UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

CRIPTOSISTEMA ESTEGANOGRÁFICO A TRAVÉS DE IMÁGENES DIGITALES PARA EL CIFRADO DE TEXTO USANDO TEORÍA DEL CAOS Y AUTÓMATAS CELULARES

Marlon Arias Cárdenas

Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá D.C.

2020

CRIPTOSISTEMA ESTEGANOGRÁFICO A TRAVÉS DE IMÁGENES DIGITALES PARA EL CIFRADO DE TEXTO USANDO TEORÍA DEL CAOS Y AUTÓMATAS CELULARES

Marlon Arias Cárdenas

Anteproyecto de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Directores:

Edilma Isabel Amaya Barrera

Magister en Ciencias Matemáticas

Luz Deicy Alvarado Nieto

Doctor en Ciencias de la Computación e Inteligencia Artificial

Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá D.C.

2020

Contenido

Índice de figuras

Índice de tablas

1. Introducción

Con el objetivo de construir sistemas de seguridad informáticos robustos y eficientes computacionalmente, a la vez que utilizan técnicas novedosas de ocultamiento y cifrado de datos aprovechando el desarrollo tecnológico y científico actual, muchos investigadores han propuesto alternativas a los algoritmos criptográficos y esteganográficos tradicionales que han mostrado ser superiores cuando se trata de procesar y compartir información en distintos formatos. Algunas propuestas involucran el uso de autómatas celulares bidimensionales que superan algunos de los algoritmos de detección de bordes clásicos (Mohammed y Nayak, 2014), la ocultación de información dentro de imágenes usando esteganografía con teoría del caos (Phadte y Dhanaraj, 2017), métodos esteganográficos híbridos que expanden el área de detección de bordes para incrementar la capacidad de incrustación de datos (Setiadi, 2019), técnicas esteganográficas en el dominio del espacio resistentes a ataques estadísticos que se basan en análisis morfológicos (Saha, Sengupta y Dasgupta, 2017), combinación de aritmética de alta precisión y atractores caóticos para la generación de secuencias cifrantes altamente aleatorias y la encriptación de imágenes (Flores et al., 2019) (Yaghouti y Moattar, 2019) y esteganografía sobre videos usando cadenas de ADN y combinación de algoritmos de cifrado y compresión (Kar, Mandal y Bhattacharya, 2018) (Cem y Elmasry, 2018) entre otros estudios.

El enfoque de este trabajo está orientado a la aplicación de sistemas no lineales con atractores caóticos, los cuales han presentado hasta la fecha resultados prometedores en el campo de la protección de datos, siendo una corriente relativamente nueva, junto a novedosas técnicas de esteganografía y marcas de agua (López, 2019) (Al-Fuqaha, Guizani, Mohammadi, Aledhari y Ayyash, 2015) (Keyvanpour y Merrikh-Bayat, 2011).

Tras una búsqueda de los desarrollos más recientes en el ámbito de la seguridad informática, se propone el diseño de un criptosistema esteganográfico aplicado al ocultamiento de mensajes de texto dentro de imágenes a color (o en blanco y negro). El mensaje de texto es encriptado mediante secuencias cifrantes generadas por un atractor caótico cuyas condiciones iniciales son la clave privada del sistema, para incrustarlo en la imagen a través de un algoritmo de detección de bordes con autómatas celulares y una técnica esteganográfica modificada para la selección de pixeles aleatorios sobre estos contornos, usando puntos del espacio de fases del atractor, de forma que respete los principios de confidencialidad, integridad y disponibilidad de la información durante el proceso comunicativo.

2. Planteamiento del problema

En las últimas décadas, los avances a escala exponencial en el desarrollo de tecnologías de la comunicación, el Internet y el nivel de procesamiento de los computadores de nueva generación han puesto a prueba la capacidad de ingenieros, matemáticos y científicos para diseñar e implementar sistemas robustos y escalables que permitan a las personas compartir información de forma segura y confidencial a través de canales desprotegidos (Al-Fuqahq et al., 2015). Además, con la masiva adopción del Internet de las Cosas (IoT por sus siglas en inglés), se estima que para finales del presente año existan más de doscientos mil millones de dispositivos electrónicos capaces de conectarse entre sí, intercambiando datos no estructurados en tiempo real (Al-Fuqahq et al., 2015).

