ISSN 1870-4069

Algoritmo de cifrado de imágenes utilizando autómatas celulares reversibles

Erendira Corona-Bermúdez, Juan Carlos Chimal-Eguía,
Uriel Corona-Bermúdez

Instituto Politécnico Nacional,
Centro de Investigación en Computación,
México

ecoronab2020@cic.ipn.mx

Resumen. Durante años se han desarrollado esquemas de cifrado y algoritmos, que han ayudado al ser humano a preservar la información compartida; además, durante la pandemia el uso del internet como medio de comunicación ha incrementado significativamente. Por ese motivo, y otros, la criptografía juega un rol importante en la actualidad. En este artículo se propone un esquema de cifrado y descifrado de imágenes, el cual se desarrolla con autómatas celulares reversibles como salida se obtienen imágenes, tales que, visualmente no revelan información acerca de la imagen original. Todo el proceso se realiza durante un tiempo de ejecución de segundos.

Palabras clave: Autómatas celulares reversibles (AC), cifrado de imágenes, criptografía, esquema criptográfico.

Image Encryption Algorithm Using Reversible Cellular Automata

Abstract. For years, encryption schemes and algorithms have been developed to help preserve shared information. Moreover, during the pandemic, the use of the internet as a means of communication increased significantly. For this reason, among others, cryptography plays an important role today. This article proposes an image encryption and decryption scheme developed using reversible cellular automata. As output, the process generates images that, visually, do not reveal any information about the original image. The entire process is executed within a matter of seconds.

Keywords: Reversible cellular automata (RCA), image encryption, cryptography, cryptographic scheme.

1. Introducción

La seguridad de la información es necesaria para los individuos. La mayoría de los datos son compartidos de forma digital, además, son almacenados y

procesados en la nube, por esa razón la criptografía juega un papel importante en la actualidad. Existen métodos y herramientas diferentes para desarrollar criptografía, entre ellos se encuentran los autómatas celulares que son un tipo de sistema dinámico, los cuales se han utilizado de manera eficaz para la construcción de criptosistemas robustos aprovechando sus propiedades [1].

Jun [2] presentó un esquema de cifrado / descifrado de imágenes. Se investigó el comportamiento de varios autómatas celulares elementales, como resultado obtuvieron buenas propiedades de confusión y difusión en su esquema. Del mismo modo en [3] se propuso una nueva estructura para el cifrado de imágenes utilizando Ácido Desoxirribonucleico (ADN) y autómatas celulares recursivos (RCA). El cifrado de imágenes se realizó en dos fases independientes las cuales son permutación y difusión.

Dos años después, [4] propuso un esquema de cifrado de imágenes basado en autómatas celulares unidimensionales reversibles, el cuál fue completamente paralelizable ya que las tareas de cifrado / descifrado se ejecutaban utilizando múltiples procesos independientes para la misma imagen única.

Ping, P. et al., [5] en 2016 presentaron un cifrador de imágenes basado en el caos y los autómatas celulares (AC) similares a las reglas de *life*. El cifrado de imagen propuesto está integrado de dos subprocesos: permutación y sustitución. Similarmente Abdo, A. et al., [6] propusieron un algoritmo con AC elementales, periódicos, y con atractores unitarios; el número de estados atractores de autómatas celulares cambiaba con respecto a la imagen cifrada, y se ocuparon diferentes claves para cifrar diferentes imágenes simples.

Debido a que la transmisión de datos de sensores a través del canal de comunicación inalámbrica juega un papel importante, Satyabrata et. al. [7] presentaron una técnica de criptografía de clave simétrica de cifrado de bloques utilizando reglas de autómatas celulares aplicadas a datos de sensores en WSN. De forma semejante los mismos autores [8], mostraron una nueva técnica de cifrado de imágenes segura y eficiente, usando un autómata celular de dos dimensiones usando la vecindad de Moore, una ventaja de tal técnica es que no tiene pérdidas y es fácil de implementar en hardware.

Finalmente, en [9] se introdujo un esquema de cifrado de imágenes de alta seguridad para la comunicación y el almacenamiento de estas. La imagen permutada se cifra en función de un único número aleatorio generado por un *tent map* sesgado.

2. Metodología

En esta sección se describen conceptos que nos ayudarán en el desarrollo del esquema criptográfico, además, se describirá el modelo propuesto.

