Conference: Interdisciplinary Congress of Renewable Energies, Industrial Maintenance, Mechatronics and Information Technology

BOOKLET

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - E-Revistas - Google Scholar

DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: Sistema de cifrado parcial dinámico para imágenes digitales

Authors: RODRIGUEZ-CARDONA, Gustavo, RAMIREZ-BELTRAN, Leonardo Humberto y RAMIREZ-TORRES, Marco Tulio.

Editorial label ECORFAN: 607-8695
BCIERMMI Control Number: 2019-031
BCIERMMI Classification (2019): 241019-031

Pages: 12
RNA: 03-2010-032610115700-14

ECORFAN-México, S.C.
143 – 50 Itzopan Street
La Florida, Ecatepec Municipality
Mexico State, 55120 Zipcode
Phone: +52 1 55 6159 2296
Skype: ecorfan-mexico.s.c.
E-mail: contacto@ecorfan.org
Facebook: ECORFAN-México S. C.
Twitter: @EcorfanC

www.ecorfan.org

Holdings
Mexico Colombia Guatemala
Bolivia Cameroon Democratic
Spain El Salvador Republic
Ecuador Taiwan of Congo
Peru Paraguay Nicaragua

Introducción

Fundamentos

Desarrollo

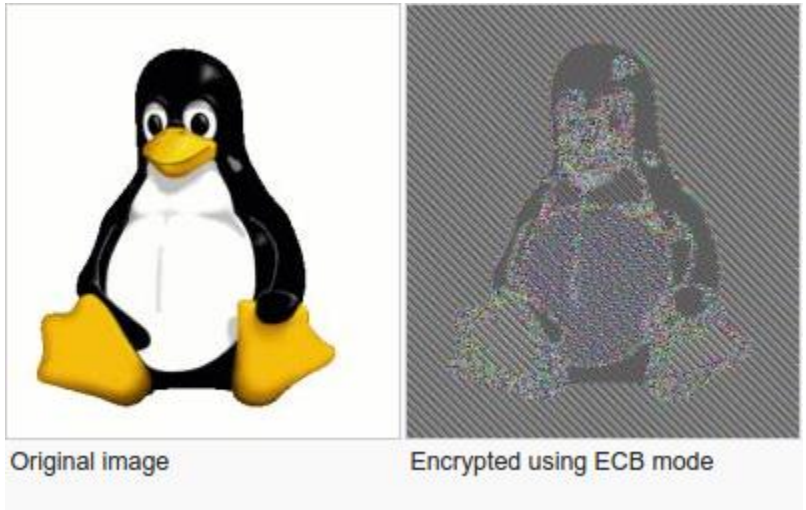
Resultados

Conclusiones

Introducción

Día a día en nuestra vida es más común que podamos realizar más operaciones vía internet, facilitando así los procesos y optimizando los tiempos. Sin embargo, esto conlleva a que los usuarios requieran más seguridad y protección en la transmisión de datos personales, ya que dichos archivos se encuentran expuestos en los enlaces de transmisión.

En la actualidad, el cifrado de imágenes es un área de investigación muy activa debido a las múltiples tareas donde se requiere, por ejemplo: videoconferencias, comunicaciones satelitales, video vigilancia, sistemas de imagen médica, entre otras. A pesar de que ya se cuenta con varios algoritmos de cifrado convencionales, como lo son AES y DES han resultado en muchas ocasiones imprácticos.