Con el propósito de contribuir a la investigación y al desarrollo de nuevos sistemas de cifrado usando la esteganografía como complemento principal, en este trabajo se plantea el siguiente interrogante: ¿cómo aplicar la dinámica de sistemas no lineales aprovechando las propiedades del caos junto a la teoría de autómatas celulares y la esteganografía con el fin de proponer un sistema criptográfico para proteger la confidencialidad de mensajes de texto a través de imágenes a color, que cumpla con los modelos de seguridad y calidad aceptados internacionalmente por la comunidad científica?

3. Justificación de la investigación

El uso de la criptografía y la esteganografía permite a los usuarios asegurar la confidencialidad y la integridad de la información, frente a un gran número de ataques que pueden darse al momento de trasmitirla o almacenarla en equipos o servidores conectados a través de Internet o redes locales (empresas, hogares o sitios públicos entre otros). Para el año 2019, según la firma de seguridad Kaspersky, tan solo en Latinoamérica se presentaron en promedio 42 incidentes relacionados con software malicioso cada segundo, en donde los ciberdelincuentes se valen de mensajes falsos por correo electrónico, descargas de aplicaciones piratas y publicidad invasiva y engañosa para capturar información sensible de sus víctimas como datos de cuentas bancarias, correos empresariales o fotos y mensajes personales. De acuerdo con el informe sobre las tendencias de incidentes informáticos en la región de América Latina, en el periodo comprendido entre noviembre de 2018 y noviembre de 2019 se registraron cerca de cien millones de intentos de phishing (suplantación de identidad y promesas falsas) y más de mil trescientos millones de ataques con algún tipo de malware (AO Kaspersky Lab, 2019).

En Colombia se presentan aproximadamente treinta mil ataques de phishing al día, dado que el país es considerado uno de los tres mercados latinoamericanos más atractivos para los cibercriminales. Estos suelen enfocarse en proveedores de servicios, entidades bancarias y gubernamentales, hogares y empresas (Casa Editorial El Tiempo, 2019). Por estos motivos, existe la necesidad de diseñar e implementar algoritmos y protocolos que impidan el robo de datos con los que criminales y piratas informáticos puedan acceder a sistemas de información (servidores, bases de datos, cuentas de administrador) para cometer fraudes o suplantaciones.

Con el objetivo de diseñar sistemas de seguridad modernos que fortalezcan la confidencialidad y la integridad de las comunicaciones en un mundo interconectado y en constante avance tecnológico, han sido propuestos diversos enfoques (Hussain, Wahab, Idris, Ho y Jung, 2018). utilizando herramientas y modelos de criptografía y esteganografía los cuales se clasifican de la siguiente forma:

- Sistemas de Seguridad
    - Encubrimiento de las Comunicaciones
        - Esteganografía
            - Esteganografía Lingüística
            - Esteganografía Digital
        - Marcas de Agua
            - Marcas de Agua Robustas
            - Marcas de Agua Frágiles
    - Cifrado de la información
        - Criptografía
            - Criptografía de clave pública (cifrado asimétrico)
            - Criptografía de clave privada (cifrado simétrico)

Otra motivación para llevar a cabo este trabajo, es la de diseñar mecanismos de protección de datos que estén a la vanguardia frente a los continuos avances en el área de la matemática, las ciencias de la computación, la inteligencia artificial y el procesamiento cuántico, los cuales han tenido importantes aplicaciones en la criptografía y el criptoanálisis, así como en mecanismos de ocultamiento de la información en diferentes tipos de datos (imágenes, videos, archivos de sonido, textos) y métodos de estegoanálisis (Hussain et al., 2018).

