

Por: David Gomez 20359596

Analizis avanzado de algoritmos

Automatas celulares

tecnica de encriptado de imágenes usando automatas celulates reversibles

ASIGNACIÓN NÚMERO TRES

El problema

se propone el desarrollo de una dinámica reversible de autómatas celulares bidimensionales no uniformes como método de encriptamiento robusto de imágenes digitales a color.

Debido a la amplia difusión de las cámaras digitales y a su incorporación a los dispositivos móviles, las imágenes digitales constituyen un tipo de data de transito común en la Internet. Dicha data debiera transmitirse de forma confiable, asegurando que la información transmitida sea accesible sólo por las partes autorizadas. Para satisfacer el requerimiento de confidencialidad se han propuesto diversos tipos de mecanismos entre los cuales el más importante, con diferencia, es el cifrado o encriptamiento de la información.

En el proceso de encriptamiento el mensaje original es convertido en un mensaje aparentemente aleatorio y sin sentido denominado. El proceso de encriptamiento consta de un algoritmo y una clave. La clave es un valor independiente del mensaje. Para un mismo mensaje original el algoritmo producirá salidas diferentes dependiendo de la clave específica que se haya utilizado. Al cambiar la clave cambia la salida del algoritmo.

Una vez que el mensaje ha sido producido, este puede ser transmitido. Luego de la recepción, el texto cifrado puede ser transformado en el texto plano original usando un algoritmo de desencriptamiento y la misma clave que fue usada para el encriptamiento.

En 1986, Steven Wolfran propuso un esquema de encriptamiento simétrico basado en el uso de Autómatas Celulares. Un autómata celular (A.C.) es un [modelo matemático](https://es.wikipedia.org/wiki/Modelo_matem%C3%A1tico) para un [sistema dinámico](https://es.wikipedia.org/wiki/Sistema_din%C3%A1mico) que evoluciona en pasos [discretos](https://es.wikipedia.org/wiki/Discreto). Es adecuado para modelar sistemas naturales que puedan ser descritos como una colección masiva de objetos simples que [interactúen](https://es.wikipedia.org/wiki/Interacciones_fundamentales) localmente unos con otros.

La secuencia de estados por las que atraviesa el sistema a lo largo del tiempo es denominada trayectoria. Se denomina dinámica a las características de las posibles trayectorias del sistema. Toda dinámica se manifiesta siguiendo un conjunto de reglas. Este conjunto de reglas constituye una descripción o caracterización de la dinámica.

Aquellas dinámicas que permiten el recorrido en sentido contrario de todas sus trayectorias, desde el estado final hasta el estado inicial, se denominan dinámicas reversibles.

Un Autómata Celular de tamaño *m* es un sistema dinámico con *m* localidades o *celdas*, junto a un conjunto de funciones, tal que en cada instante de tiempo discreto el próximo estado de las localidades viene dado por el estado actual y la aplicación de la función o funciones de transición. Aprovechando esta propiedad de los autómatas celulares podemos generar cambios controlados en el sistema aplicando una función de transición que dependa de la clave siniestrada, y utilizar una dinámica reversible para dar efecto a los procesos complementarios de encriptación de encriptamiento y desencriptamiento.

Descripción de la solución propuesta

Desarrollar e implementar en lenguaje java una dinámica reversible de autómatas celulares bidimensionales no uniformes como método de encriptamiento simétrico robusto de imágenes digitales a color.

El primer concepto a tratar es el de vecindades. Se dice que una célula o celda tiene alrededor un conjunto definido de células vecinas en cada espacio de tiempo discreto. Para el problema planteado la adopción de la vecindad de Margolus facilita la definición de funciones de transición reversibles que actúan sobre espacios celulares bidimensionales. Con este tipo de vecindad el espacio celular bidimensional se divide en bloques. En el esquema propuesto cada bloque *B* está formado por cuatro celdas *b00, b01, b10* y *b11* que están dispuestas de forma tal que en la iteración *i* conforman una matriz *Bi* de 2x2 celdas.

El siguiente concepto es el de función biyectiva. Definimos que una función es biyectiva si para cada elemento del conjunto de llegada existe un elemento único en el conjunto de partida y ambos conjuntos tienen el mismo número de elementos. Aplicando esto a las vecindades de Margolus obtenemos que la reversibilidad está garantizada ya que al aplicar la función sobre el bloque resultante obtendremos el bloque original.

En este trabajo se propone un mecanismo que modifica la vecindad de Margulos, al introducir en esta dinámica de autómata celular bidimensional, el parámetro *distancia intercelular: DI*. Durante la ejecución, este parámetro va disminuyendo o aumentando, tomando valores enteros positivos, y particiona el espacio celular C creando un conjunto de células activas CA y un conjunto de células inactivas CI. Durante la aplicación de una regla sólo las células activas conforman vecindades de Margolus (bloques) y son transformadas. Las células inactivas permanecen inalteradas.