2.1. Preliminares

Autómatas Celulares Los autómatas celulares (AC) son una clase de sistemas matemáticos espacialmente y temporalmente discretos caracterizados

por la interacción local y una forma de evolución paralela [10].

Los modelos de AC utilizados usualmente poseen 5 características:

- **Teselado discreto de células:** El sistema consiste en un teselado de células de una, dos, o hasta d-dimensiones.
- **Homogeneidad:**Todas las células son equivalentes.
- **Estados discretos:** Cada célula toma uno de un número finitos de posibles estados discretos.
- **Interacción Local:** Cada célula interactúa solo con células que están en su vecindario local.
- **Dinámica discreta:** A cada unidad discreta de tiempo, cada célula actualiza su estado presente de acuerdo a una regla de transición, tomando en cuenta los estados de las células en su vecindario.

Autómatas celulares reversibles Para describir los autómatas celulares reversibles (ACR) también llamados automatas celulares invertibles, primero se introduce el concepto de reversibilidad y la relación con estos.

Un AC es inyectivo si cada configuración tiene como máximo un elemento del dominio, y es sobreyectiva si cada configuración tiene al menos un elemento del dominio, si el mapa es tanto inyectivo como sobreyectivo, es biyectivo (un mapa biyectivo tiene una función inversa). Llamamos reversible a un AC biyectivo si también la función inversa es un autómata celular [11,12].

Cifradores

Los cifradores simétricos se pueden dividir en dos: cifradores de flujo y cifradores de bloque [13].

Cifradores de flujo: Cifran bits individualmente. Esto se logra agregando un bit de una secuencia de claves a un bit de texto plano.

Cifradores de bloque: Cifra un bloque completo de bits de texto plano a la vez con la misma clave. Esto significa que el cifrado de cualquier bit de texto plano en un bloque determinado depende de cada otro bit de texto plano en el mismo bloque.

Confusión y difusión Existen operaciones primitivas que se pueden aplicar para lograr un cifrado seguro según Claude Shannon [13]. Son dos operaciones primitivas con las que se pueden construir algoritmos de cifrado fuertes:

1. **Confusión:** Es una operación de cifrado donde la relación entre la clave y el texto cifrado se oscurece.
2. **Difusión:** Es una operación de cifrado donde la influencia de un símbolo de texto sin formato se extiende sobre muchos símbolos de texto cifrado con el objetivo de ocultar las propiedades estadísticas del texto sin formato.

Regla 232

0	0	0	0	0	0	0	0	Valor del bit en bloque de imagen
0	0	0	0	1	1	1	1	Valor del bit en bloque de llave (i-1)
0	0	1	1	0	0	1	1	Valor del bit en bloque de llave (i)
0	1	0	1	0	1	0	1	Valor del bit en bloque de llave (i+1)
1	1	1	0	1	0	0	0	Valor del bit en bloque de salida

Regla 23

1	1	1	1	1	1	1	1	Valor del bit en bloque de imagen
0	0	0	0	1	1	1	1	Valor del bit en bloque de llave (i-1)
0	0	1	1	0	0	1	1	Valor del bit en bloque de llave (i)
0	1	0	1	0	1	0	1	Valor del bit en bloque de llave (i+1)
0	0	0	1	0	1	1	1	Valor del bit en bloque de salida

Fig. 1. Reglas de los AC y modo en que evolucionan.

2.2. Motivación y objetivos

Con el tiempo, se han creado algunos protocolos, esquemas y mecanismos criptográficos para preservar nuestra información; pero a medida que avanza la criptografía, también lo hace el criptoanálisis. Dado que el uso del internet y la comunicación por el ha incrementado, es fundamental cuidar nuestros datos, con los diferentes servicios criptográficos. Este trabajo tiene como objetivo diseñar un esquema de cifrado de imágenes,como entrada se tendrá una imagen y como salida se busca obtener otra imagen que no muestre información visual relacionada con la imagen original todo este proceso usando autómatas celulares reversibles.

2.3. Modelo de cirado-descifrado usando autómatas celulares reversibles

Se propone un modelo de cifrado - descifrado de imágenes utilizando dos AC uno-dimensionales. Para las reglas de evolución, en el primer AC, se toma en cuenta el valor de los vecinos en radio uno de la llave; para el segundo se toma en cuenta el valor que tiene, en la misma posición que la célula que se está evolucionando, la imagen. A partir de ambos datos se toma una decisión del nuevo valor que tendrá el bit de la imagen cifrada. Lo anterior es explicado y colocado como una tabla de verdad en la Figura 1.