El desarrollo de este proyecto, hace hincapié en la interdisciplinariedad y la transdiciplinariedad del ejercicio investigativo, articulando diferentes áreas del conocimiento relacionadas con la ingeniería de sistemas, lo que permite desarrollar un pensamiento sistémico e integral con el objetivo de eliminar los modelos mentales reduccionistas, enriqueciendo la formación profesional y la visión del mundo desde la base de una sociedad compleja con problemáticas complejas.

4. Objetivos

4.1 Objetivo general

Diseñar e implementar un criptosistema esteganográfico, a través de imágenes digitales para el cifrado de texto, que se ajuste a los estándares de seguridad propuestos en la literatura científica, mediante el uso de teoría del caos y autómatas celulares.

4.2 Objetivos específicos

- Establecer los atractores caóticos, cuyas propiedades posibiliten la aplicación de los mismos, en la encriptación de mensajes de texto.
- Identificar el comportamiento y las características de los autómatas celulares que puedan ser de utilidad, en la detección de bordes de una imagen, usada como elemento portador en un esquema esteganográfico.
- Escoger un atractor caótico cuyas características permitan usarlo como mecanismo de selección aleatoria de pixeles en los bordes de una imagen, para el ocultamiento de datos cifrados.
- Elegir una técnica esteganográfica idónea para ocultar datos cifrados en los pixeles elegidos de una imagen.
- Definir e implementar el proceso que permita recuperar un mensaje de texto original, preservando la integridad y confidencialidad de la información.
- Evaluar la viabilidad y efectividad del criptosistema esteganográfico propuesto, aplicando indicadores estándar de desempeño y calidad.

5. Estado del arte

En la literatura científica se plantean distintos diseños e implementaciones de criptosistemas que usan atractores caóticos, modelos desarrollados para detectar bordes en imágenes digitales utilizando diversas configuraciones de autómatas celulares, así como técnicas de esteganografía y marcas de agua para ocultar datos en diferentes formatos. Algunos de los trabajos que abordan estos temas, se presentan a continuación:

Inicialmente, en (Mohammed y Nayak, 2014) definen un conjunto de reglas lineales para autómatas celulares bidimensionales utilizado en la detección eficiente de bordes de una imagen. Dado que, la evolución de los autómatas celulares es de naturaleza paralela, obtienen la salida deseada dentro de un intervalo de tiempo unitario. Estudian cuatro de 512 reglas lineales de un autómata celular rectangular con condición de bordes adiabática o reflexiva que produce un resultado óptimo. Comparan los resultados con los algoritmos de detección de bordes convencionales y concluyen que los resultados de este trabajo muestran una mejoría respecto a los métodos de Canny, Robert, Sobel y Prewitt.

Por otra parte, en (Phadte y Dhanaraj, 2017), mediante la integración de esteganografía y criptografía, plantean un nuevo método para proporcionar seguridad en el intercambio de imágenes a color de 24 bits. Este modelo está basado en la técnica LSB (Least Significant Bit) que utilizan para ocultar una imagen en otra imagen. Encriptan la estegoimágen resultante utilizando teoría del caos. Los autores garantizan una mejora en la capacidad de ocultación de información, la seguridad sobre imágenes RGB y la recuperación sin pérdidas de los datos.

Adicionalmente, en (Setiadi, 2019) exponen un método esteganográfico híbrido de detección de bordes en los tres bits más significativos (MSB) de imágenes portadoras con el

objetivo de expandir el área del borde para aumentar la capacidad de incrustación de datos. Con esta técnica logran realizar la extracción del mensaje sin la necesidad de replicar la detección de bordes en la imagen portadora original. Con base en los resultados de las pruebas realizadas, concluyen que la capacidad de incrustación de mensajes se puede aumentar gracias a un área de borde más amplia ya que, con el mismo conjunto de datos, se obtiene un aumento promedio de 4350 a 12350 píxeles, manteniendo la calidad visual de la estegoimágen.

