MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Análisis de eficiencia y calidad entre el algoritmo AES CBC y el Mapa de Arnold para el cifrado de imágenes digitales

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por los estudiantes:
Pablo Fernando MORA MEJÍA.
Roger Patricio AYORA CASTELLANOS.

Bajo la dirección de:
César Martín GONZALES ARBAIZA.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Agosto del 2018

Análisis de eficiencia y calidad entre el algoritmo AES CBC y el Mapa de Arnold para el cifrado de imágenes digitales

Efficiency and quality analysis between the AES CBC algorithm and the Arnold map for the encryption of digital images

Pablo Fernando MORA MEJÍA[1]
Roger Patricio AYORA CASTELLANOS[2]
César Martin GONZALES ARBAIZA[3]

Resumen

Este documento presenta un análisis comparativo entre el algoritmo AES CBC y el Mapa de Arnold basado en la teoría del Caos, que servirá como guía para elegir el algoritmo más eficiente al momento de cifrar y descifrar imágenes digitales. Para realizar el análisis comparativo se desarrolló un caso experimental de simulación de dos imágenes digitales con diferentes tamaños de pixeles para posteriormente aplicar en ellas el cifrado y descifrado utilizando los algoritmos AES CBC y Mapa de Arnold en distintos ambientes de ejecución con sistemas operativos basados en Linux. En esta simulación se analizaron dos aspectos fundamentales como el tiempo de procesamiento al momento de cifrar y descifrar una imagen digital aplicando los dos algoritmos y la calidad de cifrado mediante el coeficiente de correlación. Para la ejecución de la simulación se elaboró un programa basado en lenguaje de programación Python, el cual permitió trabajar de forma fácil en la manipulación de imágenes digitales. Este programa también genero datos ilustrativos acerca del análisis comparativo de las características de los algoritmos. Finalmente, luego de analizar y comparar los datos de la simulación se concluyó que el algoritmo AES CBC maneja tiempos óptimos en el proceso de cifrado y descifrado de una imagen digital. Por otro lado, el Mapa de Arnold lleva ventaja al algoritmo AES CBC con respecto a la correlación de píxeles, debido a que el mapa de Arnold no distorsiona los pixeles de una imagen. Esta investigación puede servir de punto de inicio para trabajos futuros relacionados en la calidad cifrado de imágenes digitales en entidades públicas y privadas.

Palabras clave:	AES, Coeficiente de Correlación, Imagen Digital, Mapa de Arnold.

Abstract

This document presents a cross-analysis between the AES CBC algorithm and the chaos theory-based Arnold map, which will serve as a guide for choosing the most efficient algorithm when encrypting and deciphering digital images. To perform the analysis was developed an experimental case of simulation of two digital images with different pixel sizes to later apply in them encryption and decryption using the algorithms AES CBC and Arnold map in Different execution environments with Linux-based operating systems. In this simulation two fundamental aspects were analyzed as the processing time at the time of encrypting and deciphering a digital image applying the two algorithms and the quality of encryption by means of the correlation coefficient. For the execution of the simulation a program based on Python programming language was developed, which allowed to work in an easy way in the manipulation of digital images. This program also generated illustrative data on the analysis of the characteristics of the algorithms. Finally, after analyzing and comparing the simulation data, it was concluded that the AES CBC algorithm manages optimal times in the encryption and decryption process of a digital image. On the other hand, the map of Arnold takes advantage of the algorithm AES CBC with respect to the correlation of pixels, because the map of Arnold does not distort the pixels of an image. This research can serve as a starting point for future work related to the encrypted quality of digital images in public

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail pmorame@uees.edu.ec.
[2] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail rayora@uees.edu.ec.
[3] Ingeniero de Sistemas, Post Grado en Redes y Telecomunicaciones, Master en Administración de Negocios, Examinador de Fraude Certificado - Ecuador. E-mail cgonzales@uees.edu.ec.

and private entities.

Key words		AES, Correlation Coefficient, Digital Image, Arnold Map.

1.- INTRODUCCIÓN

La seguridad informática promueve el uso de protocolos y métodos que buscan evitar el acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizada de los datos. En este contexto se busca garantizar la confidencialidad e integridad de la información implementando un conjunto de controles y estableciendo planes de acción y recomendaciones. (Galeano, Castañeda, & Camilo, 2013; Gutiérrez, Núñez, Aguirre, & Delgado, 2014)

Una imagen digital es una forma de comunicación importante hoy en día, se puede almacenar en discos duros, USB, smartphone y otros dispositivos digitales. Así mismo, son fáciles de copiar, manipular, intercambiar y distribuir a través de canales públicos como internet, por lo que se ha puesto de manifiesto la importancia de proporcionar mecanismos de seguridad que permitan salvaguardar su confidencialidad, integridad y autenticidad. (Hariyanto & Rahim, 2016; López & Villa, 2014; Rojas & Cano, 2011).

La criptografía es un mecanismo utilizado para la protección de información, que garantiza la confidencialidad, autenticidad e integridad de un documento. Dentro de la criptografía existen muchas técnicas basadas en cálculos matemáticos, entre ellos tenemos los algoritmos tradicionales tales como Advanced Encryption Standard [AES], Data Encryption Standard [DES], Rivest, Shamir y Adleman [RSA] que trabajan de forma eficiente en la seguridad de un texto plano, cumpliendo una condición muy importante basado en que un texto descifrado debe ser igual al texto original; para las imágenes ésta condición no se cumple a cabalidad debido a que una imagen está compuesta por pixeles y éstos tienden a distorsionarse en el momento de aplicar un algoritmo tradicional de cifrado. (Espinoza, 2015; López & Villa, 2014; Piper, 2002; Zeghid, Machhout, Khriji, Baganne, & Tourki, 2007)

El algoritmo AES es avalado por el Instituto Nacional de Estándares y Tecnología [NIST] de los Estados Unidos por su rápida capacidad para cifrar y descifrar documentos. Para el tratamiento de imágenes digitales se han implementado mejoras a AES, entre las mejoras se menciona el cifrado por bloques utilizando modos de operación tales como: Electronic Codebook Mode [ECB] , Cipher Block Chaining Mode [CBC], Cipher Feedback Mode [CFB] y Output Feedback Mode [OFB] (Godinez, 2015; Saraf, Jagtap, & Mishra, 2014)

Por otro lado, en las últimas décadas se han realizado estudios que permiten determinar la fuerte relación que existe entre la teoría del caos y la criptografía, a través de la difusión y confusión, por lo tanto; la teoría del caos es una alternativa que permite proteger la confidencialidad, autenticidad e integridad de una imagen digital tomando como partida los sistemas dinámicos y además aprovecha las propiedades de los mapas caóticos para elevar el nivel de robustez en el cifrado. (Boccaletti, Kurths, Osipov, Valladares, & Zhou, 2002; Espinoza, 2015; Parvees, Samath, & Bose, 2016; Pisarchik & Zanin, 2008).

