UACJ INVESTIGACIÓN

Título del Proyecto de Investigación a que corresponde el Reporte Técnico:

Sistema digital para encriptar imágenes que utiliza llaves caóticas discretas

Tipo de financiamiento

Sin financiamiento

TÍTULO DEL REPORTE TÉCNICO

Sistema digital para encriptar imágenes que utiliza llaves caóticas discretas

Autores del reporte técnico:

Dr. Héctor Garcés Guzmán
Dr. Victor Manuel Hinostroza Zubía
Ing. Priscila Betsabe Hernández Valadez

TÍTULO DEL REPORTE TÉCNICO

Resumen del reporte técnico en español (mínimo 600 palabras):

El desarrollo tecnológico de las primeras dos décadas del siglo XXI ha proveído a la población con herramientas robustas para la distribución de la información. Hoy en día es más fácil y rápido compartir conocimiento de cualquier tipo, sin importar las distancias. Todo esto gracias entre otros avances, a la red de computadoras que intercomunica al mundo entero. Sin embargo, la próxima generación de sistemas de telecomunicación enfrentará grandes retos, teniendo en cuenta que en un minuto se transmiten vía internet aproximadamente: 18 millones de textos, 4.3 millones de videos, un millón de accesos a Facebook, 3.7 millones de búsquedas en Google, etc. Entre los desafíos que se esperan para manejar esta gran cantidad de información destacan: seguridad, conexión masiva de dispositivos, tiempo de retardo extremadamente bajo, menor consumo de energía, etc. Para la sociedad la confidencialidad de la información siempre ha sido esencial, por consiguiente, el cifrado de mensajes es una importante área de estudio debido a los requerimientos de invulnerabilidad. Por ende, se requiere de métodos que aseguren la privacidad del mensaje transmitido, es decir, que la información enviada sólo sea conocida por el destinatario y que permanezca oculta a cualquier otra entidad que intente tener acceso. Para reforzar la seguridad en el intercambio de información, se han propuesto modelos de cifrado de imágenes en escala de grises que requieren de procesos diferentes a los usados hasta ahora, entre los que se encuentran la utilización de claves caóticas. Estos algoritmos destacan por tener varias propiedades tales como: ergodicidad, amplio ancho de banda, comportamiento pseudo aleatorio y alta sensibilidad a las condiciones iniciales [1]. Además, para la seguridad de un sistema de comunicación, los algoritmos de encriptado deben tener como punto fuerte la llave y no tanto el proceso usado para el cifrado. Este proyecto tiene la finalidad de analizar la fortaleza de veinte llaves caóticas, desarrolladas usando modelos discretos y unidimensionales. Para obtener una

cantidad significativa de muestras para el análisis estadístico de las llaves caóticas, se seleccionaron cinco imágenes distintas conocidas en la comunidad científica, en escala de grises: cell, circbw, eight, logo y Lena. Se valoró su capacidad de encriptación generando mil imágenes encriptadas, y mediante las siguientes herramientas estadísticas de prueba: histograma, distribución de valores de pixeles vecinos, entropía y correlación de pixeles. El desempeño que presentaron las figuras encriptadas examinadas fue satisfactorio en todas las pruebas a las que se sometieron, con la excepción de los mapas caóticos cuadrático y logístico modificado. El primero tuvo un pobre rendimiento en la evaluación de la entropía. Mientras que el segundo mostro una alta correlación entre pixeles vecinos lo cual denota una insuficiente encriptación.

Resumen del reporte técnico en inglés (mínimo 600 palabras):

The technological development of the first two decades of the 21st century has provided the population with robust tools for the distribution of information. Nowadays it is faster and easier to share knowledge of any kind, regardless of distances. All this thanks, among other advances, to the computer network that intercommunicates the entire world. However, the next generation of telecommunication systems will face great challenges, taking into account that in one minute approximately it is transmitted via internet the following: texts 18 million, videos 4.3 million, Facebook access one million, searches on Google 3.7 million, etc. Among the challenges that are expected to handle this large amount of information are: security, massive connection of devices, extremely low latency, lower energy consumption, etc. For society the confidentiality of information has always been essential, consequently, message encryption is an important area of study due to invulnerability requirements. Therefore, methods are required to ensure the privacy of the transmitted message, that is, that the information sent is only known by the recipient and remains hidden to any other entity that tries to access. To reinforce security in the exchange of information, balk and white image encryption models have been proposed that require different processes than those used so far, including the use of chaotic keys.

These algorithms stand out for having several properties such as: ergodicity, broad bandwidth, pseudo random behavior and high sensitivity to initial conditions [1]. In addition, for the security of a communication system, encryption algorithms must have the key as a strong point and not so much the process used for encryption. This project aims to analyze the strength of twenty chaotic keys, developed using discrete and one-dimensional models. To obtain a significant number of samples for the statistical analysis of the chaotic keys, five different white and black images well known in the scientific community were selected, those are: cell, circbw, eight, logo and Lena. Its encryption capacity was assessed by generating a thousand encrypted images, and using the following statistical test tools: histogram, distribution of neighboring pixel values, entropy and pixel correlation. The performance presented by the encrypted figures examined was satisfactory in all the tests they underwent, with the exception of the chaotic maps quadratic and logistic modified. The first had poor performance in the entropy evaluation. While the second showed a high correlation between neighboring pixels, which demotes insufficient encryption.

Palabras clave: Caos, encriptación, telecomunicaciones

Usuarios potenciales (del proyecto de investigación**):**

_____
_____
_____
_____
_____.....

Reconocimientos (agradecimientos a la institución, estudiantes que colaboraron, instituciones que apoyaron a la realización del proyecto, etc.**):**

_____
_____
_____
_____
_____.....

1. INTRODUCCIÓN

Los avances tecnológicos de este siglo han proporcionado a la población herramientas robustas para la distribución de la información. Es más fácil y rápido compartir conocimiento de cualquier tipo, sin importar las distancias o las limitaciones físicas. Todo esto gracias a la red de computadoras que intercomunica al mundo entero: Internet. La existencia de esta red ha traído consigo una evolución en la forma en que nos comunicamos, dándole un papel importante a las imágenes, las cuales en diversos casos han llegado a reemplazar por completo a la comunicación por texto. Al aumentar los usuarios en la red también lo hicieron la cantidad de archivos de imagen almacenados o enviados por Internet. Gracias a esto se presentó un problema importante que demandó urgentemente una solución, la seguridad de la información contenida en las imágenes. Este aumento en el tráfico de datos requiere de métodos que aseguren la privacidad del mensaje transmitido, es decir, que la información enviada sólo sea conocida por los destinatarios y que permanezca oculta a cualquier otra entidad que intente tener acceso.

