (Fig. 10).

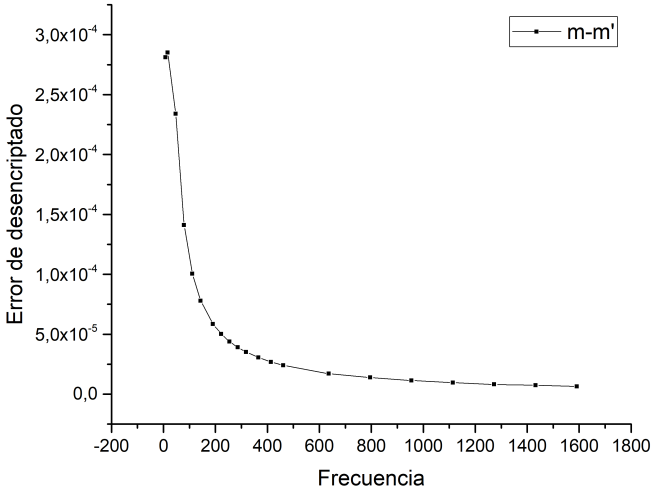

Figura 10: Error de desencriptado en función de f. Se observa como la diferencia entre el mensaje original y el desencriptado (reescaleado para que coincidan en amplitud) disminuye a medida que aumenta la frecuencia del mensaje.

Como se puede ver, el error que el sistema le suma al mensaje disminuye velozmente a medida que aumenta la frecuencia. Esto se debe a que el método de encriptado introduce un error de baja

frecuencia, por lo que si la señal enviada tiene una frecuencia en este orden el error se hace mucho mas notable en relación a frecuencias mas altas, donde se observa que el error disminuye de gran manera.

3.2. Encriptado de mensaje de audio[1]

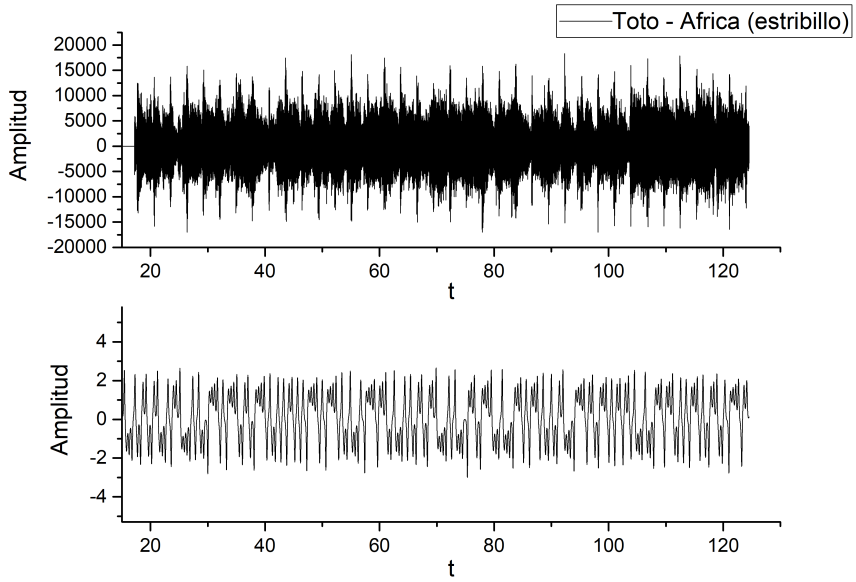

Figura 11: Arriba: Visualización del archivo de audio en formato .WAV, corresponiente al estribillo de la canción "Africa" de Toto $\big(m(t)\big)$ [4].
Abajo: Visualización del audio encriptado $\big(s(t)\big)$.

Para ilustrar el funcionamiento del sistema emisor-receptor se encriptó el fragmento de una canción $m(t)$ (Fig. 11), y luego de desencriptarlo se observaron en un mismo gráfico $m(t)$ y $m'(t)$ con el fin de compararlas (Fig. 12). También se graficó el ruido inducido por el método de encriptado para compararlo con el mensaje en sí (Fig. 13).