Para determinar si una imagen descifrada es idéntica a la imagen original se debe aplicar una medida que establece la correlación de los pixeles de la imagen original y la descifrada, si la correlación de los pixeles se aproxima a 1 significa que las imágenes son idénticas (Espinoza, 2015; López & Villa, 2014; Piper, 2002; Zeghid et al., 2007)

El mapa de Arnold es un caso particular de la teoría del caos propuesto descubierto por el matemático Ruso Vladimir Arnold quién los descubrió usando una imagen de un gato la cual es una simple ilustración de algunos de los principios del caos, en donde una imagen no necesariamente un gato recibe una transformación que aparentemente aleatoriza la organización inicial de los pixeles de la imagen sin embargo si se itera los suficiente, como arte de magia la imagen original vuelve aparecer. (Guan, Huang, & Guan, 2005; Hariyanto & Rahim, 2016)

Considerando lo expuesto anteriormente se realizó un análisis comparativo entre el Algoritmo de cifrado AES CBC y el Mapa de Arnold para determinar la calidad de cifrado y el tiempo de procesamiento de una imagen digital. La calidad de cifrado se determina por el coeficiente de correlación y el tiempo de procesamiento se mide a través de un temporizador. En este sentido se realizó la simulación de la calidad de cifrado y el tiempo de procesamiento de una imagen digital por medio de una aplicación desarrollada en Python.

2.- MARCO TEÓRICO

Criptografía

La criptografía proviene del griego kryptos que significa oculto, y graphia, que significa escritura, según Diffie & Hellman (1976) es básicamente el estudio de los sistemas matemáticos para resolver 2 tipos de problemas de seguridad como son la privacidad y la autenticación de datos, estrechamente relacionado con las teorías de la comunicación y codificación.

Granados (2006) define a la criptografía como una ciencia encargada de diseñar funciones capaces de transformar mensajes legibles a mensajes cifrados de tal manera que esta transformación y su inversa sólo puede ser factible al conocimiento de una o más llaves.

La criptografía moderna se inició después de tres hechos, el primero fue la publicación de la Teoría de la Información por Shannon, la segunda por la aparición del estándar de cifrado de datos Data Encryption Estándar [DES] en 1974 y finamente con la aparición del estudio realizado por (Diffie & Hellman, 1976) sobre la aplicación de funciones matemáticas a un cifrado de llave pública. En la criptografía moderna existen 2 grandes grupos de algoritmos basados en llaves, los primeros son los simétricos que se identifican por usar una misma llave para cifrar y descifrar datos, el segundo grupo son los algoritmos asimétricos también conocidos como algoritmos de llave pública. Estos algoritmos usan 2 llaves; una para cifrar y la otra llave para descifrar los datos (Diffie & Hellman, 1976; Granados, 2006; Kolmogorov, 1956)

Imagen Digital

Una imagen digital está definida por un arreglo de pixeles, representada de forma bidimensional a partir de una matriz numérica binaria (unos y ceros). Este arreglo de pixeles es llamado bitmap, que corresponde a un mapa de bits de una imagen o fuente, es decir si se tiene una imágen de 512 pixeles de alto x 512 pixeles de ancho significa que los datos de la imagen debe contener 262.144 pixeles (Steinmetz & Nahrstedt, 2002; Younes, 2009)

Según Younes (2009) las imagenes digitales se producen por 2 pasos que son: el muestreo y la cuantificación.

El muestreo es el proceso de dividir la imagen original en pequeñas regiones llamadas píxeles.

La cuantificación es el proceso de asignar un valor entero (color) a cada píxel. El valor entero se le puede asignar a cualquier píxel que básicamente en algunos casos hace referencia como el color de profundidad o bits de resolución, a este concepto también se lo conoce como bits por pixel denotado como bpp que represente el color de cada valor (Ozturk & Sogukpinar, 2004).

Cada valor de color de un mapa de bits de una imagen es un número binario, este número binario en un formato dado será diferente en longitud dependiendo de la profundidad del color del mapa de bits, donde la profundidad del color del mapa determina el rango de color posible, cada píxel de una imagen de 25 bits puede ser de aproximadamente 16,8 millones de colores, esto significa que cada píxel de un mapa de bits tiene 3 valores entre 0 a 255, estos colores se mezclan mediante la combinación de colores primarios (Granados et al., 2007; Guan et al., 2005; Hariyanto & Rahim, 2016).

Estándar de Cifrado Avanzado [AES]

Rijndael es un sistema de cifrado por bloques desarollado por los Belgas Joan Daemen y Vincent Rijmen y adoptado por el gobierno de los Estados Unidos el 2 de Ocutubre del año 2000. Este algoritmo es flexible para soportar cualquier combinación de datos y tamaño de llave de 128, 192 y 256 bits (Daemen & Rijmen, 2013; Rijmen & Daemen, 2001)

Según Zeghid (2007), AES permite una longitud de datos de 128 bits que se pueden dividir en cuatro bloques de operaciones básicas, éstos bloques operan en un arreglo de bytes y organizado como una matriz de tamaño 4 x 4 llamada state.

Para el cifrado completo, los datos se pasan a través de Nr rondas (Nr = 10,12,14,16). Éstas rondas se rigen por las siguientes transformaciones (Daemen & Rijmen, 2013).

SubBytes: En este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda. En la figura 1 se indica este paso de substitución.

ShiftRows: En este paso se realiza una transposición de bytes donde cada fila del state es rotada de manera cíclica un número determinado de veces.

MixColumns: Es equivalente a una multiplicación matricial de columnas del state, combinando los cuatro bytes en cada columna usando una transformación lineal.