Como respuesta a este problema, en el campo de la encriptación electrónica se han propuesto modelos de cifrado de imágenes que requieren de procesos diferentes de los actualmente utilizados. En esta área se han desarrollado diversos métodos y algoritmos, capaces de ocultar la información real que compone al archivo digital. Uno de estos métodos, el cual ha sido de gran relevancia en las últimas décadas por su innovación y alta seguridad es la utilización de llaves caóticas, obtenidas a partir de sistemas caóticos. Las llaves caóticas ofrecen una solución al problema de seguridad presente en las comunicaciones electrónicas, en específico en la simplificación del proceso de encriptado de imágenes [2].

En este proyecto se desarrolló un algoritmo de encriptación a base de llaves caóticas para imágenes en escala de grises, además de un estudio del comportamiento de algunos de los diferentes sistemas caóticos disponibles al

utilizarlos dentro del modelo de cifrado como generadores de llaves de encriptación. Dentro del estudio se contemplaron cuatro herramientas de prueba: histograma, entropía, correlación de pixeles y distribución de valores de pixeles vecinos. El desempeño que presentaron los diferentes sistemas caóticos fue satisfactorio en todas las pruebas a las que se sometieron, con la excepción de dos casos: el sistema cuadrático, que rindió pobremente en la prueba de entropía, y el logístico modificado, que mostró deficiencias en los resultados de la correlación de pixeles.

2. PLANTEAMIENTO

- Antecedentes

Un principio científico es encontrar la relación entre causa y efecto, y a través de esta conexión predecir el comportamiento de los fenómenos naturales. Isaac Newton aceleró el desarrollo de las ciencias, al aportar la herramienta base para el desarrollo de sistemas y fórmulas utilizadas en la representación de los fenómenos naturales, el cálculo infinitesimal. Los contemporáneos de Newton mantenían el principio del determinismo, el cual establece que el estado presente de cierto sistema era la consecuencia del estado anterior y la causa del estado futuro. Por lo tanto, la única dificultad presente para pronosticar los estados de cualquier fenómeno era recopilar la suficiente información necesaria [3]. Por otro lado, Laplace aseguraba que, si existiera un ser capaz de conocer la locación exacta y las velocidades de todos los objetos, así como las fuerzas que se ejercían sobre ellos, podría calcular el estado pasado o futuro del sistema para cualquiera de sus variables.

Con las leyes de Newton y el cálculo diferencial como herramientas, los científicos comenzaron a buscar ecuaciones que explicaran y describieran los fenómenos naturales, encontrando un orden en el universo. Sin embargo, seguía habiendo partes de la naturaleza en las que era imposible encontrar un orden por medio de los métodos conocidos en ese tiempo [4]. Por ejemplo, el problema

de los tres cuerpos celestes el cual consiste en determinar en cualquier instante las posiciones y velocidades de tres cuerpos, sometidos a atracción gravitacional mutua [5].

A finales del siglo XIX, Henri Poincaré como respuesta a este enigma llegó a la conclusión que la interacción de más de dos cuerpos celestes, presenta un comportamiento aparentemente aleatorio. Por consiguiente, no es posible hacer predicciones de su comportamiento. Con esto Poincaré encontró que algunos sistemas no lineales deterministas bajo ciertas condiciones pueden generar una señal que presenta un comportamiento estocástico, a pesar de que su naturaleza es esencialmente determinista. Debido a esto, el conocimiento que pueda tenerse de éstos es siempre impreciso [6]. Este fue el primer paso en el descubrimiento de lo que ahora se llama sistemas caóticos.

La teoría del caos se consideró como el más grande avance del siglo XX para las ciencias naturales. A pesar de la renuencia de los matemáticos al enfrentarse a un nuevo sistema para representar el mundo que nos rodea, la popularidad de esta teoría creció rápidamente. La mayor utilidad de la teoría propuesta fue analizar fenómenos que habían sido imposibles de estudiar con los métodos tradicionales deterministas [7].

- Marco teórico

Un oscilador caótico discreto y unidimensional se define como una función no lineal iterativa o de mapeo $f: \phi \rightarrow \phi$ que puede ser escrita como

$$\phi_{(k+1)} = f(\phi_k) \tag{1}$$

Hay un gran número de sistemas en los cuales se ha observado un comportamiento caótico; en particular en la tabla 1 se muestra la definición matemática. También se incluye el rango de valores de algún(os) parámetro(s)

donde el modelo abandona su respuesta determinista para llegar a la denominada región caótica. de los veinte mapas contemplados para este estudio [8].

Tabla 1 Mapas caóticos.

