

Encriptación de Sonidos basado en los Sistemas Caóticos de Lorenz y Rössler

Cristopher Sebastián García Pacheco

Universidad Nacional de Ingeniería. Facultad de Ciencias.
Escuela Profesional de Ciencias de la Computación.

7 de enero de 2022



Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias



Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias



Introducción.

Cuando se habla de encriptación, se busca trabajar en el fundamento de confidencialidad desde el enfoque de seguridad informática.

En esta tesis, se propone distorsionar un archivo de sonido, de tal forma que no se pueda reproducir el sonido original a simple vista, y tras aplicar el algoritmo de descifrado con las claves correctas, podemos obtener el sonido original. Existen muchas formas de encriptación de sonidos, en esta tesis se propone aplicar una transformación de sonido a imagen, y posteriormente aplicar las propiedades de los Sistemas Caóticos de Lorenz y Rössler para permutar las filas y columnas de la imagen.

Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias



Sistema Caótico de Lorenz.

Es un sistema de ecuaciones diferenciales estudiado por primera vez por Edward Lorenz en 1963 [1].

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = x(c - x) - y \\ \frac{dz}{dt} = -bz + xy \end{cases} \quad (1)$$

Donde $a = 10$, $b = 8/3$ y $c = 28$ para que el sistema de ecuaciones presente un comportamiento caótico.

Sistema Caótico de Lorenz.

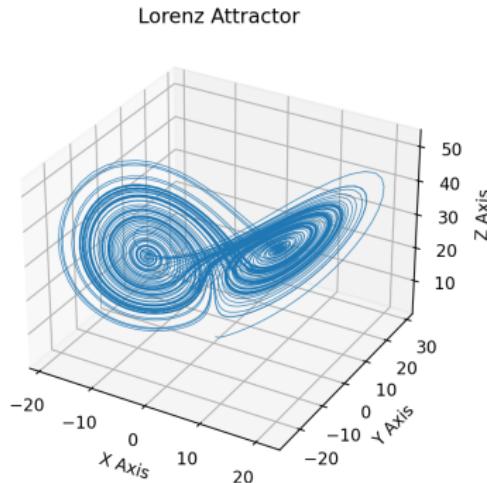


Figura: Sistema Caótico de Lorenz con $a = 10$, $b = 8/3$ y $c = 28$ [2].



Sistema Caótico de Rössler.

Es un sistema de tres ecuaciones diferenciales ordinarias no lineales. El Sistema de Rössler es de naturaleza similar al Sistema de Lorenz [3].

$$\begin{cases} \frac{dx}{dt} = -(y + z) \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = b + xz - cz \end{cases} \quad (2)$$

Donde $a = 0,2$, $b = 0,2$ y $c = 8,0$ para que el sistema de ecuaciones presente un comportamiento caótico.

Sistema Caótico de Rössler.

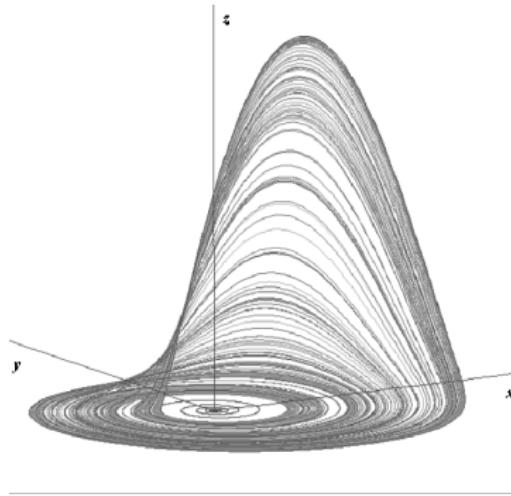


Figura: Sistema Caótico de Rössler con $a = 0,2$, $b = 0,2$ y $c = 8,0$ [4]



A New Audio Encryption Algorithm Based on Chaotic Block Cipher

Este trabajo propone un algoritmo de encriptación basado en combinación entre bloques de cifrado y mapas caóticos. [5].