Sin embargo, cabe destacar que, en un gran número de estudios se utilizan diferentes ataques basados en análisis estadísticos para detectar posibles casos de esteganografía. A la luz de esto, en (Saha et al., 2017) presentan una metodología que muestra el desarrollo de una técnica esteganográfica en el dominio del espacio que es capaz de resistir tales ataques. Esto lo consiguen efectuando un análisis morfológico de diferentes regiones en la imagen para descubrir fragmentos contiguos de píxeles que constituyen regiones de alta entropía y son lo suficientemente grandes como para ajustarse al mensaje codificado. Si hay más de una de esas regiones presentes en la imagen, la que tenga la mayor cantidad de entropía se usa en la incrustación el mensaje usando la técnica LSB después de encriptarlo con un atractor caótico.

Usando un enfoque distinto, en (Flores et al., 2019) plantean un nuevo criptosistema caótico para el cifrado de imágenes digitales de alta resolución basado en el diseño de un generador de caos digital mediante el uso de la aritmética de alta precisión. La toman como una alternativa en la reducción de la degradación dinámica que presentan los modelos caóticos cuando se implementan en dispositivos digitales y para aumentar la seguridad de los sistemas criptográficos. Los resultados obtenidos muestran que las secuencias generadas proporcionan una alta aleatoriedad y confiabilidad durante un mayor número de iteraciones de las funciones caóticas implementadas, en comparación con las secuencias generadas mediante el uso de

precisión simple o doble precisión de acuerdo con el estándar IEEE 754. Como ventaja, frente a otros trabajos recientes, los autores obtienen un aumento exponencial en el espacio de claves equivalente a 2^{33268} o superior. Con el análisis de seguridad confirman que el criptosistema caótico propuesto es seguro y robusto contra varios ataques conocidos, pasando las pruebas estadísticas sugeridas por el NIST (National Institute of Standards and Technology) y el TestU01 (librería de software para realizar pruebas de aleatoriedad en generadores de números pseudo-aleatorios).

De forma similar, el atractor caótico de Chen es aplicado en (Yaghouti y Moattar, 2019) con el objetivo de producir números aleatorios usados en la creación de arreglos para la permutación de imágenes y la producción de secuencias cifrantes. Como resultado, descubren que la complejidad algorítmica disminuye. Cada uno de los componentes de color de la imagen se convierte en un vector unidimensional que se permuta utilizando las secuencias generadas al azar. La secuencia numérica creada pasa a ser una imagen caótica. Luego, la imagen permutada y la imagen caótica son divididas en bloques iguales. Codifican los bloques usando cadenas de ADN. Las reglas de codificación las eligen al azar con una función logística tridimensional. Este proceso les permite tener varias opciones para elegir las reglas de codificación. Finalmente, todos los bloques cifrados se combinan obteniendo la imagen encriptada. Los resultados experimentales muestran que el enfoque propuesto tiene un amplio espacio de claves y es resistente a diferentes ataques. Además, logran reducir la correlación entre los píxeles vecinos y la entropía es muy cercana a la ideal.

Por otro lado, en el estudio presentado en (Cem y Elmasry, 2018), combinan diferentes técnicas en el diseño de un nuevo sistema esteganográfico donde realizan una suma de verificación CRC-32 (código de detección de errores usado comúnmente en redes de

telecomunicaciones y dispositivos de almacenamiento para detectar cambios en los paquetes de datos) en el mensaje original, luego con Gzip lo comprimen antes de encriptarlo mediante AES (Advanced Encryption Standard), y lo incrustan en la imagen portadora. Utilizan el algoritmo Shuffle de Fisher-Yates seleccionando la ubicación de los píxeles. Para ocultar un byte, usan los bits menos significativos de los canales de color del píxel seleccionado. Los resultados indican que con el método propuesto mejoran la capacidad de incrustación de mensajes, la seguridad y la verificación de integridad. Además, muestran que altera en menor medida la calidad visual de la estegoimágen en comparación con otros métodos estudiados, y hace que el mensaje secreto sea más difícil de descubrir.

