NÚMEROS SEUDOALETORIOS GENERADOS POR EL MAPEO LOGÍSTICO MODIFICADO Y SU APLICACIÓN EN LA ENCRIPTACIÓN DE IMÁGENES

Autor: **Sara Apolinar Crisanto**, Director: **Daniel Roberto Jardón Arcos**
Universidad Autónoma de la Ciudad de México

1 INTRODUCCIÓN

Distintos autores han publicado artículos en los que utilizan las propiedades caóticas de algunos mapeos para encriptar imágenes definidas por píxeles, en tonos de grises o a color.
La idea principal de este trabajo es utilizar modificaciones del bien ya conocido mapeo logístico $f(x) = \lambda x(1-x)$, que sea capaz de generar secuencias seudoaleatorias con mejores propiedades estadísticas a los obtenidos con el mapeo logístico normal. Posteriormente encriptar imágenes a tonos de gris con dichas secuencias.

2 MAPEO LOGÍSTICO

La función logística viene de la ecuación diferencial propuesta por Pierre Francois Verhulst.
$\frac{dx}{dt} = \lambda x(1-x)$
De manera sistemática ha sido estudiado el mapeo asociado $f(x) = \lambda x(1-x)$ en el intervalo $x \in (0,1)$ y $\lambda \in (0,4)$

El mapeo logístico modificado

La modificación factor $10,000$, es la función $f : [0,1] \to [0,1]$ que se define por:

$$f(x) = 10,000\lambda x(1-x) - [10,000\lambda x(1-x)]$$

donde $[a]$ es la parte entera de a.

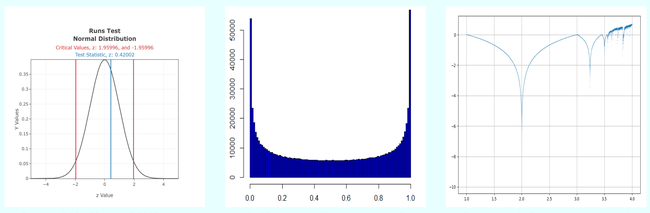
3 ANÁLISIS ESTADÍSTICO

- **Aleatoriedad**
  La prueba de rachas determina, con cierta nivel de confianza, si es aleatorio el orden de aparición de dos valores de una variables considerando dos resultados, es decir los valores por encima o debajo de la mediana.
  $H_0 =$ Existe aleatoriedad.
  $H_1 =$ No existe aleatoriedad.

- **Uniformidad**
  La prueba de chi-cuadrada busca determinar si los números de un conjunto $\{r_i = i : 1, ..., n\}$ se distribuyen de acuerdo a cierta distribución, en nuestro caso la distribución uniforme en el intervalo $[0,1]$.
  $H_0 =$ Existe uniformidad en $[0,1]$.
  $H_1 =$ No existe uniformidad en $[0,1]$.

- **Exponentes de Lyapunov**
  Los exponentes de Lyapunov reflejan la sensibilidad a las condiciones iniciales.
  $Lya(x_0) = \lim_{n\to\infty} \frac{1}{n}\sum_{k=0}^{n-1} \ln|f'(x_k)|$ (exponente de Lyapunov x_0)
  - Si $Lya(x_0) > 0$, con $x_0 \in x$, se tiene sensibilidad a condiciones iniciales.
  - Si $Lya(x_0) < 0$, con $x_0 \in x$, no se tiene sensibilidad a condiciones iniciales.

Mapeo Logístico
$f(x) = \lambda x(1-x)$



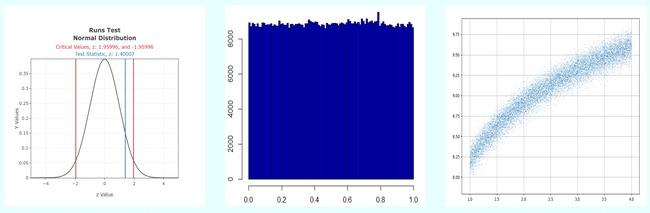
(a) Con $x_0 = 0.074135$ y $\lambda = 3.9999$, se obtiene p-valor= 0.6745

(b) Histograma uniforme recreado en R

(c) Exponentes de Lyapunov para $\lambda \in (1{,}4 : 20000)$

Figura 1: Simulaciones en *Statdisk*,*R* y *Phyton*.