Mapa	Definición	Régimen caótico
Bernoulli	$\phi_{(k+1)} = \begin{cases} B\phi_k + A & \phi_k < 0 \\ B\phi_k - A & \phi_k > 0 \end{cases}$	$\phi_k \in [-A, A]$ $0 < B < 2$
Bernoulli shift 3	$\phi_{(k+1)} = \mathrm{mod}((A * \phi_k), 1)$	
Bernoulli shift 4	$\phi_{(k+1)} = 1 - \mathrm{mod}((A * \phi_k), 1)$	
Chebyshev	$\phi_{(k+1)} = \cos(B\ arccos(\phi_k))$	$\phi_k \in [-1,1]$ $1 < B < 10$
Congruente	$\phi_{(k+1)} = \begin{cases} B\phi_k - C & \phi_k > A \\ B\phi_k & \lvert\phi_k\rvert \le A \\ B\phi_k + C & \phi_k < -A \end{cases}$	$\phi_k \in [-C, C]$ $1 < B < 2$ $C = 2A$
Coseno	$\phi_{(k+1)} = A\cos(\phi_k + B)$	$\phi_k \in [-A, A]$ $2 < A < 10$ ó $-\pi < B < \pi$
Cuadrático	$\phi_{(k+1)} = B - (A\phi_k^2)$	$\phi_k \in \left[-\frac{2}{A}, \frac{2}{A}\right]$ $\frac{3}{4} < AB < 2$
Cúbico 1	$\phi_{(k+1)} = C(3\phi_k - 4\phi_k^3)$	$\phi_k \in [-C, C]$ $0 < C < \infty$
Cúbico 2	$\phi_{(k+1)} = (1 - C)\phi_k + C\phi_k^3$	$\phi_k \in \left[-\frac{3-2c}{3\sqrt{3}}, \frac{3-2c}{3\sqrt{3}}\right]$ $-\infty < C < 3/2$
Cúbico 3	$\phi_{(k+1)} = C(\phi_k - \phi_k^3) = C\phi_k(1 - \phi_k^2)$	$\phi_k \in \left[-\frac{2c}{\sqrt{3}}, 0\right]$ $0 < C < 2.6$
Exponencial	$\phi_{(k+1)} = \phi_k \exp(B(A - \phi_k))$	$\phi_k \in [0, \frac{\exp(AB-1)}{B}]$ $AB > 2$
Hopping	$\phi_{(k+1)} = \begin{cases} D(\phi_k - A) + C & \phi_k > A \\ B\phi_k & \lvert\phi_k\rvert \le A \\ D(\phi_k + A) - C & \phi_k < -A \end{cases}$	$\phi_k \in [-C, C]$ $B, -D > 1\ \ C = BA$
Logístico	$\phi_{(k+1)} = B(A^2 - \phi_k^2) - A$	$\phi_k \in [-A, A]$ $\frac{3}{2} < AB < 2$
Logístico bipolar	$\phi_{(k+1)} = 1 - \mu\phi_k^2$	$\mu \in (0,2]$ $\phi_k \in [1 - \mu, 1]$
Logístico modificado	$\phi_{(k+1)} = \lambda\phi_k(1 - A\phi_k)$	$\lambda \in (0,4], A > 1$ $\phi_k \in [0, \lambda/4k]$
Sinusoidal 1	$\phi_{(k+1)} = Csin(\pi\phi_k)$	$\phi_k = [0, C]$ $0 < C < 1$
Tienda	$\phi_{(k+1)} = A - B\lvert\phi_k\rvert$	$\phi_k \in [A(1 - B), A]$ $0 < B < 2$
Tienda Bipolar	$\phi_{(k+1)} = \frac{1 + C^2 - 2C\phi_k - 2\lvert\phi_k - C\rvert}{1 - C^2}$	$C \in (-2,2)$ $\phi_k \in [-1,1]$
Tienda Oblicuo	$\phi_{(k+1)} = \frac{C + \phi_k(1 - 2C) - \lvert\phi_k - C\rvert}{2C(1 - C)}$	$C \in (-2,2)$ $\phi_k \in [0,1]$
Tienda Simétrico	$\phi_{(k+1)} = \beta(1 - \lvert\phi_k\rvert) - 1$	$\beta \in [0,2]$ $\phi_k \in [-1, \beta - 1]$

El comportamiento aparentemente impredecible de las señales caóticas puede ser visto de una manera diferente cuando son descritas por su mapa de retorno, éste se obtiene al graficar dos muestras sucesivas $\phi_k \; vs \; \phi_{k+1}$ generadas por (1). En los mapas de retorno ilustrados en las figuras 1–2 se observa el determinismo a corto plazo.

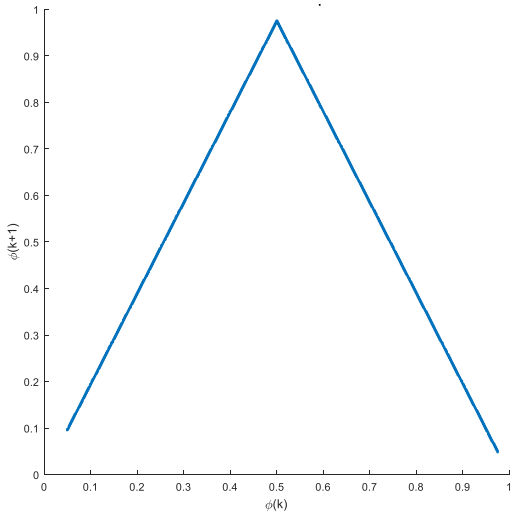


Figura 1. Mapa de retorno del oscilador tienda de campaña, para A=1.95.

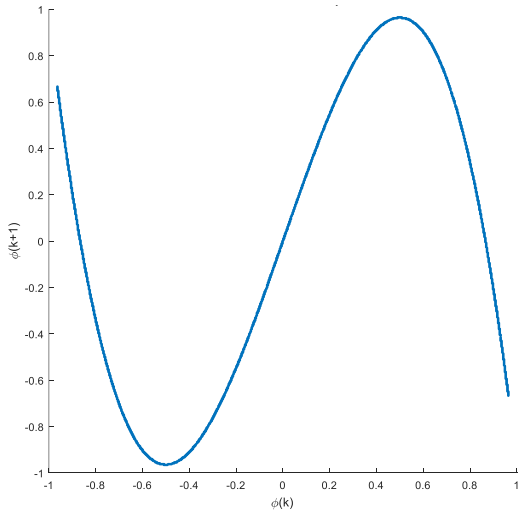


Figura 2. Mapa de retorno del oscilador cubico 1, para C=0.964.

Si bien las funciones mostradas en la tabla 1 son deterministas, poseen características singulares. Una manera de darse cuenta de ese peculiar comportamiento es variar el valor de algún parámetro de la función de mapeo dentro de un rango especifico, por consiguiente, se obtiene el denominado diagrama de bifurcación. Mitchell Jay Feigenbaum presentó en 1975 el primer mapa de bifurcación, que pertenece al sistema caótico logístico.

Una bifurcación ocurre cuando se varía un parámetro de control al sistema dinámico modificando así su comportamiento, para llegar a un punto crítico ocasionando la pérdida de estabilidad del sistema [7]. En este diagrama se aprecia que después de una bifurcación se tiene un comportamiento aleatorio, con valores sin repeticiones, pero que siempre están acotados por rangos específicos [9]. Es decir, a pesar de que el caos está relacionado con el desorden, la confusión o lo impredecible, el diagrama de bifurcación muestra que el caos tiene fronteras. Por ejemplo, para el mapa coseno, en la figura 3 se ilustra su evolución al variar el parámetro A en el rango de [1.5 3]. En esta grafica claramente se distinguen dos regiones, en la primera por ejemplo para $A = 1.7$ el resultado de todas las iteraciones siempre es el mismo $\phi(k) = \pm 1.5$, esto es dentro de la zona determinista. Por lo contrario para $A = 2.25$ el resultado de cada iteración varia en un rango aproximado de $\phi(k) \in [-2.2 \ \ 2.2]$, esta es un área de operación caótica. Un análisis cuidadoso de la figura 3 muestra una alternancia o bifurcación entre regiones caóticas y deterministas.