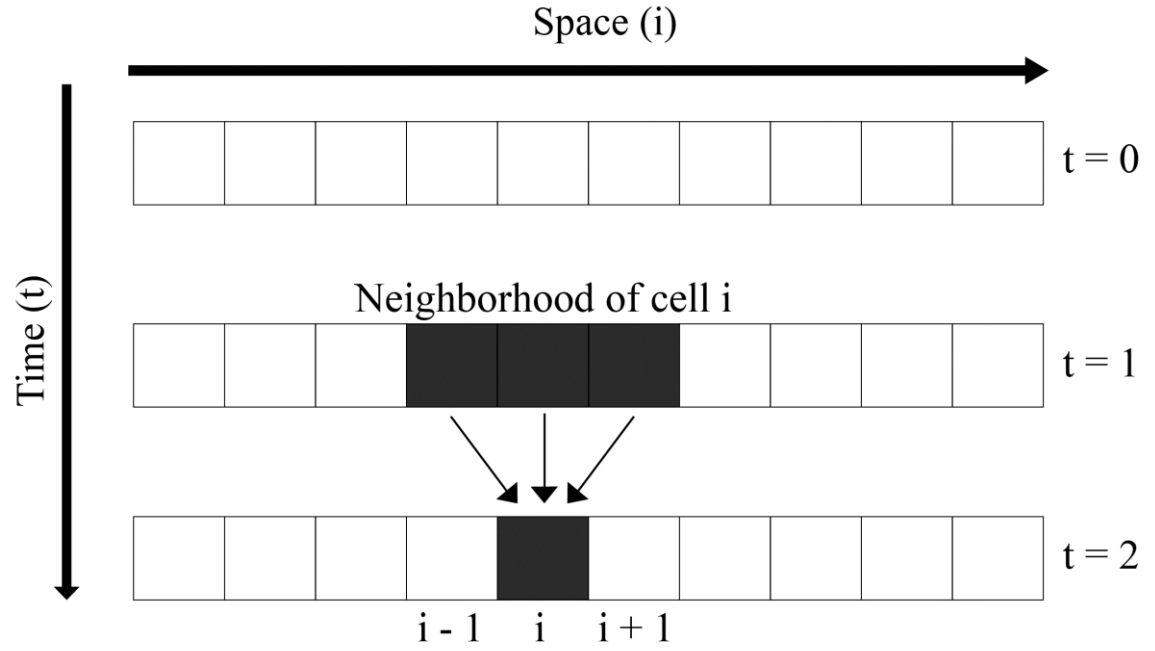


Original image

Encrypted using ECB mode

Autómatas celulares

Los autómatas celulares consisten en un conjunto ordenado de celdas, en forma de rejilla, donde cada celda tiene un número finito de estados. Los autómatas celulares forman una rejilla de dos dimensiones donde sus celdas evolucionan en pasos discretos, acorde a una regla local.

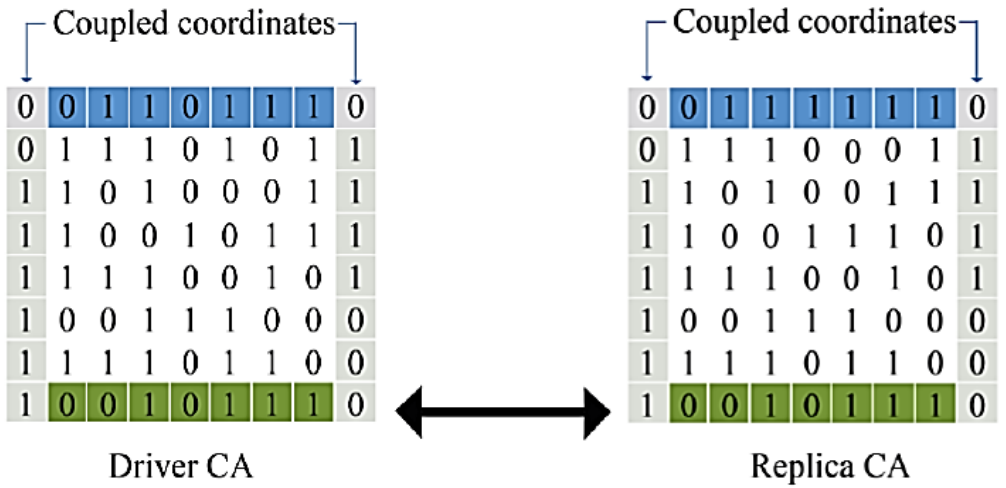


Regla 90 y fenómeno de sincronización

La regla local 90 es descrita por la expresión de la ec.:

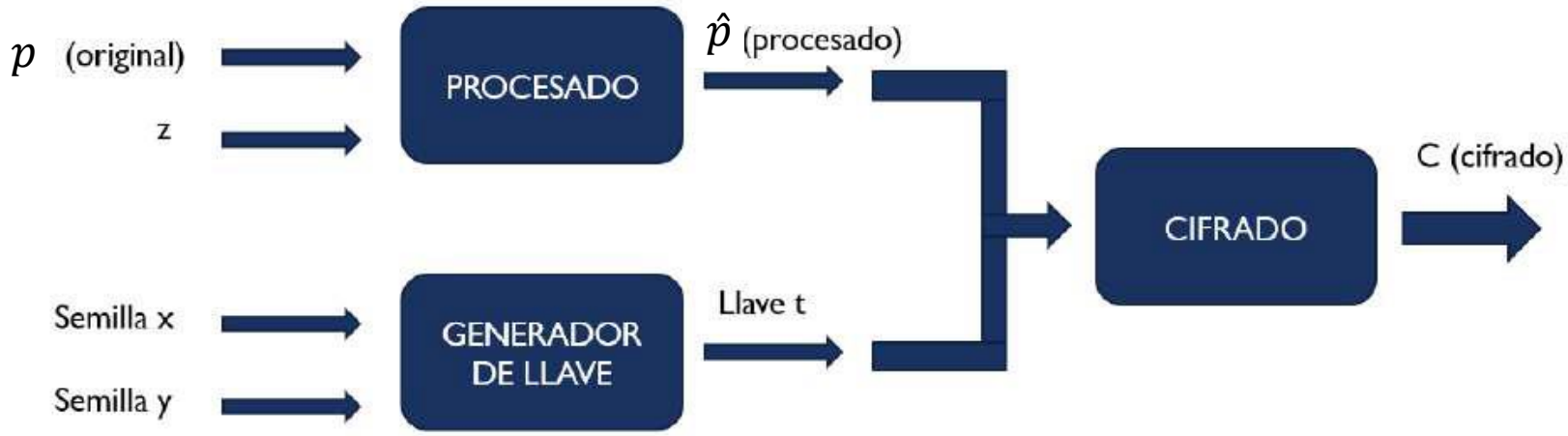
$$X_i{}^{t+1} = (X^t{}_{i-1} + X^t{}_{i+1}) \bmod 2$$

El acoplamiento de autómatas celulares se produce cuando un conjunto dado de coordenadas (coordenadas acopladas) se copian de uno de los sistemas que es el autómata celular conocido como controlador, en el sistema que será denominado réplica.



Sistema ESAC

El sistema de Encriptación por Sincronización con Autómatas Celulares (ESAC). Es un cifrador simétrico que encripta bloques de $\mathbf{2^k-1}$ bits, utilizando para cada bloque una subllave generada a partir de una llave inicial



Sistema ESAC (Ecuaciones)

Ecuaciones para generar la llave secreta **t**

$$t1 = x1 + y2$$
$$t2 = x2 + y1 + y3$$
$$t3 = x1 + x3 + y4$$
$$t4 = x4 + y1 + y3 + y5$$
$$t5 = x1 + x3 + x5 + y2 + y6$$
$$t6 = x2 + x6 + y1 + y5 + y6$$
$$t7 = x1 + x5 + x7 + y8$$
$$t8 = x8 + y1 + y5 + y7 + y9$$
$$t9 = x1 + x5 + x7 + x9 + y2 + y6 + y10$$
$$t10 = x2 + x6 + x10 + y1 + y3 + y5 + y9 + y11$$
$$t11 = x1 + x3 + x5 + x9 + x11 + y4 + y12$$
$$t12 = x4 + x12 + y1 + y3 + y9 + y11 + y13$$
$$t13 = x1 + x3 + x9 + x11 + x13 + y2 + y10 + y14$$
$$t14 = x2 + x10 + x14 + y1 + y9 + y13 + y15$$
$$t15 = x1 + x9 + x13 + x15 + y16$$

Donde $\boldsymbol{t}$ es la llave secreta, $\boldsymbol{x}$ equivale semilla inicial, y $\boldsymbol{y}$ equivale a semilla inicial

Ecuaciones de procesado

$$\widehat{p1} = \text{p1} \oplus \text{z2}$$
$$\widehat{p2} = \text{p2} \oplus \text{z1} \oplus \text{z3}$$
$$\widehat{p3} = \text{p1} \oplus \text{p3} \oplus \text{z4}$$
$$\widehat{p4} = \text{p4} \oplus \text{z1} \oplus \text{z3} \oplus \text{z5}$$
$$\widehat{p5} = \text{p1} \oplus \text{p3} \oplus \text{p5} \oplus \text{z2} \oplus \text{z6}$$
$$\widehat{p6} = \text{p2} \oplus \text{p6} \oplus \text{z1} \oplus \text{z5} \oplus \text{z7}$$
$$\widehat{p7} = \text{p1} \oplus \text{p5} \oplus \text{p7} \oplus \text{z8}$$
$$\widehat{p8} = \text{p8} \oplus \text{z1} \oplus \text{z5} \oplus \text{z7} \oplus \text{z9}$$

Donde $\boldsymbol{p}$ es el texto en claro, $\widehat{\boldsymbol{p}}$ equivale al texto procesado, y $\boldsymbol{z}$ es un vector de n+1 bits.