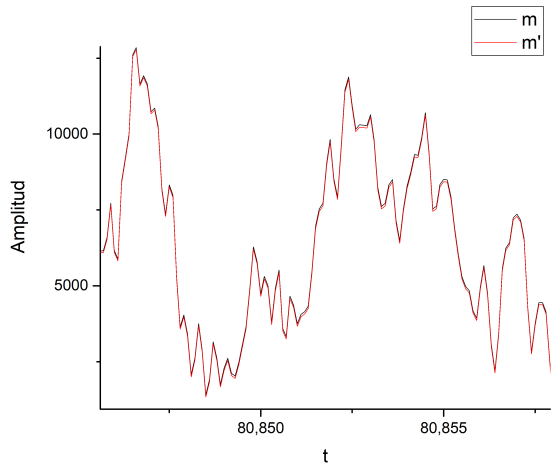

Figura 12: Acercamiento sobre una sección del gráfico. Se puede observar como el mensaje desencriptado se acerca con mucha precisión al original.

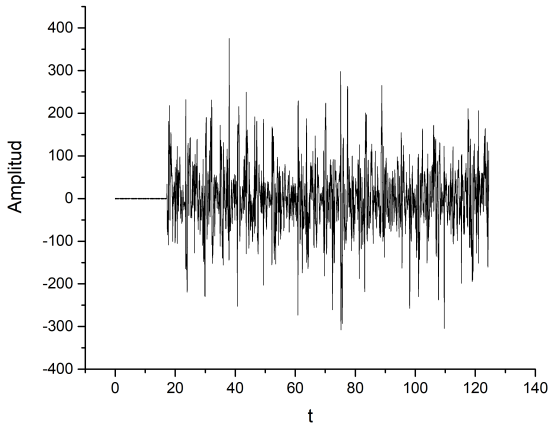

Figura 13: Ruido inducido sobre el mensaje por el método de encriptado.

[1] Audios original, encriptado y desencriptado:
https://drive.google.com/drive/folders/1n_VA-J1XIGLhU_-wmj14w-z1ZL0W33Pb?usp=sharing

En la Fig. 12 se puede notar la cantidad de cambios en la amplitud que ocurren en un muy breve período de tiempo, lo cual se debe a la alta frecuencia de grabación del mensaje de aproximadamente 226, 76 KHz. Por esto, como podemos ver en la Fig. 13 la amplitud del ruido inducido sobre el mensaje por el método de encriptado oscila entre aproximadamente -300 y 400 mientras que la amplitud de la canción oscila entre -18000 y 18000, lo cual resulta en un error de desencriptado de $\simeq 2\,\%$.

Sin embargo, al escuchar el audio encriptado se puede distinguir el mensaje original con volumen muy reducido, montado sobre un ruido fuerte de baja frecuencia (lo cual es esperado debido al procedimiento aplicado para enmascarar la canción), por lo que si el mensaje encriptado es interceptado, la señal original podría filtrarse con un filtro pasa-altos. A partir de esto surge una limitación del sistema de encriptado, y permite argumentar que para encriptar un mensaje resultaría mas eficiente un método que distorsione la señal en lugar de enmascararla, ya que la diferencia notable de frecuencias podría permitir filtrarlo.

Una posible solución sería definir un intervalo de sampleo S no necesariamente igual al paso de Runge-Kutta h, y de esta manera enmascarar (y desenmascarar) la señal con puntos cada cierta distancia sobre el atractor en lugar de punto a punto. De esta forma resultaría posible ajustar la frecuencia de la variable caótica para hacerla mas cercana a la del mensaje, y dificultar así el filtrado del mensaje encriptado mediante un filtro pasa-altos (Figs. 14 y 15).