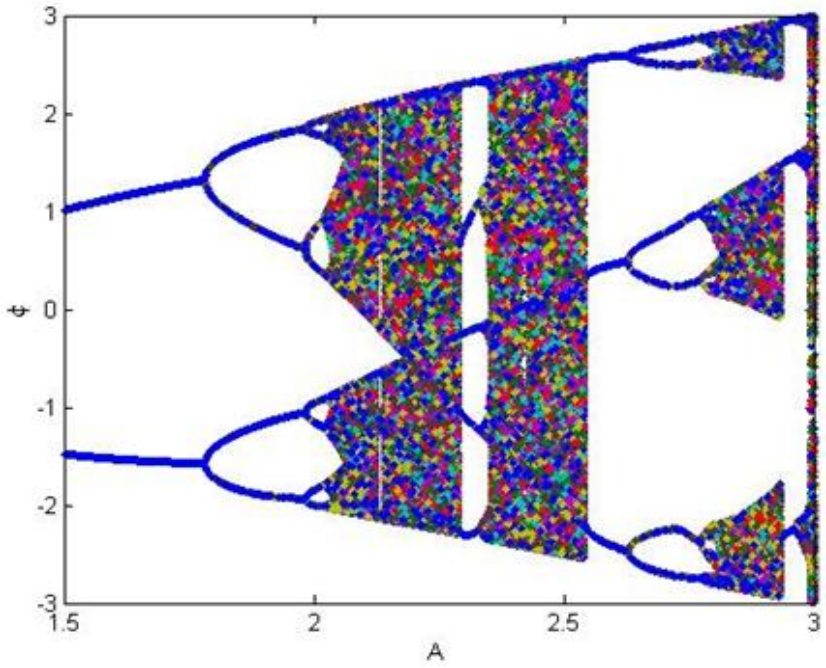


Figura 3 Diagrama de bifurcación del mapa coseno.

3. METODOLOGÍA

Por lo que se refiere al proceso de encriptación de imágenes y su posterior análisis, en primer lugar, se construyó un cifrador en una Raspberry Pi. A continuación, los datos obtenidos fueron estudiados en Matlab. Se seleccionó la Raspberry pi por las siguientes razones: bajo costo, lenguaje de programación de alto nivel (Python), considerable potencia computacional y tamaño no mayor a una tarjeta de crédito. En lo que concierne a Python, este es un lenguaje para scripts, no tiene la necesidad de un compilador en sí y la sintaxis es más sencilla. Debido a esto, es muy atractivo para un rápido desarrollo de aplicaciones [10].

Para el diseñó del encriptador digital se utilizó como base el algoritmo presentado por el Dr. Inzunza [11], el cual tiene como elemento esencial al operador booleano XOR para la adición de la llave de cifrado a la imagen original, tal como se muestra en la figura 4.

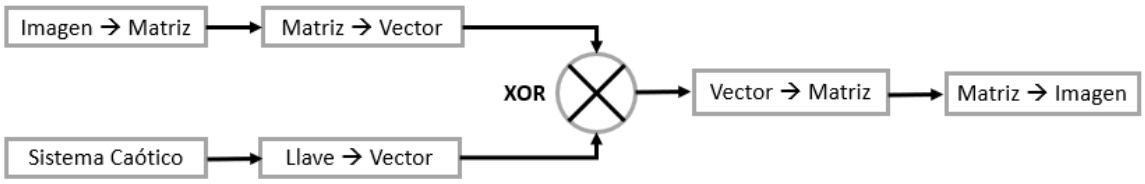


Figura 4. Sistema de encriptación desarrollado.

El proceso de des encriptación es en esencia el mismo. Se comienza con la lectura a un vector de la imagen encriptada, luego se genera de nuevo la misma llave caótica utilizando parámetros iniciales idénticos. A continuación, se realiza la operación XOR, después de esto los pixeles recobrarán sus valores originales, obteniendo la imagen que se tenía en un principio. Este proceso se repite para cada uno de los veinte sistemas caóticos enlistados en la tabla 1.

Con el propósito de realizar un análisis exhaustivo de las veinte llaves caóticas se seleccionaron cinco figuras comúnmente empleadas en el procesamiento de imágenes: cell, circbw, eight, Lena y logo. Estas difieren en dos aspectos; tamaño y entropía, en la tabla 2 se especifican sus características.

Tabla 2. Características principales de las imágenes de prueba.

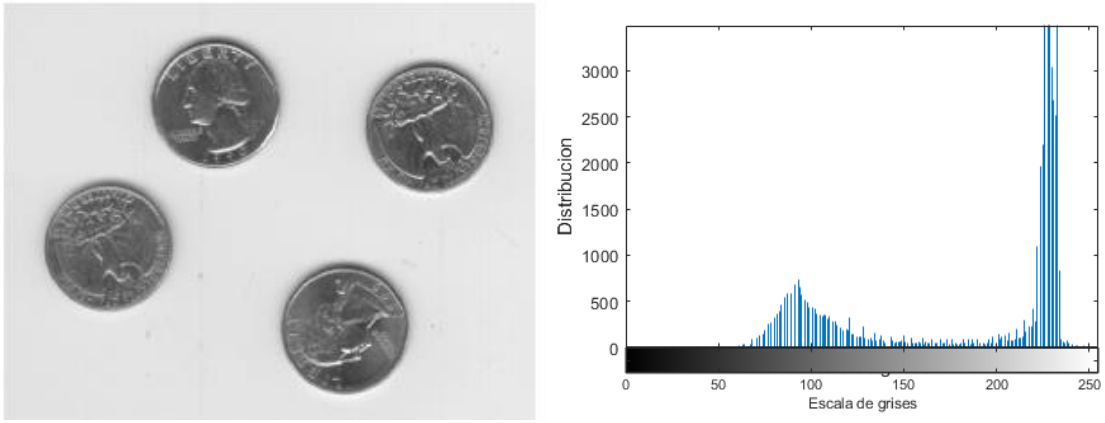
Imagen	Tamaño en pixeles	Entropía
cell.tif	159x91	4.6024
circbw.tif	280x272	0.9996
eight.tif	242x308	4.8796
lena.bmp	512x512	7.4455
logo.tif	107x122	1

Además, se eligió variar un parámetro de control de cada uno de los veinte mapas, es decir uno de los parámetros de su definición mostrada en la tabla 1.