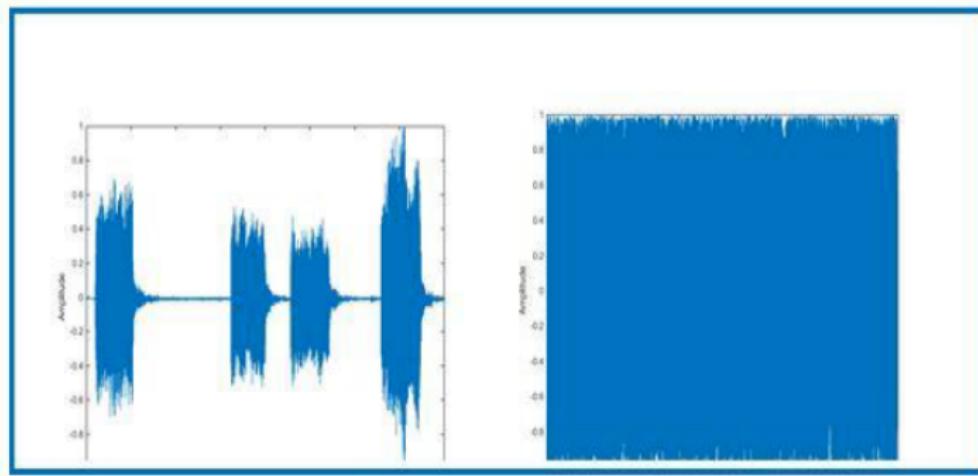


Figura: Gráfico de forma de onda de audio original y encriptado.

An Audio Encryption Algorithm Based on DNA Coding and Chaotic System

Este trabajo propone un método de encriptación de audios basado en sistemas caóticos y códigos de ADN para realizar procesos de confusión y difusión a los audios. [6].

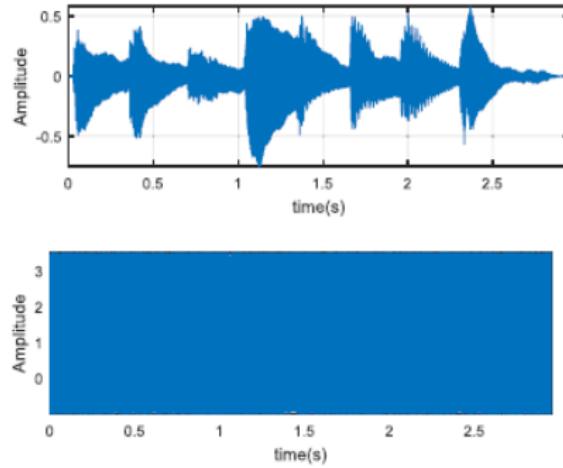


Figura: Gráfico de forma de onda de audio original y encriptado.

Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias



Encriptación de sonido.

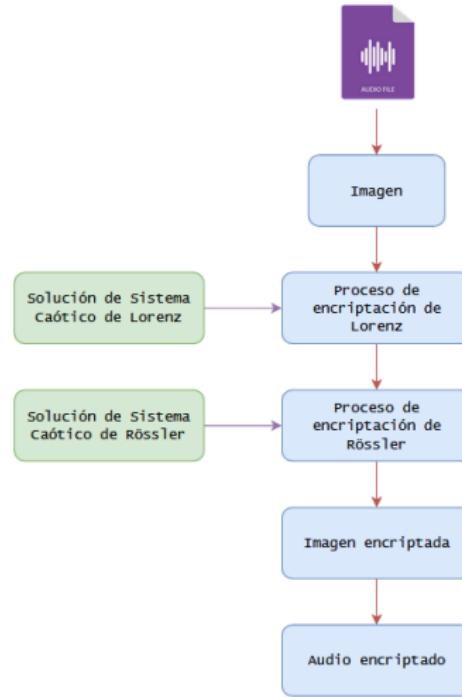


Figura: Proceso de encriptación de sonido. Fuente: Elaboración propia



UNIVERSIDAD
NACIONAL DE
INGENIERÍA

Descifrado de sonido.