AddRoundKey: Es un simple XOR entre el state y la llave round; cada clave round se deriva de la clave de cifrado usando una iteración de la clave.

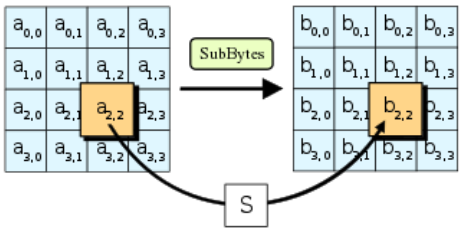


Figura 1. SubBytes (Daemen & Rijmen, 2013)

En la fase de SubBytes, cada byte en el state es reemplazado con su entrada en una tabla de búsqueda fija de 8 bits, S; bij = S(aij).

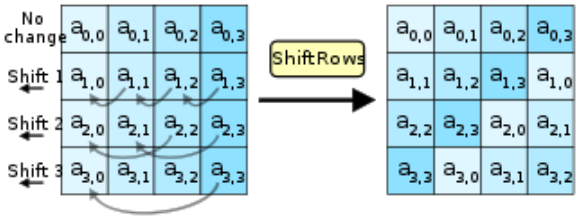


Figura 2. ShiftRows (Daemen & Rijmen, 2013)

En el paso ShiftRows, los bytes en cada fila del state son rotados de manera cíclica hacia la izquierda. El número de lugares que cada byte es rotado difiere para cada fila.

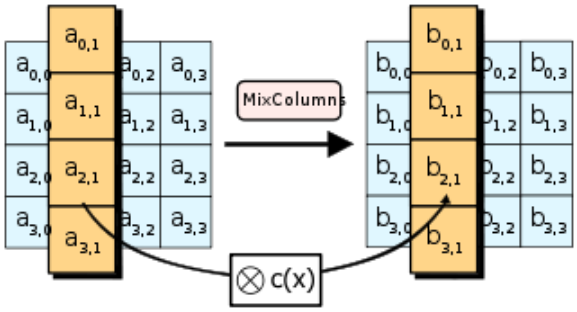


Figura 3. MixColumns (Daemen & Rijmen, 2013)

En el paso MixColumns, cada columna del state es multiplicada por un polinomio constante c(x).

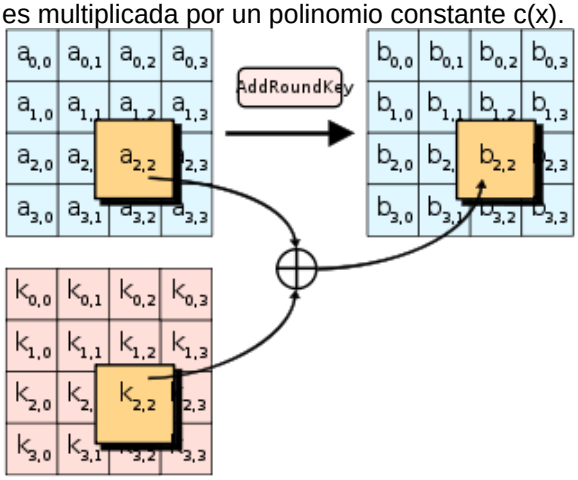


Figura 4. AddRoundKey (Daemen & Rijmen, 2013)

En el paso AddRoundKey, cada byte del state se combina con un byte de la subclave usando la operación XOR.

Modo de Operación de Cifrado de Bloque [CBC] de AES

NIST ha definido 5 modos de operación de AES como son CBC (Cipher Block Chaining), ECB (Electronic CodeBook), CFB (Cipher FeedBack), OFB (Output FeedBack) and CTR (Counter).

El modo CBC es uno de los modos más seguros para el cifrado simétrico. Para su funcionamiento requiere de un vector de inicialización (más adelante indicado como “IV”) cuyo tamaño debe ser igual al tamaño del bloque. El uso de un IV generado aleatoriamente evita la generación de texto cifrado idéntico a partir de paquetes, el cual tienen datos que abarcan el primer bloque del tamaño del algoritmo de cifrado (Ferguson, 2006; Frankel, Glenn, & Kelly, 2003). La llave de

AES CBC puede ser de 128 o 256 bits dependiendo de la versión, el tamaño del bloque siempre es múltiplo de 16 bytes. La fórmula de IV por sector **s** es:

$$IV_s = E(K_{AES}, e(s))$$

Donde **E** es la función de cifrado AES y es la función de codificación que asigna cada número de sector **s** a un valor único de 16 bytes. Cabe recalcar que IV depende de la llave y el número del sector y no de los datos.

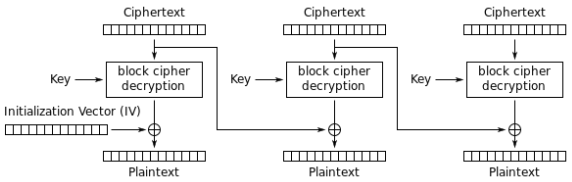


Figura 6: Cipher Block Chaining (CBC) (Ferguson, 2006; Frankel et al., 2003)

Teoría del Caos

Los primeros estudios de la Teoría del Caos datan a finales del siglo XIX con el aporte del físico–matemático Henri Poincaré quién introdujo el concepto de no linealidad, que implica divergencia entre el resultado y el origen y la simple adición de las partes de un hecho no corresponde al producto final por lo que los algoritmos lineales poco pueden aportar para explicar su dinámica. (Velastegui, Arquímides Haro; Albuerne, Yolanda Llosas; Fernández, 2017)

Otro aporte a la Teoría del Caos se dio en el año de 1961 cuando Edward Norton Lorenz del Massachussetts Institute Of Technology planteó un argumento a un modelo climatológico en donde una mínima variación de las condiciones iniciales de un determinado sistema atmosférico puede provocar que el sistema evolucione de formas diferentes, es decir que las condiciones iniciales de un fenómeno atmosférico la más mínima variación como el aire puede aumentar o disminuir su desarrollo esto incluye algo tan insignificante como el aleteo de una mariposa. Lorenz reveló que con tres variables (la temperatura, la presión atmosférica y la velocidad del viento), es posible predecir el clima terráqueo (Munné & others, 1995; Vilchis, Alvarado, & Ortigoza, 2007). Como el clima es un fenómeno de carácter claramente caótico, esta predicción conllevaba algo científicamente inesperable: nada menos que la "*determinabilidad*" del caos. Se trata de una determinación que es formulable matemáticamente y que se puede representar mediante una curiosa y bella figura en forma de alas de mariposa, más exactamente en forma de ochos sucesivos y continuos en espiral, que tienden hacia un atractor, esto es y para entendernos, hacia un foco que "*atrapa*" trayectorias (Munné & others, 1995; Vilchis et al., 2007).