Ecuaciones de cifrado

$$c1 = t1 \oplus t9 \oplus t13 \oplus t15 \oplus \widehat{p1}$$
$$c2 = t2 \oplus t10 \oplus t14 \oplus \widehat{p2}$$
$$c3 = t3 \oplus t11 \oplus t15 \oplus \widehat{p1} \oplus \widehat{p3}$$
$$c4 = t4 \oplus t12 \oplus \widehat{p4}$$
$$c5 = t5 \oplus t13 \oplus \widehat{p3} \oplus \widehat{p5}$$
$$c6 = t6 \oplus t14 \oplus \widehat{p2} \oplus \widehat{p6}$$
$$c7 = t7 \oplus t15 \oplus \widehat{p1} \oplus \widehat{p3} \oplus \widehat{p5} \oplus \widehat{p7}$$
$$c8 = t8 \oplus \widehat{p8}$$

Donde $\boldsymbol{t}$ es la llave secreta, $\widehat{\boldsymbol{p}}$ equivale al texto procesado, y $\boldsymbol{c}$ equivale al texto cifrado

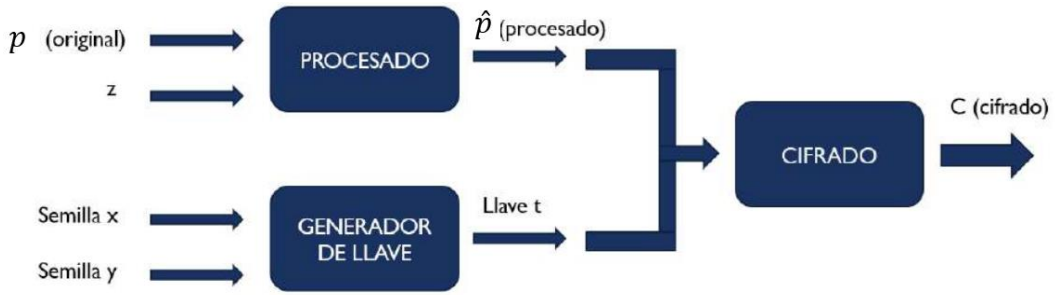
Sistema de cifrado parcial

Para evitar una alta latencia en el sistema de cifrado, una opción es utilizar algoritmos de cifrado parcial. Este tipo de cifrado consiste en que solo una cantidad específica de bits del bloque de texto en claro son cifrados, mientras que el resto se mantienen inalterados

Por lo tanto desarrollamos 8 algoritmos de cifrado parcial

Versión	Bits Cifrados
1	c1 , c2, c3
2	c2 , c3, c4
3	c3 , c4, c5
4	c4 , c5, c6
5	c5 , c6, c7
6	c6 , c7, c8
7	c7 , c8, c1
8	c8 , c1, c2

Algoritmo de cifrado parcial



1.- Primero se selecciona la imagen a cifrar.

2.- Se elige la secuencia de la versión de cifrado tomada de la Tabla 1 de 8 combinaciones.

3.- Se obtiene el pixel como bloque de texto en claro $\boldsymbol{p}$.

4.- Después se realiza el procesamiento $\boldsymbol{p}$ con el vector $\boldsymbol{z}$ para obtener $\widehat{\boldsymbol{p}}$.

5.- Se genera la llave $\boldsymbol{t}$ haciendo uso de las ecuaciones (2).

6.- Se cifran los 3 bits de la imagen de acuerdo a la versión de cifrado en turno.

7.- Se cambia de versión de cifrado y se repite del paso 2 al 6 hasta cifrar toda la imagen.

8.- Se obtiene la imagen cifrada.