Hay que destacar que el rango de variación del parámetro de control está dentro de la región de operación caótica. Combinando las cinco figuras, los veinte mapas y la variación del parámetro de control se obtuvieron más de mil imágenes cifradas. Esta es una cantidad significativa de muestras requeridas con la finalidad de evaluar la habilidad de encriptación de las llaves bajo estudio. Finalmente se obtuvo el valor medio de cada una de las siguientes herramientas estadísticas, a las que se sometieron las mil imágenes: histograma, distribución de valores de pixeles vecinos, entropía y correlación de pixeles.

4. RESULTADOS

El histograma es un método muy útil para representar de una manera organizada un conjunto de datos. Por ende, su uso puede corroborar analíticamente la diferencia existente entre la imagen original y la encriptada. En la figura 5 se puede apreciar como los valores de los pixeles para la imagen de eight varían dentro del rango posible para la escala de grises, presentando dos picos en los valores más recurrentes de la escala de grises.

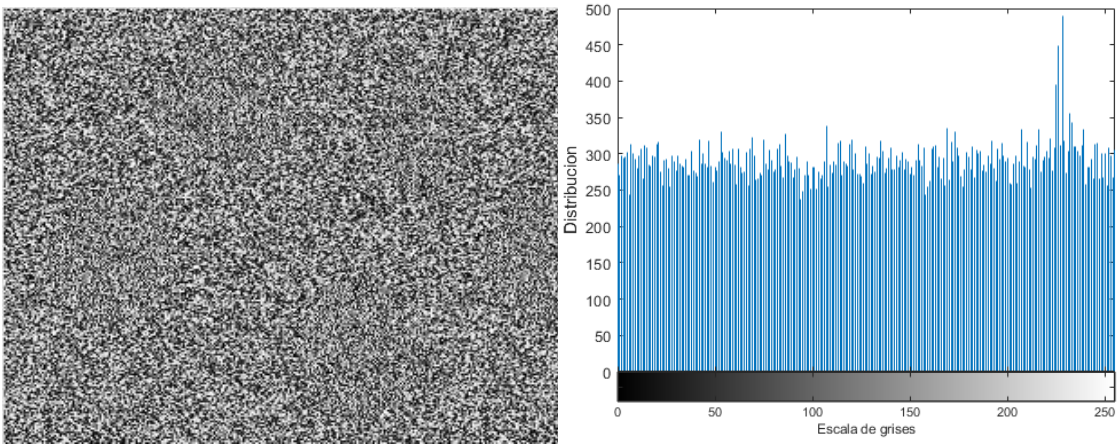


a) *b)*

Figura 5. a) Eight original b) Histograma

Por lo contrario, en la figura 6 se exhibe la imagen de eight encriptada con una llave basada en el sistema Hopping y su histograma. Esta representación gráfica semeja una pdf uniforme, note la casi ausencia de crestas y valles. Del

histograma se puede inferir que no es posible obtener información concreta de la imagen original a partir de la cifrada, gracias a la distribución uniforme. En la mayoría de los mil casos examinados se observó una distribución de probabilidad casi uniforme de valores en la escala de grises, confirmando la eficacia del proceso de cifrado.



a) *b)*

Figura 6. a) Eight encriptada. b) Histograma de eight encriptada.

Más adelante, para observar de manera gráfica la distribución de valores de pixeles vecinos se recurrió al empleo de un plano cartesiano como herramienta de análisis. Cada punto en el esquema se obtuvo de la siguiente manera; en el eje horizontal del plano se consideró el valor en la escala de grises de un pixel ubicado en la imagen en las coordenadas [x, y], mientras que en el eje vertical se usó el valor del pixel contiguo localizado en [x, y+1]. Como resultado, en la figura 7 b) es posible apreciar como la concentración de valores de la imagen cell es más densa en una línea recta con pendiente uno, lo que indica la existencia de alta redundancia entre pixeles adyacentes. Por el contrario, la distribución de valores de pixeles vecinos en la imagen cell cifrada, figura 7 d) ocupa todo el espacio delimitado por la gráfica. Es decir, los pixeles de la imagen encriptada no presentan relación alguna con los pixeles próximos. También este resultado se repite en la generalidad de las muestras analizadas,

lo que comprueba una vez más la eficacia de la encriptación a base de llaves caóticas.

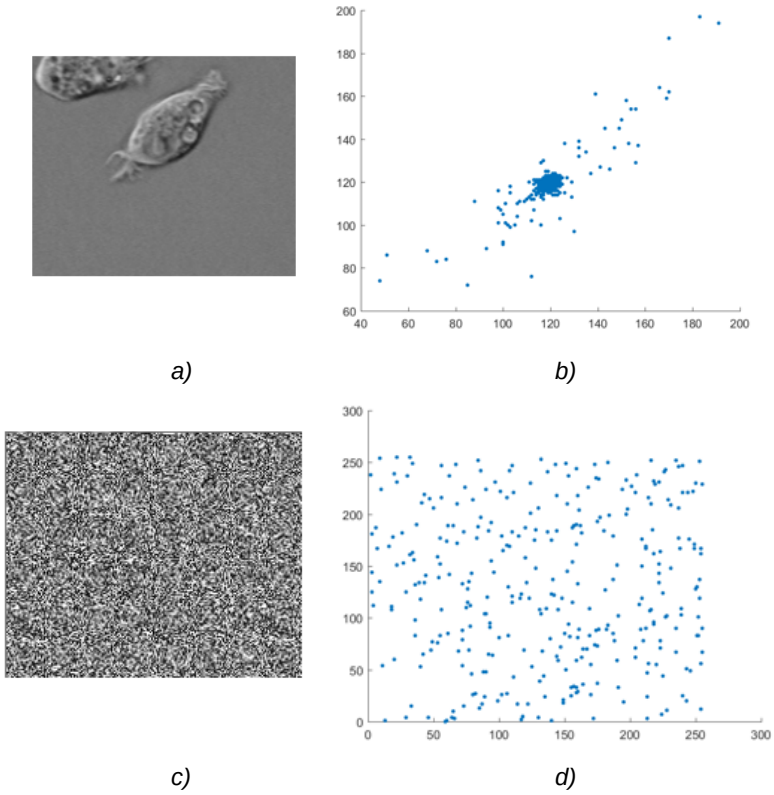


Figura 7. a) cell. b) dist. de pixeles vecinos, c) cell encriptado, d) dist, de pixeles vecinos.