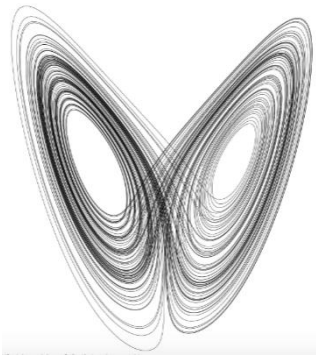


Figura 5. Atractor de Lorenz ((Munné & others, 1995; Vilchis et al., 2007)

Con este hecho se inicia el estudio de la dinámica caótica. Así mismo, Lorenz dedujo en el año de 1963 las propiedades generales del caos como son la dependencia y sensibilidad a las condiciones climáticas iniciales (Munné & others, 1995; Vilchis et al., 2007). Caos significa un estado de desorden es decir que se lo puede definir como un efecto impredecible, pero determinable, por lo tanto surge el concepto de la teoría del caos como una rama de las ciencias exactas que se enfoca en los comportamientos aparentemente aleatorios en los sistemas dinámicos (Rodriguez, Barrera, Parra, & Posada, 2017).

Desde la década de los 90 se han presentado trabajos relacionados con la aplicación de la teoría del caos tales como: Chaos-based image encryption algorithm (Guan, Zhi-Hong and Huang, Fangjun and Guan, Wenjie), Cifrador Caótico de Bloques Usando el Mapeo Logístico (IBARRA OLIVARES, ERIC), Arnold's Cat Map Algorithm in Digital Image Encryption (Hariyanto, Eko and Rahim, Robbi), Integrated confusion-diffusion mechanisms for chaos based image encryption (Koduru, Sai Charan and Chandrasekaran, V), entre otros. Los mapeos caóticos con la principal aportación que hace la Teoría del Caos en la protección de la

información, generan secuencias pseudo aleatorias con propiedades estadísticas por lo que la convierte en uno de los mejores métodos para propósitos criptográficos, esteganográficos y de canales subliminales, donde se requieren de secuencias cifrantes con muy buenas propiedades de impredictibilidad y aleatoriedad, además de ofrecer baja probabilidad de interpretación (Devaney & Eckmann, 1987; Millérioux, Hernandez, & Amigo, 2005).

Confusión y Difusión

Según (Shannon, 1949) hay dos principios generales que guían el diseño de algoritmos prácticos como son la confusión y la difusión, debido a que frustran el análisis estadístico que es muy utilizado para resolver muchos tipos de cifrados. El método de difusión consiste básicamente en el intercambio de posiciones de los pixeles de tal manera que puedan ser mezclados en toda la imagen digital sin alterar los valores de los píxeles, aunque a través de esta etapa la imágen queda irreconocible no es muy seguro dejarlo en este estado es por eso que se debe aplicar otra etapa como es la confusión, es aquí en donde los valores de los pixeles son modificados secuencialmente por medio de una secuencia generada por el sistema caótico (Espinoza, 2015; Koduru & Chandrasekaran, 2008). El proceso de confusión y difusión se repite n veces con la finalidad de lograr un nivel satisfactorio de seguridad; debido a que la confusión y difusión suponen un desorden determinístico, un sistema criptográfico tradicional puede ser considerado como un sistema caótico o sistema pseudorandómico (Espinoza, 2015; Pisarchik & Zanin, 2008).

Mapas Caóticos

Según Guan, Huang, & Guan (2005); Pisarchik & Zanin, (2008) la criptografía basada en la Teoría del Caos ha llamado la atención a muchos investigadores debido a sus propiedades como son la ergodicidad y a su alta sensibilidad a las condiciones y parámetros iniciales la cual es ideal para el diseño de algoritmos de cifrado con buena difusión y confusión. Los mapas caóticos son fáciles de implementar en microprocesadores y computadores por su alta velocidad a bajo costo, siendo así que los hace ideales para cifrar datos multimedia en comparación a los algoritmos de cifrado tradicionales. Los mapa caóticos son utilizados en el cifrado de imágenes digitales como claves de difusión y confusión para modificar los valores de los pixeles y cambiar su posición (Lian, Sun, & Wang, 2005; Pisarchik & Zanin, 2008). Lian et al (2005) considera que un algoritmo de cifrado es ideal si un texto cifrado se distribuye uniforme y aleatoriamente y es independiente al texto sin formato lo que significa que el cifrado no proporciona ayuda a los atacantes. Kolmogorov (1956) explica que la seguridad de un criptosistema depende de su complejidad computacional.

Mapa de Arnold

El Mapa de Arnold es un algoritmo de cifrado de imágenes digitales propuesto por el Matemático Ruso Vladimir Arnold en el año de 1960 quién ilustro este algoritmo mediante el uso de la imagen de un gato. La técnica del algoritmo permite girar la imagen de tal forma que no sea visible mediante un número de iteraciones, las iteraciones van desde 1 hasta el tamaño máximo de una imagen, cuando el número de iteraciones es igual al tamaño de la imagen el resultado es la imagen original debido a que la posición de los pixeles se mueven de forma giratoria conforme a un número de repeticiones. (Guan et al., 2005; Hariyanto & Rahim, 2016; Peterson, 1997). El Mapa de Arnold utiliza dos dimensiones que se puede utilizar para cambiar la posición de un píxel de la imagen sin alterar su información, la imagen de un píxel puede asumirse mediante la siguiente fórmula (Guan et al., 2005; Hariyanto & Rahim, 2016)

$$S = (x, y)|x, y = 0,1,2..N - 1$$

La fórmula del Mapa de Arnold se la expresa de la siguiente manera (Hariyanto & Rahim, 2016):

$$\begin{bmatrix} x \\ y \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \ (m\acute{o}d\ n)$$

$$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = (m\acute{o}d\ n)$$

A continuación, se ilustra la operación del Mapa de Arnold.