Esto implica además que el número de células tanto activas como inactivas que puede contener un bloque está en función de la distancia intercelular. Ya que si bien un bloque solo puede contener cuatro células activas, el número de células inactivas entre cada una de las 4 células activas está determinado por *DI.*

La distribución de los bloques puede generarse o bien usando una rejilla par o una impar. En la rejilla par se comienza a hacer efectiva la división del espacio celular en bloques en el punto (0,0). En la rejilla impar, dicho punto es (1,1).

La aplicación conjugada de desplazar y agrandar los bloques asegura que todas las células en el espacio celular serán desplazadas sin importar las dimensiones del espacio celular y contribuye a elevar el grado de desorden en la imagen encriptada.

Otro punto importante a describir es el efecto de la reglas sobre los bloques. De manera general, se tiene que la clave suministrada al autómata celular determina la forma en que la función de transición F ha de aplicarse sobre el espacio celular y sus respectivos bloques. Definimos una función de transición F como un conjunto de reglas, y definimos a las reglas como un valor decimal cuya representación binaria nos indica la manera en que serán reordenadas las células en un bloque.

Para ilustrar el efecto de las reglas, tomemos por ejemplo la regla definida por el número 27.

La regla 27 corresponde a la función biyectiva de {00,01,10,11} en {00,01,10,11} definida por:

f(00) = 11

f(01) = 10

f(10) = 01

f(11) = 00

Para este trabajo, los pares 57 y 27 son utilizados como reglas principales por su capacidad para generar desorden en el espacio celular. Y los pares 180, 225 y 108, 198 se aplican como complemento.

Al aplicar la dinámica de encriptamiento sobre un espacio celular de dimensión nxm, un cicloe(x) consiste en la aplicación de la secuencia de reglas 180, 225, 57, 27, 108 y 198 para cada uno los valores de (distancia intercelular) DI:0,1,2,…,maxDI; con maxDI = ( max(n,m) – 4 ) / 3. El cicloe tiene un parámetro x que toma valores en el conjunto {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}, que indica cuantas veces debe aplicarse la combinación de reglas 57,27 y que viene determinado por el valor del digito en posición actual en la clave. Las combinaciones de regla 180, 225 y 108,198 se aplican sólo una vez cada una.

El [Pseudocódigo](https://es.wikipedia.org/wiki/Pseudoc%C3%B3digo) del cicloe sería como sigue:

**Inicio**

**por\_cada** X **en** Clave

cicloe(X)

**para\_cada** Di **desde** 0 **hasta** (max(n,m)-4)/3

Dividir C en rejilla par usando Di

Aplicar regla 180

Dividir C en rejilla impar usando Di

Aplicar regla 225

**para\_cada** xi **desde** 0 **hasta** X-1

Dividir C en rejilla par usando Di

Aplicar regla 57

Dividir C en rejilla impar usando Di

Aplicar regla 27

Dividir C en rejilla par usando Di

Aplicar regla 108

Dividir C en rejilla impar usando Di

Aplicar regla 198

**Fin**

Donde X es el valor del digito en la clave hexadecimal suministrada, n y se me refieren al número de células verticales y horizontales presentes respectivamente en el espacio celular y C es dicho espacio.

El ciclo de desencriptado viene dado por la aplicación revertida del cicloe, sin ninguna modificación salvo que la regla 57 requiere una consideración particular. Por no ser esta directamente reversible, requiere que para obtener el valor original sea aplicada 3 veces luego de la primera aplicación. La regla 147, resulta como la regla inversa, que devuelve el orden original tras ser aplicada sobre el resultado de una única aplicación de la regla 57.

Ilústrese así que:

**Inicio**

**por\_cada** X **en** Clave-1

ciclod(X)

**para\_cada** Di **desde** (max(n,m)-4)/3 **hasta** 0

Dividir C en rejilla impar usando Di

Aplicar regla 198

Dividir C en rejilla par usando Di

Aplicar regla 108

**para\_cada** xi **desde** 0 **hasta** X-1

Dividir C en rejilla impar usando Di

Aplicar regla 27

Dividir C en rejilla par usando Di

Aplicar regla 147

/\*

Nótese que:

Aplicar regla 147

Es análogo a:

Aplicar regla 57

Aplicar regla 57

Aplicar regla 57

\*/

Dividir C en rejilla impar usando Di

Aplicar regla 225

Dividir C en rejilla par usando Di

Aplicar regla 180

**Fin**

Experimentos y resultados

En una imagen digital a color un conjunto de píxeles dispuestos según una distribución particular sobre una matriz bidimensional representan una imagen. La correlación entre los píxeles vecinos es uno de los indicadores fundamentales de la información contenida en la imagen. Por lo que un método de encriptamiento robusto aplicado a imágenes digitales debe construir una imagen cifrada en la cual se minimiza la correlación entre los píxeles vecinos, ocultando la información de la imagen original.

