

Resumen

En esta tesis se formula un sistema no lineal para la encriptación y desencriptación de señales de información por métodos caóticos de cifrado. El sistema consiste de dos bloques: encriptador y desencriptador, cuya dinámica es caótica. Tales bloques se sincronizan al convertir el desencriptador en un observador no lineal del encriptador, y al estar sincronizados el desencriptador puede recobrar la señal de información.

Además, se realiza el diseño de un circuito que lleve a cabo la dinámica del sistema formulado. El sistema caótico que se usa es el de tirón debido a su sencillez y ventajas estructurales que presenta: las no linealidades del circuito que se usan son lineales por partes y hay pocas sumas en el sistema, lo que se traduce en un número reducido de componentes electrónicos.

Se llevan a cabo simulaciones del criptosistema diseñado para caracterizar el comportamiento del mismo en distintos escenarios. Por último se plantean ciertos requerimientos acerca de la función de encriptación, la energía de la señal de información y la relación señal a ruido en el canal para lograr una comunicación segura con una baja relación señal a ruido.