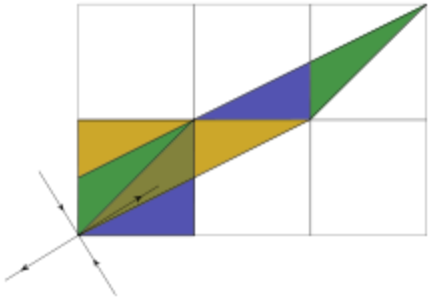


Figura 7: Operación del Mapa de Arnold (Hariyanto & Rahim, 2016)

Coeficiente de Correlación

El coeficiente de correlación determina la relación entre 2 variables, es decir es una medida que permite calcular el grado de similitud entre dos variables. La correlación permite calificar la calidad de cifrado de cualquier criptosistema. Un sistema criptográfico de imagen se dice que es bueno si se oculta todos los atributos de una imagen a texto plano (Ahmad & Ahmed, 2010). Si una imagen y el texto plano son completamente diferentes el coeficiente de relación es muy bajo o cercano a cero. Si el coeficiente de correlación es igual a 1 entonces la imagen y el texto plano son idénticas, por ende se le denomina correlación perfecta. Si el coeficiente de correlación es menor (-1), entonces la correlación es inversa (Bruck, McNeill, Sutton, & Peters, 1989). Matemáticamente el coeficiente de correlación puede escribirse de la siguiente manera:

$$C.C = \frac{Cov(x,\ y)}{\sigma_x x \sigma_y}$$

$$\sigma_{x=}\ \sqrt{VAR(x)}$$

$$\sigma_{y=}\ \sqrt{VAR(y)}$$

Donde x, y son los valores de las escalas de grises de los pixeles en el mismo texto plano y el texto cifrado, CC es el coeficiente de correlación y Cov es la covarianza de pixeles, VAR(x) es la varianza en el pixel x y en la imagen del texto plano, σx es la desviación estándar.

3.- METODOLOGÍA.

El estudio tiene un enfoque cualitativo con un alcance descriptivo a través del cual se permitirá determinar el factor comparativo entre el algoritmo AES CBC y Mapa de Arnold. Se desarrolló una aplicación que permitió comparar el comportamiento de los algoritmos evaluados y se tomaron los datos descriptivos que fueron simulados.

Para el análisis se consideran dos bases fundamentales como: rendimiento en el procesamiento de imágenes digitales y correlación de píxeles. La experimentación se realiza en dos máquinas virtuales con sistema operativo Linux y sus características son las siguientes:

Características	VM 1	VM 2
Procesador	2.7 GHz	2.7 GHz
Memoria	2 GB	6 GB
Disco Duro	20 GB	20 GB

Tabla: 1 Máquinas Virtuales

En estas máquinas virtuales se recolectan los tiempos de procesamiento medidos en segundos y el coeficiente de correlación al momento de cifrar y descifrar una imagen digital.

El programa de cifrado y descifrado corre en cada una de las máquinas virtuales para lo cual se utilizan dos imágenes digitales con las siguientes particularidades: (1080 x 1080) pixeles y peso de 345.2 KB en la imagen original 1; (2160 x 2160) píxeles y peso de 1300 KB en la imagen original 2.

Figura 8. Imagen Original 1

Figura 9. Imagen Original 2

La experimentación se realiza con el lenguaje de programación Python en el cual se desarrolla la programación de los algoritmos de cifrado y descifrado de imágenes digitales, haciendo uso de sus librerías Numpy, Crypto, Hashlib y Time.

.

DESARROLLO DE LA APLICACIÓN Y SIMULACIÓN DEL CIFRADO Y DESCIFRADO

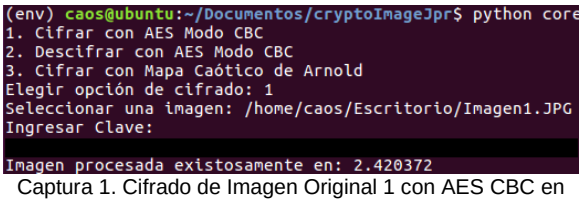
En la tabla 2 y 3 se puede apreciar el comportamiento de los algoritmos al momento de cifrar y descifrar las imágenes originales 1 y 2 en relación a los tiempos de procesamiento en cada una de las máquinas virtuales.

En la tabla 2 con el algoritmo AES CBC se puede evidenciar el tiempo de ejecución por cada imagen digital. En las máquinas virtuales 1 y 2, se señala cantidades decimales, que representan los tiempos de procesamiento de las imágenes en segundos por cada algoritmo. Sin embargo, con el Mapa de Arnold se describen varios tiempos de ejecución relacionados con el número de iteraciones que van desde 1 hasta un número menor o igual al tamaño máximo de la imagen. Las iteraciones permiten dar un movimiento a los píxeles de una imagen, esta es una propiedad del Mapa de Arnold.

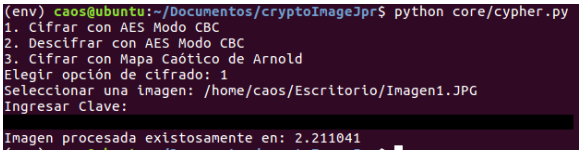
Imag.	VM	AES CBC	Mapa de Arnold			
			Iteraciones			
			100	500	1000	2000
1	1	2.42	2.63	11.49	23.30	X
	2	2.21	2.57	11.10	23.07	X
2	1	5.42	14.22	58.42	112.90	314.70
	2	5.36	11.02	52.96	96.48	288.26

Tabla: 2 Tiempo de Procesamiento de Cifrado

Se evidencia en las siguientes capturas el tiempo de procesamiento al momento de cifrar con AES CBC la imagen original 1, en la máquina Virtual 1 y 2.