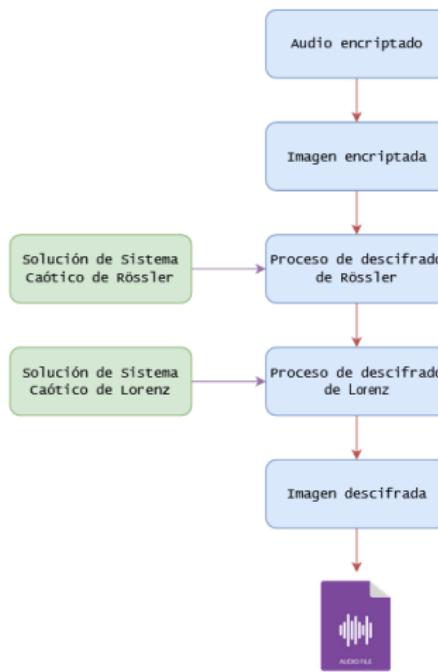


Figura: Proceso de descifrado de sonido. Fuente: Elaboración propia



Aplicación del algoritmo.

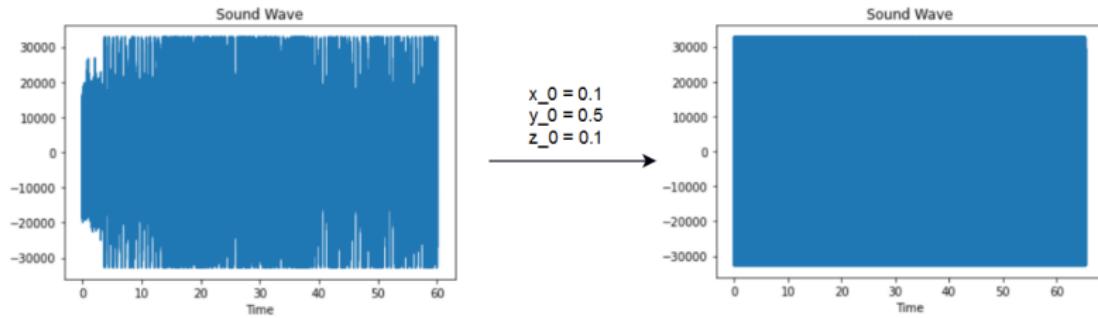


Figura: Aplicación del algoritmo de encriptación de sonido a un audio de 30 segundos.

Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias



Performance.

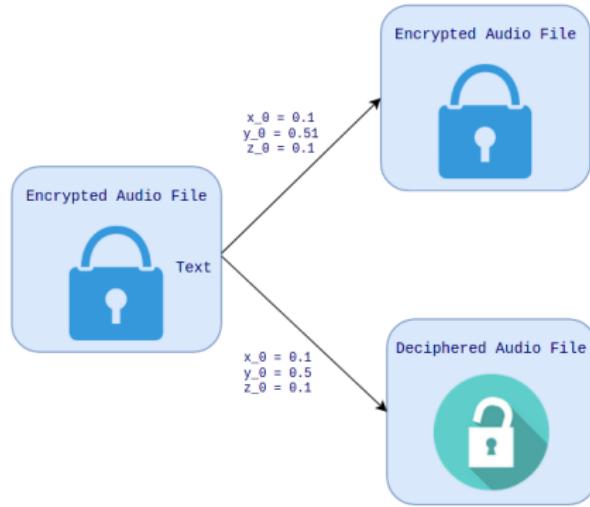


Figura: Descifrado con claves correctas e incorrectas . Fuente: Elaboración propia.

Métricas.

Cuadro: Proceso de encriptación de sonido.

Audio Original	Conversión a Imagen
	
Encriptación	Conversión a Audio
	

Correlación entre píxeles adyacentes.

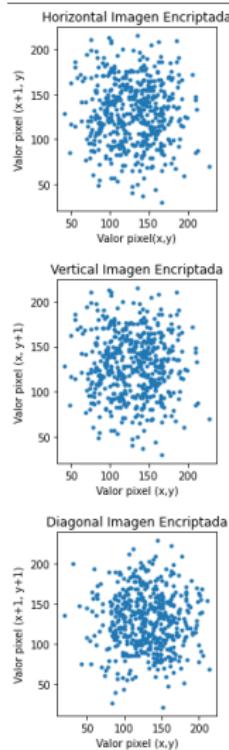


Figura: Análisis de correlación entre píxeles adyacentes.

Correlación entre píxeles adyacentes.

Cuadro: Valores de correlación de píxeles adyacentes.

Imagen	Horizontal	Vertical	Diagonal
Imagen original (audio)	0.98764	0.97489	0.98612
Imagen encriptada	0.00331	-0.01581	0.02512

Entropía.

Cuadro: Valor de entropía.