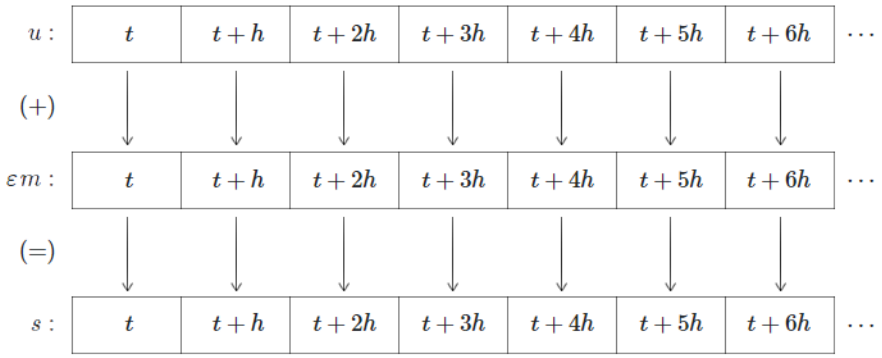

Figura 14: Esquema del método utilizado, enmascarando el mensaje punto a punto con la variable caótica.

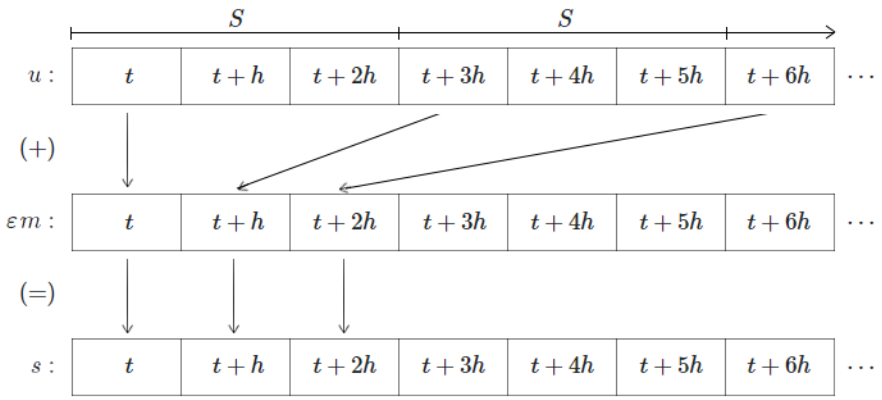

Figura 15: Esquema del método sugerido, enmascarando el mensaje cada cierto intervalo de sampleo S de la variable caótica para así ajustar su frecuencia y utilizar una comparable a la de la señal a encriptar.

4. Conclusiones

Se estudiaron algunas características de la auto-sincronización del sistema de Lorentz. Respecto a esto se observó que, si bien no todas, es posible forzar algunas de las variables caóticas del sistema para hacer tender asintóticamente la trayectoria del sistema forzado a la del forzador. En estos casos se vio que la convergencia asintótica es independiente de las condiciones iniciales, lo cual resulta de mucho interés debido a que los sistemas caóticos son principalmente identificados por la sensibilidad a las condiciones iniciales.

Una posible aplicación de los sistemas caóticos con esta propiedad es el encriptado de señales, y mediante el encriptado y desencriptado de funciones senoidales de distinta frecuencia se observó la dependencia del error inducido por el método en función de la frecuencia del mensaje enviado, y se notó que este disminuye de gran manera a medida que aumenta la frecuencia.

Por último se encriptó el estribillo de una famosa canción y graficando la señal enviada junto a la desencriptada, y notando la amplitud del error en función del tiempo, se concluye que el método propuesto funciona relativamente bien para recuperar el mensaje encriptado.

Una sugerencia para quienes deseen experimentar con este método de encriptación sería implementar el sistema definiendo una distancia de sampleo en el atractor del sistema para enmascarar la señal en lugar de hacerlo punto a punto, estudiar el error de desencriptado en función del tamaño de sampleo, y de esta manera obtener frecuencias similares entre el mensaje y la máscara para dificultar el desencriptado por simple filtrado (y en base al error considerar si esta propuesta es una solución factible a la limitación mencionada del sistema).

5. Referencias

[1] *https://getsmart.fandom.com/wiki/KAOS*, accedido 6/10/2020.

[2] *"Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications"*, Kevin M. Cuomo, Alan V. Oppenheim, Steven H. Strogatz, 1993.

[3] *"The statistical prediction of solutions of dynamic equations"*, Edward N. Lorentz, 1960.

[4] *"Africa"* by Toto. Toto IV, 1982.