Resultados

Análisis de histogramas y cálculo de correlación

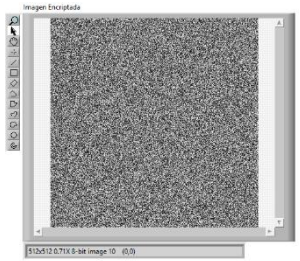
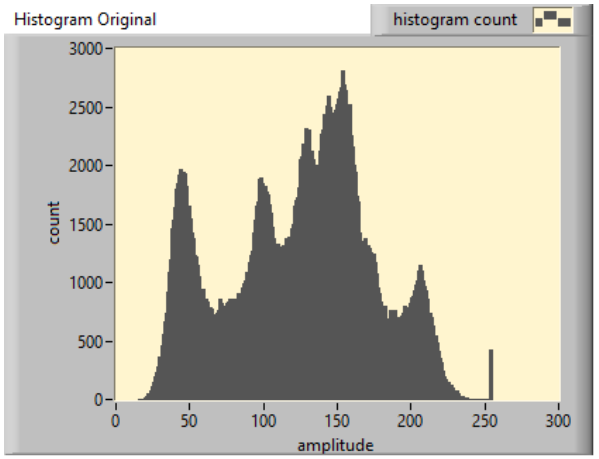
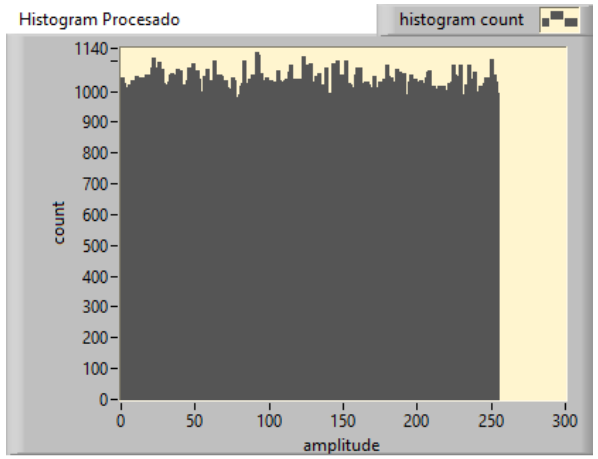


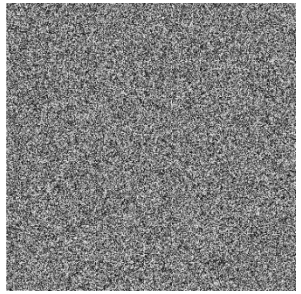
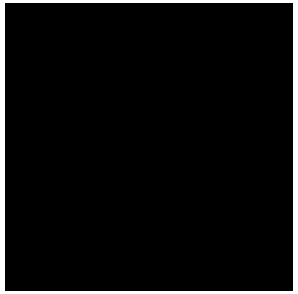
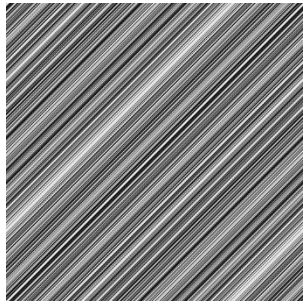
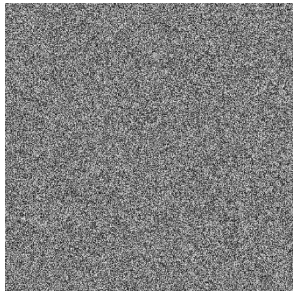
Imagen	Correlación
Lena	0.0001186
Mandril	0.0001540
Pimientos	0.0016889



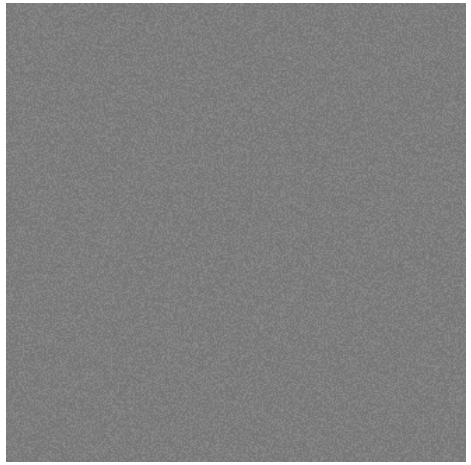


Resultados

Chosen plain-text attack

Replacement attack



Conclusiones

- En el presente trabajo se propuso un sistema de cifrado parcial dinámico para imágenes digitales, que fue capaz de ofrecer seguridad criptográfica y perceptual. Haciendo uso de la sincronización de autómatas celulares y la regla local 90, para cifrar de mejor manera esta información. Se llevaron a cabo diferentes pruebas estadísticas y de criptoanálisis las cuales el algoritmo propuesto pasó de forma exitosa cada una de ellas. Por lo cual este algoritmo puede ser implementado en el cifrado de información importante.

ECORFAN®