Otro punto considerado en este estudio fue la entropía, es decir la medición del desarreglo de los pixeles en su nivel en la escala de grises. Para comparar el orden o desorden en el contenido de la imagen, antes y después de la encriptación. La figura 8 ilustra la diferencia existente entre la entropía calculada de una imagen simple como circbw original a la obtenida en la encriptada. Aquí se observa como el proceso de cifrado incrementa la entropía de un valor menor a uno hasta su valor máximo de ocho. En particular el desempeño de la llave basada en el mapa cuadrático es muy pobre, solo incrementa la entropía a un valor cercano a dos. Al continuar comparando las cuatro imágenes encriptadas restantes con las veinte llaves caóticas se observó

el mismo comportamiento, todos los valores de la entropía obtenidos están cerca del valor máximo ocho, con la excepción del mapa cuadrático.

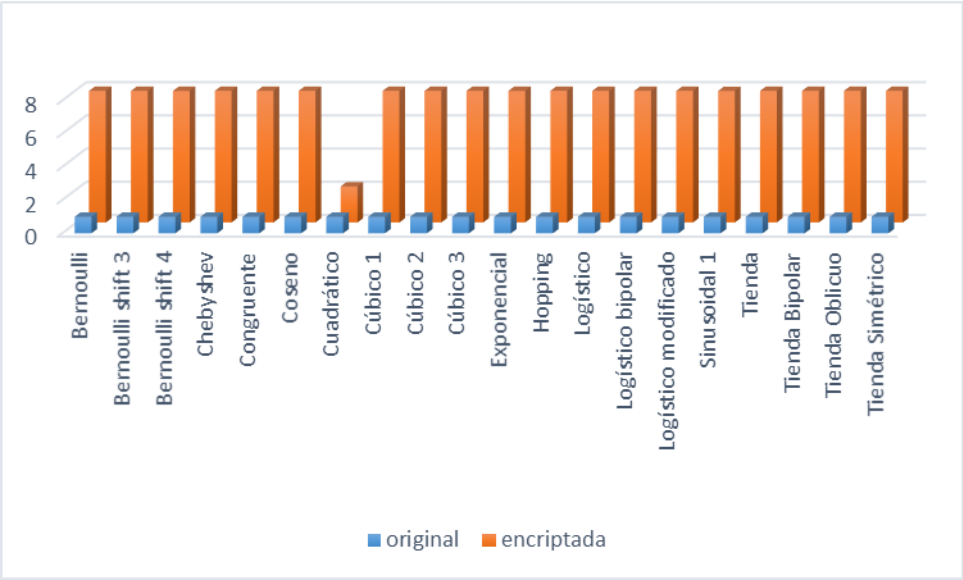


Figura 8. Entropía de la imagen circbw.

Finalmente, para conocer si el proceso estudiado reduce la redundancia entre pixeles vecinos o si esta persiste aun después de la encriptación, se evaluó su correlación. Considerando las variables aleatorias x y y definidas por los valores del nivel de gris de un par de pixeles, su coeficiente de correlación está dado por (2)

$$\rho_{xy} = \frac{C_{xy}}{\sigma_x \sigma_y} \tag{2}$$

donde σ_x es la desviación estándar de x, y C_{xy} es la covariancia entre x y y. Para cada una de las imágenes se seleccionaron aleatoriamente 333 pixeles y se compararon con tres de los pixeles adyacentes, estos que se encuentran localizados abajo, a la derecha y en la esquina inferior derecha como se muestra en la figura 6. Por ende, se formaron 999 pares de pixeles.

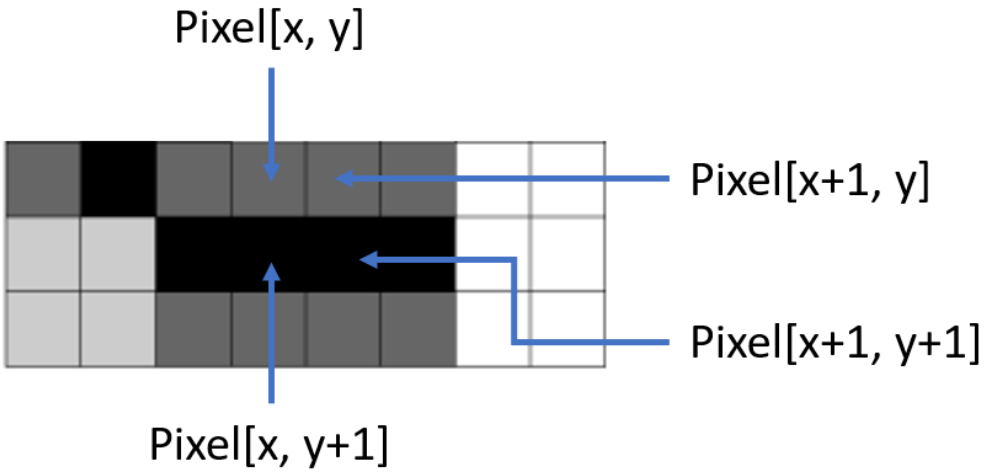


Figura 9. Tres pixeles adyacentes.

Como parámetro de referencia se calculó la correlación de pixeles de las cinco imágenes originales. Luego de cada una de ellas se seleccionaron imágenes encriptadas con los valores intermedios de su parámetro de control, para cada uno de los veinte sistemas caóticos. Como resultado, solo se evaluaron cien imágenes cifradas. Tomando como ejemplo a la imagen cell, en la gráfica de la figura 10 se muestra la comparación de los coeficientes de correlación por sistema caótico entre el pixel central [x, y] y el inferior inmediato [x, y+1]. A continuación, en la figura 11 se ilustra lo mismo, pero partir del pixel central [x, y] y su vecino a la derecha [x+1, y]. Por último, el tercer coeficiente, mostrado en la figura 12, se obtuvo con la combinación del pixel central [x, y] y el adyacente hacia la derecha [x+1, y+1].