La salida que se obtiene del modelo es otra imagen, tal que, no tiene relación visual con la imagen de entrada , o su relación sea mínima. El flujo del modelo es presentado en un diagrama de bloques en la Figura 2.

Los AC unidimensionales ocupados en este algoritmo están definidos como una 4-tupla (S,N,f,d), donde:
$S : \{0, 1\}$

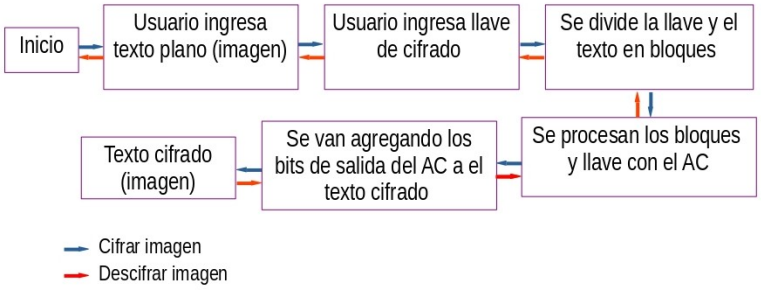


Fig. 2. Diagrama de bloque para explicar el flujo del modelo.

N: Es considerado radio 1.
f: $S^n \rightarrow S$: Regla 232 y 23.
$d \in Z^+$: Uno dimensional.

Dentro de las 256 reglas de Wolfram para los autómatas celulares unidimensionales, solo existen seis que son reversibles; se eligen las reglas 232 y 23 de estas porque tienen la propiedad de ser AC reversibles, además la probabilidad de ser la salida 0 o 1 es la misma. Otra propiedad que tiene es que la función que cifra el archivo es la misma que lo descifra. En el algoritmo 1 se muestra el flujo que se ocupó para desarrollar el modelo.

Algorithm 1 Algoritmo del modelo propuesto para cifrar/descifrar imágenes

InputEntrada OutputSalida
Imagen en claro D, llave K Imagen cifrada E
Inicialización El usuario ingresa la imagen a cifrar D y la llave K Se realiza una transformación a la llave para obtener tamaño de bloque fijo k Se parte la imagen en j bloques de tamaño k existan bloques de la imagen valor del bloque j_i de la imagen en la posición [i] = 0 Se toma la regla 232 de Wolfram para realizar cifrado Se ve el valor de los bits de la llave en la posición $i-1,\ i,\ i+1$ Se regresa el valor del bit de salida, ya sea 0 o 1
Se toma la regla 23 de Wolfram para realizar cifrado Se ve el valor de los bits de la llave en la posición $i-1,\ i,\ i+1$ Se regresa el valor del bit de salida, ya sea 0 o 1
Se agrega a la nueva imagen cifrada E el valor de bit regresado. Se guarda la imagen E.

3. Resultados

El modelo propuesto fue simulado en el lenguaje de programación *Python*, con un procesador intel core i5 y 4 GB de RAM. El procesamiento se hizo a nivel de bits, esto es, se realizaron corrimientos y operaciones lógicas para este proceso, esto hizo que la ejecución del algoritmo fuera rápida. Además, se

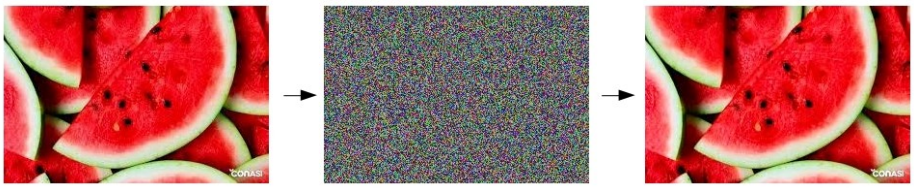


Fig. 3. Figura de sandías en plano, imagen cifrada con el algoritmo porpuesto y salida obtenida.

Fig. 4. Figura de frutas en plano, e imagen cifrada con el algoritmo porpuesto y salida obtenida.