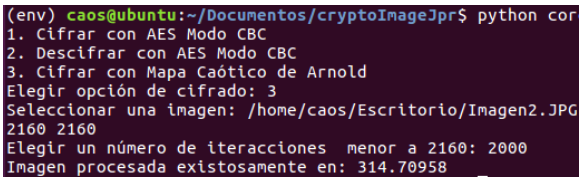


Captura 1. Cifrado de Imagen Original 1 con AES CBC en VM 1

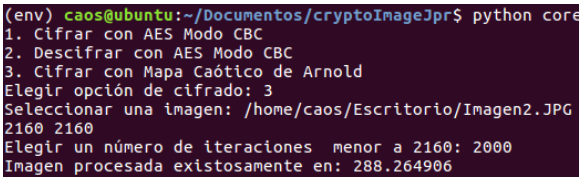


Captura 2. Cifrado de Imagen Original 1 con AES CBC en VM 2

A continuación, en las siguientes capturas se puede evidenciar los tiempos de procesamiento al momento de cifrar con el Mapa de Arnold la Imagen Original 2, en la máquina Virtual 1 y 2 utilizando 2000 iteraciones.



Captura 3. Cifrado de Imagen Original 2 con el Mapa de Arnold en VM 1



Captura 4. Cifrado de Imagen Original 2 con el Mapa de Arnold en VM 2

Cifrado con AES CBC

Seguidamente se ilustra en la figura 10 el cifrado de la imagen original 1 en la máquina virtual 1 aplicando el algoritmo de AES CBC. Como se puede observar los pixeles se encuentran completamente distorsionados. Para cifrar la imagen se lo hace mediante una llave pública, misma que deberá ser utilizada para el proceso de descifrado.

Imagen Original 1

Figura 10. Imagen original 1 cifrada con AES

Cuadro 1. Cifrado imagen original 1

El código en python para cifrar la imagen con AES CBC es el siguiente:

```
def aes_cbc_encrypt(key, data, mode=AES.MODE_CBC):
    IV = os.urandom(IV_SIZE)
    aes = AES.new(key, mode, IV)
    new_data = aes.encrypt(data)
    return new_data
```

Figura 11. Código Cifrado con Aes

En donde **key** es la llave que se utiliza para cifrar la imagen, **data** es un array de pixeles obtenidos de una imagen y **mode** es el modo de AES a implementar.

Cifrado con el Mapa de Arnold

A continuación, en la figura 13 se ilustra el cifrado de la Imagen Original 2 en la máquina virtual 1, aplicando el algoritmo Mapa de Arnold, para lo cual se tomó 2000 iteraciones cuyo número es menor al tamaño máximo de la imagen.

Imagen Original 2

Figura 13. Imagen original 2 Cifrada con Mapa de Arnold usando 2000 Iteraciones

Él código respectivo para el cifrado y descifrado de imágenes con el Mapa de Arnold es el siguiente.

```
def map_arnold(filename, iteractions):
image = Image.open(filename)
im = array(image)
N = image_array.shape[0]
    x, y = meshgrid(range(N), range(N))
    xmap = (2 * x + y) % N
    ymap = (x + y) % N
    for i in range(iteractions):
        im = im[xmap, ymap]
    result = Image.fromarray(im)
```

Figura 14: Código de Cifrado y Descifrado Con Mapa de Arnold

En donde **filename** es la ruta de la imagen, **im** es el array de pixeles de la imagen, **N** representa al tamaño de la imagen e **iteractions** es el número de veces que la imagen va rotando.

Descifrado de imágenes

En la tabla 3, respecto al algoritmo Mapa de Arnold, se aplica las iteraciones faltantes para llegar al tamaño máximo de la imagen, que indica; si él número de iteraciones faltantes aplicadas a la imagen a descifrar, es igual al tamaño de la imagen, el resultado del descifrado debe ser igual a la imagen original.

Imag.	VM	AES CBC	Mapa de Arnold			
			Iteraciones Faltantes			
			980	580	80	
1	1	1.78	51.42	30.81	4.72	X
	2	1.76	43.97	23.89	3.96	X
			Iteraciones Faltantes			
			2060	1660	1160	160
2	1	4.83	535.26	429.88	322.55	43.49
	2	4.81	456.13	391.15	267.41	36.36

Tabla: 3 Tiempo de Procesamiento en el Descifrado

Descifrado con AES CBC

En la figura 15 se ilustra el descifrado de la Imagen Original 1 (figura 10), para lo cual se aplica la llave publica usada en el proceso de cifrado.

Imagen original 1 Cifrada con AES CBC

Figura 15. Imagen original 1 Descifrada con AES

Así mismo, se muestra el código implementado para realizar este proceso, muy similar al del cifrado con AES CBC.

```
def aes_cbc_decrypt(key, data,mode=AES.MODE_CBC):
    IV = os.urandom(IV_SIZE)
    aes = AES.new(key, mode, IV)
    new_data = aes.decrypt(data)
    return new_data
```

Figura 16: Código Descifrado con Aes

Descifrado con Mapa de Arnold

Finalmente en la figura 17, se puede apreciar el resultado al descifrar la Imagen Original 2 (Figura 13) utilizando el Mapa de Arnold, para esto se complementó con el número de iteraciones faltantes (160) para llegar al tamaño máximo de la imagen original. Es decir, si el

tamaño de la imagen original 2 es 2160 pixeles y el número de iteraciones que se tomó para el cifrado fue de 2000 iteraciones, quiere decir que se debe aplicar 160 iteraciones para obtener la imagen descifrada.

Imagen original 2 Cifrada con Mapa de Arnold usando 2000 Iteraciones

Figura 17: Imagen 2 Descifrada con Mapa de Arnold utilizando 160 Iteraciones

Él código respectivo para el cifrado y descifrado de imágenes con el Mapa de Arnold es el siguiente.

```
def map_arnold(filename, iteractions):
image = Image.open(filename)
im = array(image)
N = image_array.shape[0]
    x, y = meshgrid(range(N), range(N))
    xmap = (2 * x + y) % N
    ymap = (x + y) % N
    for i in range(iteractions):
        im = im[xmap, ymap]
    result = Image.fromarray(im)
```

Figura 18: Código de Cifrado y Descifrado Con Mapa de Arnold

En donde **filename** es la ruta de la imagen, **im** es el array de pixeles de la imagen, **N** representa al tamaño de la imagen e **iteractions** es el número de veces que la imagen va rotando.

Coeficiente de Correlación

Podemos observar en la tabla 4 y 5, en la cual hace referencia al resultado del coeficiente de correlación de cada algoritmo. Para determinar si una imagen descifrada es similar a la original, el resultado del coeficiente de correlación debe aproximarse a 1.

Correlación con AES CBC

Con AES se puede evidenciar que, el resultado de la correlación es igual a 0.999994, obteniendo un margen de error de 0,000006.