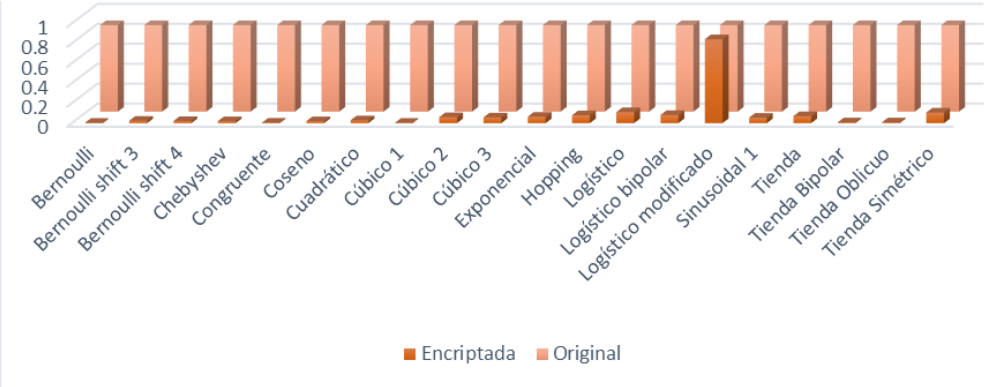


Figura 10. Correlación de pixeles hacia abajo.

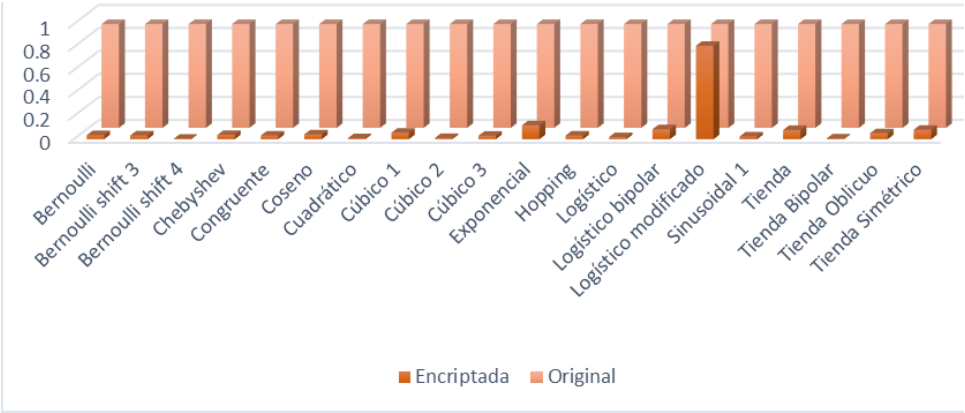


Figura 11. Correlación de pixeles hacia la derecha.

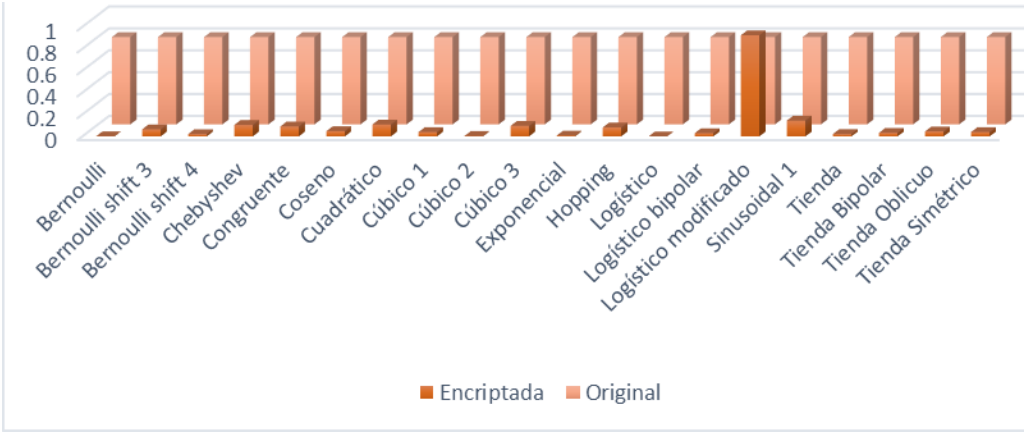


Figura 12. Correlación de pixeles en diagonal.

Al analizar las gráficas en las figuras 10 al 12, es posible observar que el coeficiente de correlación calculado en la imagen original tiene un valor cercano a uno. Obviamente por la alta redundancia contenida en la imagen. Por el contrario, los valores evaluados a partir de las imágenes encriptadas se muestran muy cercanos al cero. Indiscutiblemente esto indica una correlación casi nula entre los pares de pixeles, en cualquiera de sus tres direcciones. La diferencia existente entre las cien imágenes evaluadas es pequeña. El único sistema que no presentó consistencia fue el logístico modificado, pero de una forma negativa, pues sus valores de correlación en las tres direcciones se muestran similares a la imagen original.

5. CONCLUSIONES

En este trabajo de investigación se consiguió el objetivo planteado ya que se pudo poner en funcionamiento una sencilla y barata implementación de un encriptador digital, con hardware y software de uso común y fácilmente accesible. Específicamente un sistema de cifrado de imágenes en escala de grises, empleando el sistema de cómputo reducido Raspberry Pi. Además, se profundizó en el conocimiento de diversas llaves de encriptación elaboradas a partir de secuencias caóticas discretas y unidimensionales, al estudiar estadísticamente su fortaleza. También se procedió a realizar un análisis de la estabilidad del comportamiento de cada uno de los veinte osciladores caóticos estudiados, al variar un parámetro de control dentro de la región caótica. Como resultado se obtuvieron y analizaron mil imágenes cifradas.

Para comprobar la efectividad del proceso de cifrado, las mil imágenes encriptadas se sometieron a cuatro diferentes análisis estadísticos: histograma, entropía, correlación de pixeles y la distribución de los valores en la escala de gris de los pixeles vecinos Con la información que se obtuvo hasta este punto, se puede concluir que la mayoría de los sistemas caóticos seleccionados para la implementación del encriptador son eficaces. El rendimiento que presentaron como generadores de llaves de cifrado para imágenes fue adecuado al presentar valores satisfactorios en las pruebas. Los resultados demuestran también que la imagen encriptada aumenta su entropía casi a su límite máximo, sin aumentar excesivamente el tiempo de procesamiento y costo. Sin embargo, es necesario mencionar que se presentaron dos comportamientos atípicos. El primero fue el sistema cuadrático, que presenta pobres resultados en la prueba de entropía, y el segundo es el sistema logístico modificado, que no rindió satisfactoriamente en el análisis de la correlación de pixeles.