Mapeo Logístico Modificado
$f(x) = 10000\lambda x(1-x) - [10000\lambda x(1-x)]$



(a) Con $x_0 = 0.074135$ y $\lambda = 3.9999$, se obtiene p-valor = 0.5598

(b) Histograma uniforme recreado en R

(c) Exponentes de Lyapunov para $\lambda \in (1{,}4 : 20000)$

Figura 2: Simulaciones en *Statdisk*,*R* y *Phyton*.

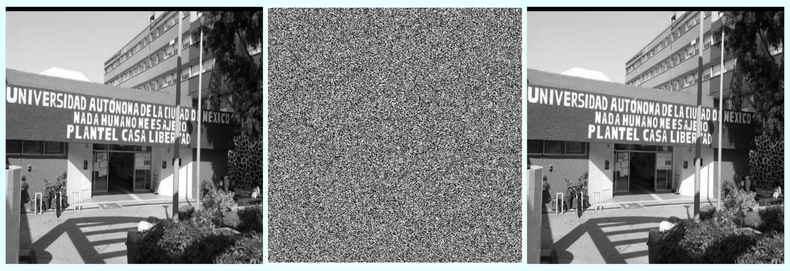
4 ENCRIPTACIÓN DE IMÁGENES MÓDULO 1

(a) Diagrama de flujo encriptado

(b) Diagrama de flujo desencriptado

Figura 3: 820×1082

Mapeo Logístico Modificado
$f(x) = 10000\lambda x(1-x) - [10000\lambda x(1-x)]$
$\lambda = 3.999916$ puntos semilla $x_0 = 0.125148$ y $x_0 = 0.160126$



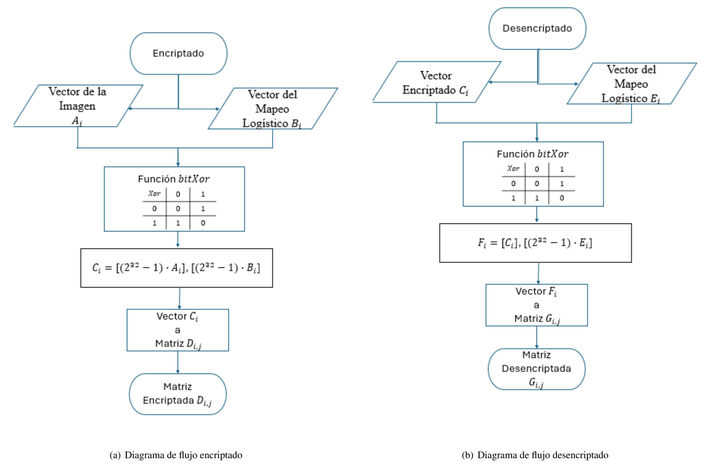
(a) Imagen original

(b) Imagen encriptada método suma módulo 1

(c) Imagen desencriptada

Figura 4: 820×1082

5 MÉTODO XOR

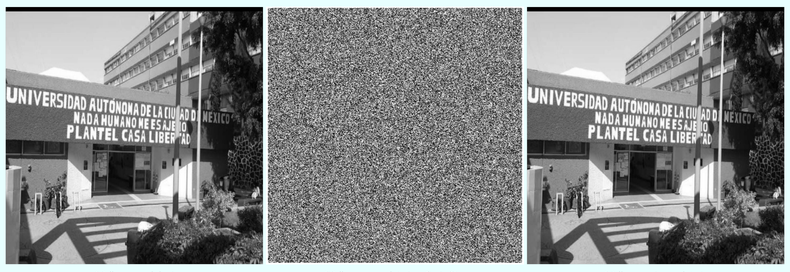


(a) Diagrama de flujo encriptado

(b) Diagrama de flujo desencriptado

Figura 5: 820×1082

Mapeo Logístico Modificado
$f(x) = 10000\lambda x(1-x) - [10000\lambda x(1-x)]$
$\lambda = 3.999916$ puntos semilla $x_0 = 0.125148$ y $x_0 = 0.160126$