La calidad del cifrado puede ser estimada usando diversos indicadores. En este trabajo se utilizan tres indicadores de calidad del cifrado: los histogramas de frecuencia, la entropía y el coeficiente de correlación.

Utilizamos dos claves E4C817A8 y 12345 para contrastar los resultados entre una clave de fuerza promedio contra una muy simple. Trabajamos el análisis sobre la imagen Lena.

Debido a que no se modifica la información contenida en la imagen, solo se desordena, los histogramas de frecuencia y los análisis de entropía serán iguales tanto para la imagen encriptada como para la original y tanto para la clave E4C817A8 como para la clave 12345.

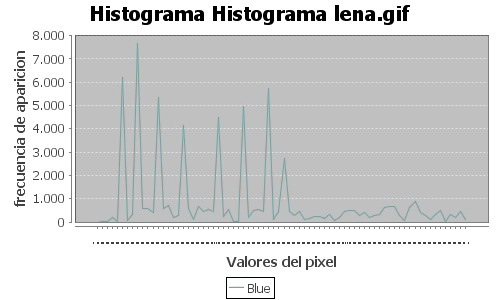
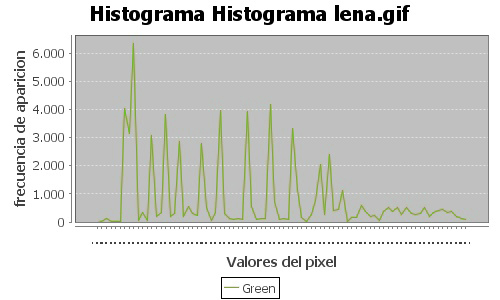
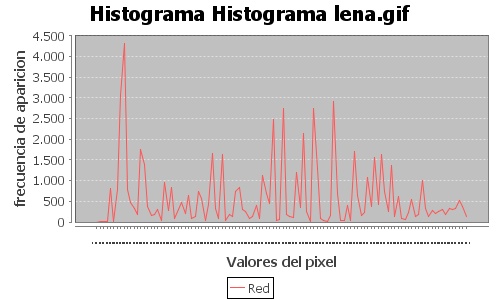
Para la entropía se obtuvieron los siguientes valores:

* Para la componente R=0.0280
* Para la componente G=0.020
* Y para la componente B=0.0195

Que se obtiene de la fórmula:

Donde N es el número de bits que conforman a cada bloque de información y P(si) es la probabilidad de ocurrencia de la configuración si. Dado que en las imágenes estudiadas, se utilizan 8 bits para representar la configuración de un color, dentro de un píxel, el tamaño del bloque de información N es 8.

Los histogramas de frecuencia arrojan la siguiente distribución de color para todos los casos.



Y por último, se calcularon los coeficientes de correlación horizontal, vertical y diagonal para píxeles adyacentes en la horizontal, la vertical y la diagonal respectivamente. Para alcanzar este fin se seleccionaron aleatoriamente 3000 pares de píxeles adyacentes para cada una de las tres direcciones estudiadas. Para el cálculo de los coeficientes de correlación rxy , se emplearon las siguientes ecuaciones, con M=3000 (tamaño de la muestra):



Los resultados mostraron

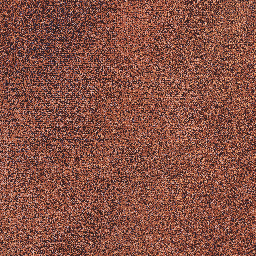
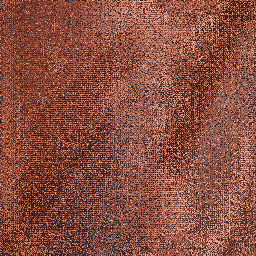
* Para los verticales: 0.00116
* Para los horizontales: -0.01444
* Para los diagonales: 0.04995

Para la codificación con la clave E4C817A8. Y Para la clave 12345:

* Para los verticales: 0.0714
* Para los horizontales: -0.098
* Para los diagonales: 0.043

Vemos que los valores siguen siendo bajos aun con una clave tan vulnerable, pero se observa una relación inversa más pronunciada en las componentes horizontales y que las verticales cambian bastante menos.

 Original E4C817A8 12345



Conclusiones

* La notación utilizada y los mecanismos creados para describir la dinámica, evidencian que la teoría de autómatas celulares ofrece un marco de referencia apropiado para el diseño de algoritmos de encriptamiento.
* La descripción formal del algoritmo de encriptamiento facilita el proceso de codificación en un lenguaje de programación.
* Los resultados obtenidos demuestran que la dinámica propuesta produce un cifrado de alta calidad.
* La incorporación del parámetro Distancia Intercelular propicia un proceso de difusión de naturaleza no lineal que favorece la calidad de la dinámica.