Para confirmar los resultados obtenidos, se podría continuar el estudio de estas llaves caóticas médiate otras herramientas. Por ejemplo, examinar su robustez al someterlas a ataques cibernéticos. También se podría modificar el

diseño del encriptador digital para procesar imágenes más complicadas, de mayor resolución o a color, las cuales presentan una estructura diferente a las compuestas por escala de grises. Asimismo, se podrían generar otras llaves caóticas empleando sistemas caóticos no contemplados en esta investigación, tales como: discretos de más de una dimensión y los de tiempo continúo sometidos a un proceso de discretización, buscando analizar la eficacia de las llaves cifradoras que puedan generar.

Derivado del proyecto se realizó un proyecto de titulación de licenciatura, donde se trabajó con las señales caóticas estudiadas para ser usadas como elementos centrales para generar llaves de encriptación de imágenes fijas.

El proyecto se terminó en su totalidad, aunque falta estudiar más señales caóticas discretas unidimensionales y de más variables. Aún más, se considera continuarlo con otros proyectos, que se someterán en el futuro inmediato.

REFERENCIAS (bibliografía)

[1] Broer Henk, Takens Floris, Dynamical Systems and Chaos, vol. 139. New York: Springer, 2009.

[2] L. Carlota and J. Manuel, “Cifrado De Imágenes Digitales Basado En Teoría Del Caos – Mapas Logísticos,” pp. 1–20, 2014

[3] I. Ivanov Bonev, La Teoría del caos, Primera. Buenos Aires: Rundinuskín, 1995.

[4] F. Almarza, “La Teoría del Caos. Modelo de interpretación epistémica e instrumento de solución: reconciliación entre ciencias y humanidades,” *Rev. Univ. Arte y Cult. Esc. Arte. Univ. Cent. Venez.*, vol. III, no. 14, pp. 107–150, 2002.

[5] A. Elisa and C. Ureta, “La creación de la metáfora ‘ el efecto mariposa ,’” *Comun. Libr.*, vol. 10, no. 6, pp. 66–73, 2014.

[6] Espinoza Illanes, Marcos, Cifrado de imágenes digitales basado en teoría del caos: mapas logísticos, Tesis maestría, pp. 1–20, 2014.

[7] Peitgen Heinz-Otto, Hartmut Jürgens Dietmar Saupe, Chaos and Fractals, Second. New York: Springer, 2004.

[8] Garcés Guzmán Héctor, Hinostroza Zubía Victor Manuel, Priscila Betsabe Hernández Valadez, Encriptador de imágenes en escala de grises con llaves caóticas, Pistas educativas, vol. no 40, noviembre 2018, pp. 478 – 489.

[9] Ives Crystal, “Human beings as chaotic systems,” Life Sci. Tehcnology, vol. 8, no. 2, pp. 1–7, 2004.Bonev Ivan Ivanov, La Teoría del caos, Primera. Buenos Aires: Rundinuskín, 1995.

[10] Donat Wolfram, Learn Raspberry Pi, Programming with Python, Primera ed. United Kingdom: Technology in action, 2005.

[11] Inzunza, Gonzalez Everardo, Encriptado caótico en sistemas biométricos, Tesis doctoral, Universidad Autónoma de Baja California, Ensenada, Baja California, 2012, pp. 59 – 60.

[12] Chen Guanrong, Mao Yaobin, Chui Charles K., A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons and Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[13] Gao, T. G. y Chen, Z. Q, A new image encryption algorithm based on hyper chaos. Physics Letters A, 372(4): 394–400, 2008.

[14] Isabelle Steven. H., A Signal Processing Framework for the Analysis and Application of Chaotic Systems, Ph.D. Dissertation, Massachusetts Institute of Technology (MIT), Cambridge, MA, May 1995

[15] Rodríguez-Orozco Eduardo, García-Guerrero Enrique Efrén, Inzunza-Gonzalez Everardo, López-Bonilla Oscar Roberto, Flores-Vergara Abraham, Cárdenas-Valdez Jose Ricardo Tlelo-Cuautle Esteban, FPGA-based Chaotic Cryptosystem by Using Voice Recognition as Access Key, Electronics, www.mdpi.com/journal/electronics, 2018.

[16] Smart Nigel Paul, Cryptography: An Introduction, New York: McGraw Hills, 2010.

[17] Stewart Ian, Historia de las matemáticas en los últimos 10000 años. España: Crítica, 2007.

ANEXOS

****Nota: El reporte técnico tendrá una extensión mínima de 20 cuartillas y máxima de 30, a espacio y medio.**
CONSIDERACIONES:

- Los reportes deben estar escritos en español o en inglés.
- Se debe entregar en formato Word acorde a este formato.
- El texto debe ser escrito en hoja tamaño carta a espacio y medio, y los márgenes deberán encontrase al menos a una pulgada (2.54 cm). La totalidad del texto debe escribirse en minúsculas, utilizando las mayúsculas sólo al principio de las oraciones y para los títulos de capítulos.
- Se recomienda usar el tipo de letra Arial tamaño 10, o Times new Roman tamaño 12.
- Todas las páginas deben estar numeradas en secuencia comenzando desde la portada.
- La extensión total del texto es de un mínimo de 20 cuartillas y un máximo de 30 cuartillas, con un interlineado de espacio y medio.
- Archivos de Excel de tablas y gráficas deben ser adjuntados al reporte enviado electrónicamente.
- Las figuras, fotografías y tablas, serán insertadas en el cuerpo del texto y numeradas en forma consecutiva comenzando con 1 y de manera independiente de las tablas. El número y descripción de la figura, tabla, etc., deberá colocarse antes de la misma.
- Se recomienda evitar el uso de sombras y líneas punteadas que no permitan una legibilidad clara de imágenes.
- Las fórmulas y ecuaciones deben hacerse con un editor de ecuaciones como el que viene en Word. Estarán centradas y separadas del texto. La numeración será consecutiva comenzando con 1. El número de la fórmula deberá encerrarse entre paréntesis y colocarse a la derecha de la fórmula lo más cercano posible al margen derecho.
- Las referencias bibliográficas en el texto deben ser en cualquier estilo reconocido como APA, MLA, ISO, etc.
- Los anexos se colocarán al final del documento después de la bibliografía, utilizando caracteres alfabéticos para distinguirlos: Anexo A, Anexo B, etc. La información contenida en los anexos es importante pero no indispensable para la comprensión del trabajo. Se recomienda colocar en los anexos mapas, fotografías, tablas, desarrollos matemáticos, diagramas, etc.