

Encriptación de Imágenes basado en los Atractores Caóticos de Lorenz y Rössler

Cristopher Sebastián García Pacheco

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

9 de agosto de 2021



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

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 la imagen de tal forma que no se pueda reconocer la imagen original a simple vista, y tras aplicar el algoritmo de descifrado con las claves correctas, podemos obtener la imagen original. Existen muchas formas de encriptación de imágenes, en esta tesis se propone aplicar las propiedades del Sistema Caótico de Lorenz y el Sistema Caótico de Rössler para encriptar una imagen utilizando un algoritmo de permutación de filas y columnas.



Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

Atractor 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.



Atractor Caótico de Lorenz.

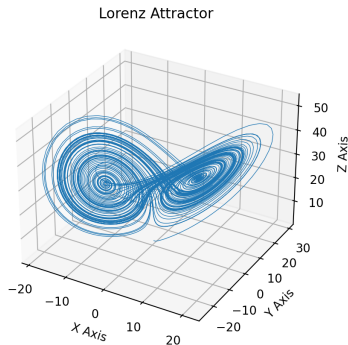


Figura: Sistema Caótico de Lorenz con $a = 10$, $b = 8/3$ y $c = 28$ [2].

Atractor Caótico de Rössler.

Un atractor de Rössler es un sistema de tres ecuaciones diferenciales ordinarias no lineales. El atractor de Rössler es de naturaleza similar al atractor 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.



Atractor Caótico de Rössler.

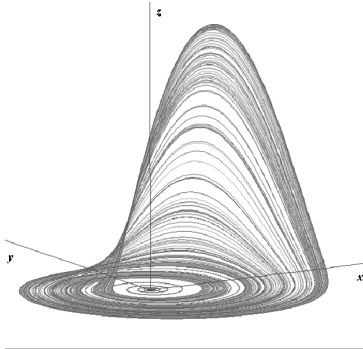



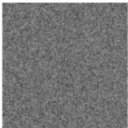
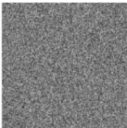

Figura: Sistema Caótico de Rössler con $a = 0,2$, $b = 0,2$ y $c = 8,0$ [4]



UNIVERSIDAD
NACIONAL DE
INGENIERÍA

Algoritmo de Encriptación de Imágenes Utilizando el Atractor Caótico de Lorenz.

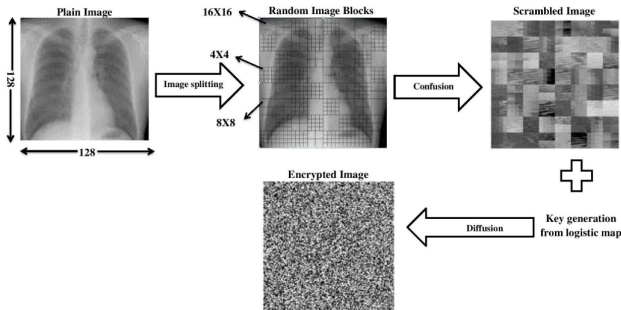
Este trabajo propone un algoritmo de encriptación basado en el Atractor Caótico de Lorenz para imágenes a escala de grises [5].

<i>Imagen Original</i>	<i>Permutada</i>	<i>Cifrada</i>	<i>Decodificada</i>
			



A New Image Encryption Algorithm for Grey and Color Medical Images.

Este trabajo propone un método de encriptación basados en los procesos de confusión y difusión para imágenes a escala de grises y a color [6].



Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

Encriptación de la imagen.

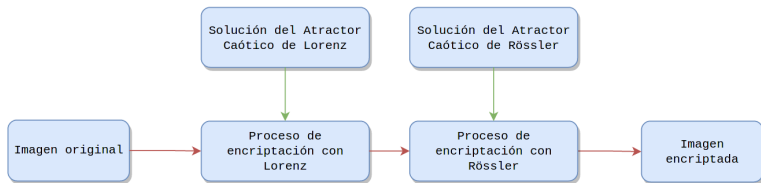


Figura: Proceso de encriptación de imagen. Fuente: Elaboración propia.



Descifrado de la imagen.

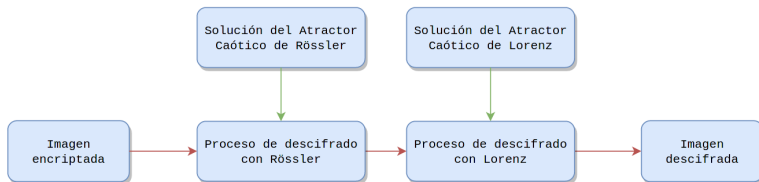


Figura: Proceso de descifrado de imagen. Fuente: Elaboración propia.



Aplicación del algoritmo.