Imagen encriptada	Entropia
Blinding Lights (image)	7.6413

Comparación con otros algoritmos.

Cuadro: Comparación de correlación de pixeles adyacentes de distintos algoritmos.

Imagen encriptada	Horizontal	Vertical	Diagonal
Algoritmo propuesto	-0.00159	0.01847	0.01904
Algoritmo de Khalid M. Hosny [7]	-0.0182	-0.0108	0.0165
Algoritmo de Sumit, Rajib y Bhaskar Panna. [8]	0.0944	0.0057	0.0067
Algoritmo de Zhongyun, Shuang y Yicong. [9]	0.0098	-0.0078	0.0181

Análisis de tiempo de ejecución.

Cuadro: Tiempo de ejecución del algoritmo propuesto para audios de 30 segundos.

Cantidad de imágenes	Tiempo de ejecución
1	12.512 s
10	130.359 s
100	1305.786 s

Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias

Conclusiones.

- La propiedad caótica de los Sistemas Caóticos optimiza los procesos de encriptación de sonidos si se procede con un algoritmo que aproveche esta propiedad.
- El algoritmo de encriptación propuesto cumple con los estándares de seguridad según las métricas mostradas en el capítulo anterior.
- El algoritmo de encriptación propuesto está al nivel de los demás algoritmos de encriptación, comparando las métricas con otros algoritmos de referencia.

Trabajo a Futuro.

Una de las razones por las que se desarrolló la presente tesis, fue para aplicarla al sonido de videos, y adaptarlo a un algoritmo de encriptación de videos; por lo que el punto principal es obtener un algoritmo que se pueda optimizar en tiempo de ejecución porque se debe aplicar a un video. Por supuesto, que al aplicar este algoritmo de encriptación a videos, se debe sincronizar con otro algoritmo para encriptar los frames del video; por tal motivo, antes de desarrollar este algoritmo de encriptación de videos, se ha desarrollado un algoritmo de encriptación de imágenes basado igualmente en Sistemas Caóticos.

Contenido

- 1 Introducción
- 2 Conocimientos Previos
- 3 Estructuración y método
- 4 Resultados
- 5 Conclusiones y Trabajo Futuro.
- 6 Referencias



Referencias I

- [1] George Lindfield y John Penny. *Solution of Differential Equations*. URL: <https://www.sciencedirect.com/topics/mathematics/lorenz-system>.
- [2] Darren Dale John Hunter, Michael Droettboom Eric Firing y the Matplotlib development team. *Lorenz Attractor*. 2012. URL: https://matplotlib.org/devdocs/gallery/mplot3d/lorenz_attractor.html.
- [3] Comsol. *Rössler Attractor*. URL: <https://www.comsol.com/model/r-ssler-attractor-10656>.
- [4] Wolfram Mathworld. *Rössler Attractor*. URL: <https://mathworld.wolfram.com/RoesslerAttractor.html>.

Referencias II

- [5] Ekhlas Albahrani. «A new audio encryption algorithm based on chaotic block cipher». En: mar. de 2017, págs. 22-27. DOI: 10.1109/NTICT.2017.7976129.
- [6] Xingyuan Wang y Yining Su. «An Audio Encryption Algorithm Based on DNA Coding and Chaotic System». En: *IEEE Access* 8 (2020), págs. 9260-9270. DOI: 10.1109/ACCESS.2019.2963329.
- [7] Khalid M. Hosny Sara T. Kamal,
Mohamed M. Darwish Taha M. Elgindy y Mostafa M. Fouad. *A New Image Encryption Algorithm for Grey and Color Medical Images*. URL: <https://ieeexplore.ieee.org/document/9366688>.
- [8] Sumit Kumar, Rajib Kumar Jha y Bhaskar Panna. «Medical Image Encryption Using Fractional Discrete Cosine Transform with Chaotic Function». En: *Medical Biological Engineering Computing* (ago. de 2019). DOI: 10.1007/s11517-019-02037-3.

Referencias III

- [9] Zhongyun Hua, Shuang Yi y Yicong Zhou. «Medical image encryption using high-speed scrambling and pixel adaptive diffusion». En: *Signal Processing* 144 (oct. de 2017). DOI: [10.1016/j.sigpro.2017.10.004](https://doi.org/10.1016/j.sigpro.2017.10.004).