(a) Imagen original

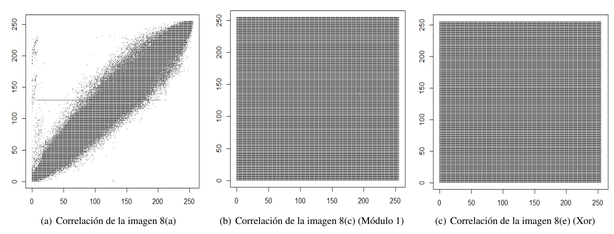
(b) Imagen encriptada método *Xor*

(c) Imagen desencriptada

Figura 6: 820×1082

6 ANÁLISIS DEL ALGORITMO

- **Correlación entre los píxeles vecinos**
  El coeficiente de correlación de Pearson, es un índice que mide el grado de correlación entre dos variables relacionadas. El coeficiente de correlación toma valores entre -1 y 1.
  - valores cercanos a -1, 1 indica correlación lineal alta,
  - valores cercanos a 0, indica la correlación lineal baja.



(a) Correlación de la imagen 8(a)

(b) Correlación de la imagen 8(c) (Módulo 1)

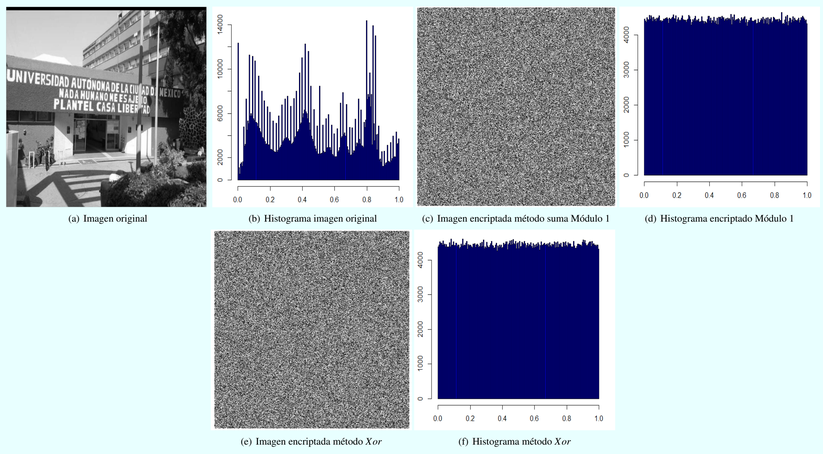
(c) Correlación de la imagen 8(e) (Xor)

Figura 7: Correlación dentro de la matriz.

Imagen		Módulo 1		Xor	
Correlación	p-valor	Correlación	p-valor	Correlación	p-valor
0.986186	2.2×10^{-16}	-0.001032578	0.3307	0.0006583353	0.5352

Tabla 1: Análisis de correlación píxeles vecinos

- **Histograma de Píxeles**



(a) Imagen original

(b) Histograma imagen original

(c) Imagen encriptada método suma Módulo 1

(d) Histograma encriptado Módulo 1

(e) Imagen encriptada método *Xor*

(f) Histograma método *Xor*

Figura 8: 820×1082.

Secuencia de Píxeles

- Aleatoriedad
  H_0 : Existe aleatoriedad.
  H_1 : No existe aleatoriedad.

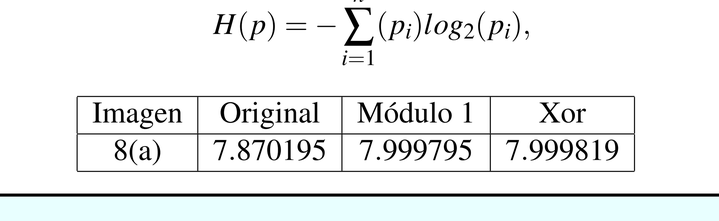
Imagen	Original	Módulo 1	Xor
8(a)	$p-valor = 2.2 \times 10^{-16}$	$p-valor = 0.2072$	$p-valor = 0.9391$

- Uniformidad
  Prueba de Kolmogorov-Smirnov:
  H_0: La secuencia tiene una distribución uniforme $[0,1]$.
  H_1: La secuencia no tiene una distribución uniforme $[0,1]$.