Im.	Im. Original 1	Im. Descifrada con AES	Coeficiente de Correlación AES
1	 Imagen Original 1	 Figura 14. Imagen original 1 Descifrada con AES	0.999994

Tabla: 4 Coeficiente de Correlación AES CBC

Correlación con Mapa de Arnold

Utilizando el algoritmo caótico Mapa de Arnold, el coeficiente de correlación es igual a 1.000000.

Im.	Im. Original 2	Im. Descifrada con Mapa de Arnold	Coeficiente de Correlación Mapa de Arnold
2	 Imagen Original 2	 Figura 17: Imagen 2 Descifrada con Mapa de Arnold	1.000000

Tabla: 5 Coeficiente de Correlación Mapa de Arnold

En python el código para el cálculo del coeficiente de correlación es el siguiente.

```
pic_original = Image.open(image_original)
pic_decrypt = Image.open(image_decrypt)
pix_original = np.array(pic_original)
pix_decrypt = np.array(pic_decrypt)
correlation = np.corrcoef
(pix_original.reshape(-1)
```

Figura 19: Código de Coeficiente de Correlación

4.- ANÁLISIS DE RESULTADOS

Tiempos de Procesamiento

En la Tabla 2 se muestran los resultados del procesamiento de cifrado de imágenes digitales. Por consiguiente, se demuestra que AES CBC es superior al Mapa de Arnold, En el Mapa de Arnold mientras mayor es el número de iteraciones, los pixeles de la imagen se cambian de posición n número de veces y, el tiempo de procesamiento se incrementa. En el siguiente gráfico se puede observar que utilizando AES CBC para el cifrado de la imagen digital su

complejidad algorítmica de acuerdo a la notación Big-O es constante O(1) debido a que el tiempo de procesamiento es el mismo. En cambio, el Mapa de Arnold depende mucho del número de iteraciones cuya complejidad es O(n) lineal porque su tiempo de procesamiento es proporcional al número de iteraciones.

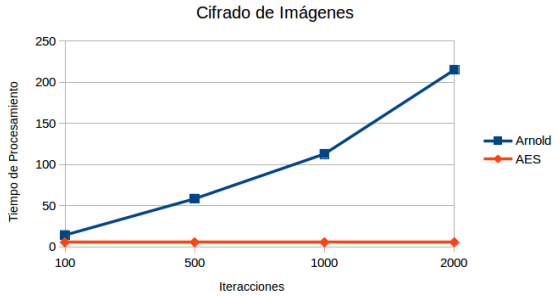


Figura 20: Resultado de comparación de Cifrado de Imágenes

Para el descifrado de una imagen digital de acuerdo a la tabla 3, el valor de procesamiento es más representativo puesto a que en AES CBC muestra los resultados de los tiempos de procesamiento y en el caso del Mapa de Arnold se ilustran el resultado de los tiempos de procesamiento aplicando las iteraciones faltantes. Los resultados obtenidos dan una clara evidencia de que AES CBC procesa una imagen con tiempos más cortos que el Mapa de Arnold.

Coeficiente de correlación

Para el análisis del coeficiente de correlación, en la tabla 5 indica que en el algoritmo Mapa de Arnold los pixeles de la imagen descifrada y la original son similares, debido a que éste algoritmo usa una técnica de difusión, permitiendo que los pixeles solo sean movidos de posición, dicha técnica hace que los pixeles no se distorsionen y sean exactamente iguales a los originales, caso muy distinto sucede con el algoritmo tradicional AES CBC que cifra cada pixel de la imagen provocando una distorsión significativa. En la siguiente imagen se indica la ventaja de la correlación de pixeles del Mapa de Arnold sobre AES CBC.

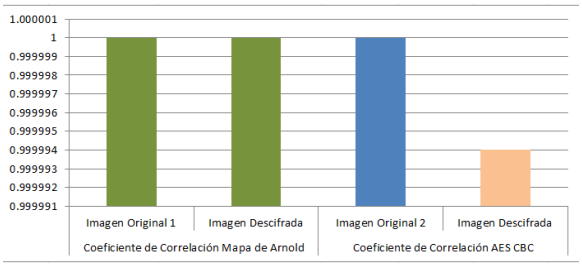


Figura 21: Resultado de comparación de Correlación de Imágenes

En las figuras 22 y 23 respectivamente se puede visualizar los valores de los pixeles de la imagen original y la descifrada de AES CBC y Mapa de Arnold respectivamente.

Pixeles de imagen original 1:
[112 120 99 176 128 80]
Pixeles de Imagen Original 1 descifrada:
[68 22 122 176 128 80]

Figura 22: Coeficiente de Correlación con AES CBC

Pixeles de la Imagen Original 2
[4 11 4 11 22 8]
Pixeles de Imagen Original 2 descifrada:
[4 11 4 11 22 8]

Figura 23: Coeficiente de Correlación con Mapa de Arnold

5.- CONCLUSIONES Y RECOMENDACIONES

El algoritmo AES CBC es más rápido y eficiente comparativamente versus el mapa de Arnold, esto se demostró a través de la simulación de los algoritmos en donde se pudo observar el tiempo de procesamiento de las imágenes digitales esto demuestra que este algoritmo puede ser utilizado con mayor precisión en la vida real por ejemplo en imágenes médicas, etc. Una vez realizada la simulación de los algoritmos AES CBC y Mapa de Arnold en dos máquinas virtuales, se llegó a la conclusión con respecto al tiempo de procesamiento de las imágenes digitales que AES CBC tiene una amplia ventaja tanto en cifrar y descifrar una imagen en un computador con diferentes características de hardware, esto debido a que el Mapa de Arnold utiliza una técnica de iteración que permite mover los pixeles de posición cumpliendo con una particularidad muy fundamental en los algoritmos basados en la teoría del Caos. Sin embargo, una de las ventajas del Mapa de Arnold está en la calidad de cifrado de una imagen respecto al algoritmo tradicional AES CBC, de acuerdo a la figura 19 los resultados indican que el coeficiente de correlación del Mapa de Arnold es superior al de

AES CBC, concluyendo que; el Mapa de Arnold no altera cada uno de los pixeles de una imagen como si lo hace AES CBC.