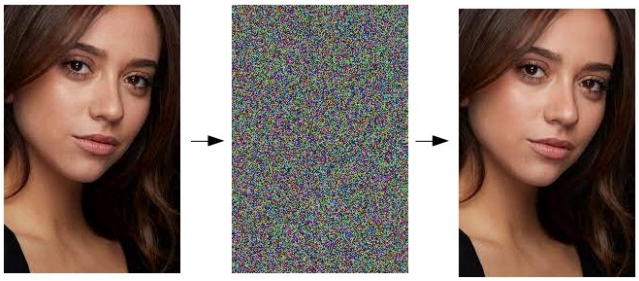


Fig. 5. Figura de rostro en plano, e imagen cifrada con el algoritmo porpuesto y salida obtenida.

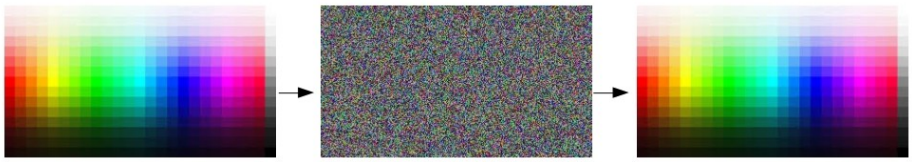


Fig. 6. Figura de gama de colores en plano, e imagen cifrada con el algoritmo porpuesto y salida obtenida.

obtuvieron como salida imágenes, las cuales no tenían relación visual con las imágenes de entrada.

Tabla 1. Valores de la imagen en claro, y de la imagen cifrada obtenida con el modelo propuesto

Figura	Entropía texto cifrado	Entropía texto plano
Sandías	7.6552590369485	7.4757733701720
Frutas	7.6626427475365	7.3809175636137
Rostro	7.6595972685455	7.4639996896011
Gama de colores	7.65532224872648	7.3518466899058

En las Figuras 3, 4, 5 y 6 se observa la imagen original a cifrar, la cual llamamos texto plano o imagen en plano; seguida a esta, se muestra lo que es llamado imagen cifrada, que es la que se obtiene al procesar la imagen con una llave k. Finalmente, se muestra la imagen que obtenemos al hacer el proceso inverso a la imagen cifrada; se regresa a la imagen original teniendo la misma llave k, esto es, de no poner la llave correcta no se obtendría la misma imagen.

3.1. Entropía

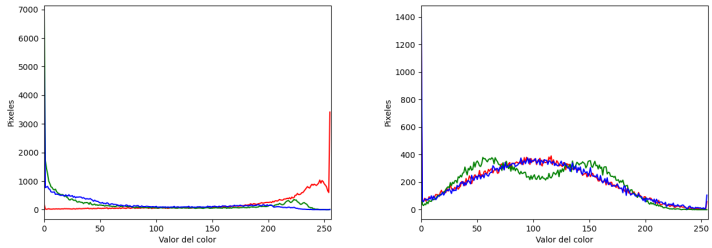
La entropía de la información es una medida estadística de aleatoriedad, por lo tanto, se puede utilizar para caracterizar la textura de una imagen de entrada. Si la entropía de la imagen cifrada es menor que la entropía de la imagen en plano, entonces la imagen puede predecirse y amenaza su seguridad [14]. En la tabla 1 se muestran los valores obtenidos de la entropía de las imágenes 3, 4, 5 y 6.

La entropía $H(m)$ de un mensaje m, con $p(m_i)$ representa la probabilidad del símbolo m_i y N es el número total de píxeles en la imagen y la entropía se expresa en bits se puede calcular como:

$$H(m) = \sum_{i=1}^{N-1} p(m_i) log_2 \frac{1}{p(m_i)} \; bits. \tag{1}$$

3.2. Histogramas

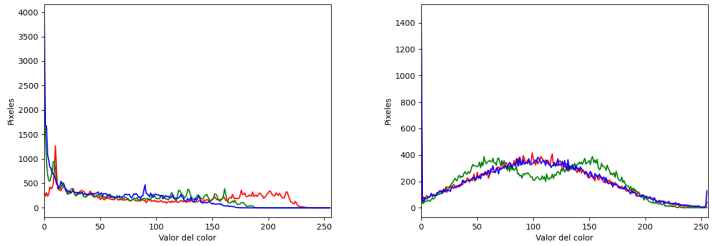
En las Figuras 7, 8 y 9 se muestran los histogramas de las figuras presentadas previamente. Con los histogramas se muestra que, a pesar de la distribución que tenga la imagen original, todas las imagen cifradas tienden a poseer distribuciones similares. Eso es, debido a las operaciones que se realizan en el cifrador, además de que la llave que se ocupó fue la misma para todas las imágenes; los histogramas no muestran patrones existentes.