Imagen	Original	Módulo 1	Xor
8(a)	$p-valor = 2.2 \times 10^{-16}$	$p-valor = 0.27$	$p-valor = 0.1887$

- **Análisis de sensibilidad en las llaves**
  Para tener un buen cifrado se debe contar con una cantidad grande de llaves para no sea fácil su ataque utilizando la fuerza bruta para obtener la llave correcta.
  Con ambos métodos se pueden obtener 4 llaves; los puntos iniciales x_0 y dos $\lambda \in (3.9999, 4)$, es decir:

$$10^{15} \times 10^{15} \times 10^{11} \times 10^{11} = 10^{52} \approx 2^{172}.$$



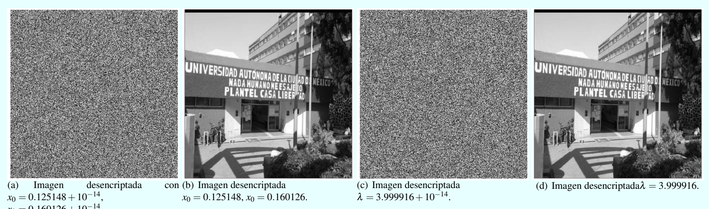
(a) Imagen desencriptada con $x_0 = 0.125148 + 10^{-14}$, $x_0 = 0.160126 + 10^{-14}$.

(b) Imagen desencriptada $x_0 = 0.125148$, $x_0 = 0.160126$.

(c) Imagen desencriptada $\lambda = 3.999916 + 10^{-14}$.

(d) Imagen desencriptada$\lambda = 3.999916$.

Figura 9: Módulo 1, 820×1082.



(a) Imagen desencriptada con $x_0 = 0.125148 + 10^{-14}$, $x_0 = 0.160126 + 10^{-14}$.

(b) Imagen desencriptada $x_0 = 0.125148$, $x_0 = 0.160126$.

(c) Imagen desencriptada $\lambda = 3.999916 + 10^{-14}$.

(d) Imagen desencriptada$\lambda = 3.999916$.

Figura 10: Xor, 820×1082.

- **Entropía de Shannon**
  - La entropía máxima = 8, no hay una secuencia determinista.

$$H(p) = -\sum_{i=1}^{n}(p_i)log_2(p_i),$$

Imagen	Original	Módulo 1	Xor
8(a)	7.870195	7.999795	7.999819

- **Tasa de cambio de píxeles**
  La tasa de cambio de número de píxeles o NPCR (Number of Pixels Change Read) siglas en inglés. Indica el % de píxeles que presentan un cambio en el tono de gris.

$$d(i,j) = \begin{cases} 1 & \text{si } C_1(i,j) \neq C_2(i,j), \\ 0 & \text{si } C_1(i,j) = C_2(i,j) \end{cases} \quad NPCR = \sum_{i,j}\frac{d(i,j)}{S} \times 100\%,$$

Original vs Encriptada		Original vs Desencriptada	
Módulo 1	Xor	Módulo 1	Xor
99.60811%	99.60304%	0%	0.0001127091%

7 CONCLUSIONES

Mediante las pruebas realizadas obtuvimos que el mapeo logístico modificado con factor 10,000 es un mejor generador de números seudoaleatorios, además de contar con mayor sensibilidad a las condiciones iniciales que el mapeo logístico normal.
El algoritmo propuesto para la encriptación de imágenes en tonos de gris, utilizando el mapeo logístico modificado, nos muestra eficiencia en su seguridad, robustez ante un ataque utilizando la fuerza bruta, además de tener resultados favorables en las pruebas estadísticas realizadas.

BIBLIOGRAFÌA

[1] Dávalos, J. E. K., & Lango, H. M. (2014). Sistemas Dinámicos Discretos. UNAM, Facultad de Ciencias.
[2] Devaney, R. L. (2021). An introduction to chaotic dynamical systems. CRC press.
[3] Gonzales, R. C., & Wintz, P. (1987). Digital image processing. Addison-Wesley Longman Publishing Co., Inc..
[4] Triola, M. F. (2000). Estadística elemental.
[5] Wackerly, D., Mendenhall, W., & Scheaffer, R. L. (2014). Mathematical statistics with applications. Cengage Learning.
[6] Zhao, Y., & Liu, L. (2021). A bit shift image encryption algorithm based on double chaotic systems. Entropy, 23(9), 1127.