Esta investigación es el punto de partida que puede ayudar en otras investigaciones en la que se analice la calidad de cifrado, descifrado y el tiempo de procesamiento que se pueden usar al momento de cifrar y descifrar imágenes digitales como: ecografías, radiografías, tomografías, resonancia magnética, que se almacenan como historia clínica de un paciente y que necesitan tener un alto grado de calidad al momento de descifrar, considerando además características físicas de un equipo de cómputo para la optimización del cifrado y descifrado de las imágenes digitales

La limitante durante el análisis de los algoritmos de cifrado y descifrado estuvo determinado por el porcentaje de iteraciones Para el proceso de cifrado de una imagen digital con el Mapa de Arnold se recomienda utilizar un número de iteraciones entre el 25 al 75 por ciento del tamaño de la imagen debido a que en este intervalo se consigue una mejor calidad de cifrado, teniendo en cuenta que, cuando el número de iteraciones es igual al tamaño de la imagen el resultado es la imagen original.

Para trabajos futuros se puede aplicar esta investigación a casos reales, desarrollando un servicio que pueda ser consumido desde una aplicación móvil para cifrar las imágenes almacenadas en dispositivos móviles y así poder recopilar más datos que ayuden a mejorar el presente trabajo.

Además la presente investigación puede ser utilizada para otro análisis, en donde se pueda realizar comparativas de rendimiento al momento de cifrar y descifrar imágenes entre sistemas operativos de libre distribución y comerciales

REFERENCIAS BIBLIOGRAFICAS

Ahmad, J., & Ahmed, F. (2010). Efficiency analysis and security evaluation of image encryption schemes. *Computing*, *23*, 25.

Boccaletti, S., Kurths, J., Osipov, G., Valladares, D. L., & Zhou, C. S. (2002). The synchronization of chaotic systems. *Physics Reports*, *366*(1–2), 1–101.

Bruck, H. A., McNeill, S. R., Sutton, M. A., & Peters, W. H. (1989). Digital image correlation using Newton-Raphson method of partial differential correction. *Experimental Mechanics*, *29*(3), 261–267.

Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

Devaney, R. L., & Eckmann, J.-P. (1987). An Introduction to Chaotic Dynamical Systems. *Physics Today*, *40*, 72.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *Information Theory, IEEE Transactions On*, *22*(6), 644–654.

Espinoza Illanes, M. (2015). *Cifrado de imágenes digitales basado en teoria del caos: mapas logisticos*. ETSI_Informatica.

Ferguson, N. (2006). AES-CBC+ Elephant diffuser: A disk encryption algorithm for Windows Vista.

Frankel, S., Glenn, R., & Kelly, S. (2003). *The AES-CBC cipher algorithm and its use with IPsec*.

Galeano Villa, J. L., Castañeda, Á., & Camilo, C. (2013). Protocolo de politicas de seguridad informática para las universidades de Risaralda.

Godinez Rodriguez, E. (2015). Cifrado de imágenes utilizando advanced encryption standard (AES) con permutación variable.

Granados Paredes, G. (2006). Introducción a la Criptografia. *Articulos*.

Guan, Z.-H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. *Physics Letters A*, *346*(1–3), 153–157.

Gutiérrez-Martinez, J., Núñez-Gaona, M. A., Aguirre-Meneses, H., & Delgado-Esquerra, R. E. (2014). Implementación de la seguridad en el manejo de las imágenes médicas. *Investig En Discapac*, *3*(4), 177–184.

Hariyanto, E., & Rahim, R. (2016). Arnold's Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research (IJSR)*, *5*(10), 1363–1365.

Koduru, S. C., & Chandrasekaran, V. (2008). Integrated confusion-diffusion mechanisms for chaos based image encryption. In *Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on* (pp. 260–263).

Kolmogorov, A. (1956). On the Shannon theory of information transmission in the case of continuous signals. *IRE Transactions on Information Theory*, *2*(4), 102–108.

Lian, S., Sun, J., & Wang, Z. (2005). A block

cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals*, *26*(1), 117–129.

López-Mancilla, D., & Villa, J. M. R. (2014). Encriptado de Imágenes Usando Modelos Caóticos Continuos y Discretos. In *XXIX Congreso de Instrumentación*.

Millérioux, G., Hernandez, A., & Amigo, J. M. (2005). Criptografia caotica con reinyeccion de la informacion. In *III Congreso Iberoamericano di Seguridad Informatica, CIBSI'05* (pp. 207–220).

Munné, F., & others. (1995). Las teorias de la complejidad y sus implicaciones en las ciencias del comportamiento. *Revista Interamericana de Psicologia*, *29*(1), 1–12.

Ozturk, I., & Sogukpinar, I. (2004). Analysis and comparison of image encryption algorithms. *International Journal of Information Technology*, *1*(2), 108–111.

Parvees, M. Y. M., Samath, J. A., & Bose, B. P. (2016). Secured medical images-a chaotic pixel scrambling approach. *Journal of Medical Systems*, *40*(11), 232.

Piper, F. (2002). *Cryptography*. Wiley Online Library.

Pisarchik, A. N., & Zanin, M. (2008). Image encryption with chaotically coupled chaotic maps. *Physica D: Nonlinear Phenomena*, *237*(20), 2638–2648.

Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, 19–22.

Rodriguez, I. F. R., Barrera, E. I. A., Parra, C. A. S., & Posada, J. D. M. (2017). Algoritmo de Encriptación de Imágenes Utilizando el Atractor Caótico de Lorenz. *Ingenieria*, *22*(3), 1.

Rojas Matas, Á., & Cano Rojas, A. (2011). Cifrado de imágenes y Matemáticas. *TE & ET*.

Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption using advanced encryption standard. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *3*(3), 118–126.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal*, *28*(4), 656–715.

Steinmetz, R., & Nahrstedt, K. (2002). *Multimedia: Computing, Communications and Applications: Media Coding and Content Processing*. Prentice Hall PTR.

Vilchis, M. A. M., Alvarado, E. V., & Ortigoza, R. S. (2007). Teoria del Caos en la Protección de Información. *Polibits*, (35), 7–11.

Younes, M. (2009). An Approach To Enhance Image Encryption Using Block-Based Transformation Algorithm. *University Sains Malaysia*.

Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. *World Academy of Science, Engineering and Technology*, *27*, 206–211.