(a) Histograma de imagen en plano de Sandía.

(b) Histograma de imagen cifrado de Sandía.

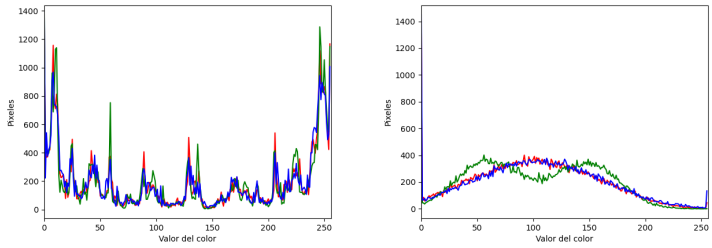
Fig. 7. Histogramas de la imagen 3.



(a) Histograma de imagen en plano de rostro.

(b) Histograma de imagen cifrado de rostro.

Fig. 8. Histogramas de la imagen 5.



(a) Histograma de imagen en plano de gama de colores.

(b) Histograma de imagen cifrado de gama de colores.

Fig. 9. Histogramas de la imagen 6.

4. Conclusión

En este trabajo un novedoso esquema de cifrado de imágenes fue propuesto. Además, cuenta con alta entropía y salida de imágenes sin relación visual, su

tiempo deejecución es de segundos debido a que todas las operaciones fueron realizadas a niveles de bits. En el proceso de cifrado y descifrado no se cuenta con pérdida de información. Por lo descrito anteriormente, se dice que el sistema mantiene la confidencialidad en las imágenes. El algoritmo se puede aplicar para cualquier tipo de imagen representada por una proundidad de 24 bits así como a diferentes formatos de imagen (.JPEG, .JPG, .BMP, .PNG).

Referencias

1. Hameed, Y., Nada, M.: Enhanced RC5 key schedule using one-dimensional cellular automata for audio file encryption. Iraqi Journal of Science, 60, 388–401 (2019)
2. Jun, J.: An image encryption based on elementary cellular automata. Optics and Lasers in Engineering 20(12), 1836–1843 (2012)
3. Abdorreza, B., Homayun, M., Rasul, E.: A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. Optik, 203 (2020)
4. Faraoun, K.: A parallel block-based encryption schema for digital images using reversible cellular automata. Engineering Science and Technology, an International 17(2), 85–94 (2014)
5. Ping, P., Jinjie, W., Yingchi, M., Feng, X., Jinyang, F.: Design of image cipher using life-like cellular automata and chaotic map. Signal Processing 150, 233–247 (2018)
6. Abdo, A., Shiguo, L., Ismail, A., Amin, M., Diab, H.: A cryptosystem based on elementary cellular automata. Communications in Nonlinear Science and Numerical Simulation, 18(1), 136–147 (2013)
7. Satyabrata, R., Jyotirmoy K., Rawat, U., Dayama, P., Nilanjan, D.: Symmetric Key Encryption Technique: A Cellular Automata based Approach in Wireless Sensor Networks. Procedia Computer Science 78, 408–414 (2016)
8. Satyabrata, R., Manu, S., Umashankar, R., Chirag, V., Sanjeet, K.: IESCA: An efficient image encryption scheme using 2-D cellular automata. Journal of Information Security and Applications 61, 2126–2214 (2021)
9. Bhaskar, M., Shrey, S., Prabhakar, K.: A secure image encryption scheme based on cellular automata and chaotic skew tent map. Journal of Information Security and Applications, 45, 117–130 (2019)
10. Ilachinski, A.: Cellular automata a discrete universe. 2nd edn. World Scientific (2001)
11. Hedlund, G.: Endomorphisms and automorphisms of the shift dynamical systems. Mathematical Systems Theory 3(4), 320–375 (1969)
12. Kari, J.: Reversible Cellular Automata: From Fundamental Classical Results to Recent Developments. New Generation Computing 36, (2018)
13. Christof, P., Jan, P.: Understanding cryptography. Springer, New York (2009)
14. Kaur, T., Sharma, R.: Image cryptography by TJ-SCA: Supplementary cryptographic algorithm for color images. International Journal of Scientific & Engineering Research (IJSER), 4(7) (2013)