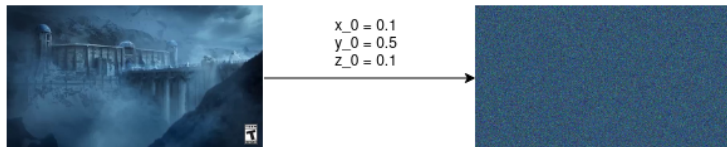


Figura: Aplicación del algoritmo de encriptación de imagen a color.

Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

Performance.

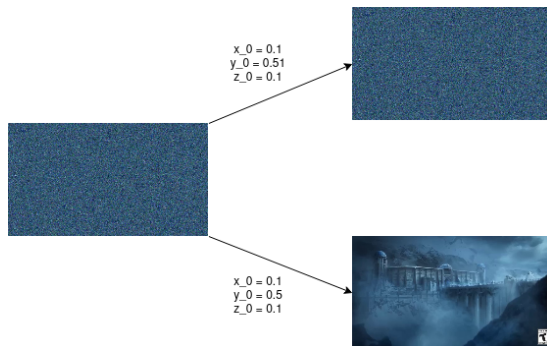
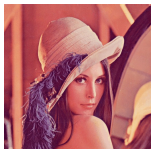


Figura: Descifrado con claves correctas e incorrectas . Fuente: Elaboración propia.



(a) Lena original.



(b) Lena encriptado.

Figura: Imagen "Lena", tamaño 512x512.



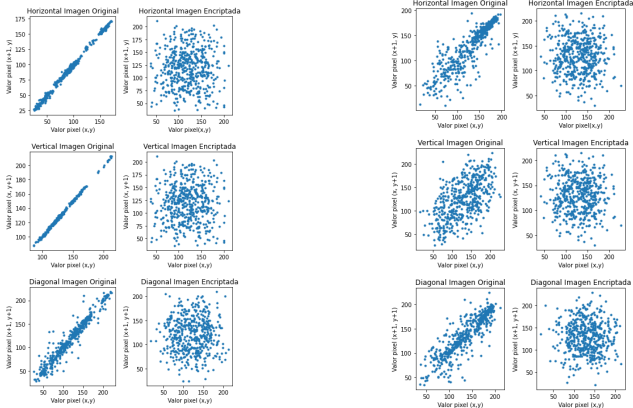
(a) Baboon original.



(b) Baboon encriptado.

Figura: Imagen "Baboon", tamaño 512x512.

Correlación entre píxeles adyacentes.



(a) Correlación entre píxeles adyacentes de la imagen Lena.

(b) Correlación entre píxeles adyacentes de la imagen Baboon.

Figura: Análisis de correlación entre píxeles adyacentes.

Correlación entre píxeles adyacentes.

Cuadro: Valores de correlación de pixeles adyacentes.

Imagen	Horizontal	Vertical	Diagonal
Lena original	0.99784	0.99859	0.96335
Lena encriptado	-0.00271	0.02619	0.02029
Baboon original	0.89109	0.57361	0.86805
Baboon encriptado	-0.10606	-0.03397	-0.01724



Cuadro: Valores de entropía.

Imagen encriptada	Entropía
Lena	7.4321
Baboon	7.3738



Comparación con otros algoritmos.

Cuadro: Comparación de correlación de pixeles adyacentes.

Imagen encriptada	Horizontal	Vertical	Diagonal
Lena	-0.00271	0.02619	0.02029
Baboon	-0.10606	-0.03397	-0.01724
[6]	-0.0182	-0.0108	0.0165
[7]	0.0944	0.0057	0.0067
[8]	0.0098	-0.0078	0.0181



Análisis de tiempo de ejecución.

Cuadro: Tiempo de ejecución con varias imágenes.

Cantidad de imagenes	Tiempo de ejecución
1	1.967 s
10	20.587 s
100	210. 541 s
500	1059.152 s



Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

Conclusiones.

- La propiedad caótica de los Atractores Caóticos optimiza los procesos de encriptación 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.



Una de las razones por las que se desarrolló la presente tesis, fue para aplicarla a los frames de videos, y adaptarlo a un algoritmo de encriptación de videos. Por supuesto que al aplicar este algoritmo de encriptación a videos, se debe sincronizar con otro algoritmo para encriptar sonidos; por tal motivo, antes de desarrollar un algoritmo de encriptación de videos, se debe investigar previamente algún método de encriptación de sonido.



Contenido

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



**UNIVERSIDAD
NACIONAL DE
INGENIERÍA**

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>.

- [5] Iván Rodríguez y col. «Algoritmo de Encriptación de Imágenes Utilizando el Atractor Caótico de Lorenz». En: *Ingeniería* 22 (sep. de 2017), pág. 396. DOI: 10.14483/23448393.11976.
- [6] Khalid M. Hosny Sara T. Kamal, Mohamed M. Darwish Taha M. Elgindy y Mostafa M. Fouda. *A New Image Encryption Algorithm for Grey and Color Medical Images*. URL: <https://ieeexplore.ieee.org/document/9366688>.
- [7] 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.
- [8] 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.