No obstante, en (Kumar, Singh y Kumar, 2019) proponen un método de esteganografía adaptativo basado en la identificación de bordes mediante lógica difusa, bajo la premisa de que las técnicas de detección convencionales existentes, como las de Canny o Sobel, no pueden garantizar el reconocimiento de las ubicaciones exactas de los bordes en las imágenes portadoras. El método que proponen es útil para estimar las áreas de forma precisa en una imagen portadora y con ello aseguran la ubicación exacta del borde después de incrustar el mensaje secreto. Con los resultados experimentales revelan que la técnica logra una buena imperceptibilidad en comparación con el método de Hayat Al-Dmour y Ahmed Al Ani llamado Edge XOR, en el dominio del espacio.

Adicionalmente, en (Kar et al., 2018) modelan un mecanismo basado en las propiedades del ADN para enviar datos ocultos dentro de un archivo de video. Inicialmente, fragmentan el archivo en frames. Seleccionan los frames aleatorios, y los datos se ocultan en estos, en ubicaciones al azar utilizando el método de sustitución LSB. Al analizar la arquitectura propuesta en términos de relación pico señal sobre ruido, así como el error cuadrático medio medido entre

los archivos originales y los esteganográficos, promediados en todos los cuadros logran obtener una degradación mínima del video esteganográfico.

Por último, en (Amrogowicz, Zhao, y Zhao, 2016) introducen un detector de bordes utilizando autómatas celulares totalistas exteriores. Comparan su rendimiento con otros detectores basados en el mismo concepto, además de algunos métodos clásicos, a través de pruebas de imágenes de un repositorio público. Con la medición visual y cuantitativa de la similitud con bordes correctos marcados manualmente confirman la superioridad del método propuesto sobre los detectores convencionales y de vanguardia basados en autómatas celulares.

Para abordar el interrogante propuesto en este trabajo y con base en los sistemas y técnicas planteadas en los artículos de referencia (Mohammed y Nayak, 2014), (Phadte y Dhanaraj, 2017) y (Setiadi, 2019), se propone utilizar un sistema dinámico caótico para generar una secuencia cifrante que permita encriptar un mensaje en texto plano. Posteriormente, utilizando autómatas celulares se efectuará un proceso de detección de bordes sobre una imagen RGB portadora y mediante el mismo sistema caótico usado en la encriptación del texto, se seleccionarán pixeles de los bordes de forma pseudo-aleatoria de manera que se pueda camuflar el mensaje cifrado en la imagen a través de técnicas esteganográficas modernas. Finalmente, se elegirán los criterios y estándares de seguridad y calidad correspondientes para verificar y validar el funcionamiento y la robustez de la aplicación.

6. Marco Teórico

Desde el surgimiento de las primeras civilizaciones, las personas han considerado como necesidad de primer orden la protección de la privacidad y la confidencialidad de la información que se comparte en ámbitos políticos, sociales y militares. Las primeras técnicas para lograr este objetivo se valían de instrumentos mecánicos los cuales permitían ocultar o cifrar mensajes que solo podían ser legibles a los ojos de un destinatario en particular. De allí surgió lo que actualmente se conoce con el nombre de criptografía, cuya definición es el estudio de técnicas de comunicación segura que permiten solo al emisor y receptor autorizados, visualizar el contenido de los mensajes compartidos sin que un tercero pueda interpretar su significado (Singh, 2002). De forma similar, a lo largo de la historia se conformó otra disciplina conocida como esteganografía la cual estudia técnicas de intercambio de mensajes secretos incrustados o "disfrazados" al interior de otro elemento llamado portador (Hussain et al., 2018).

Con el advenimiento de la segunda guerra mundial, comienza la era moderna de la criptografía. El proyecto ULTRA llevado a cabo en Bletchley Park por un grupo de científicos británicos entre los cuales se hallaba Alan Turing, tenía como objetivo encontrar la forma de desencriptar los mensajes enviados por el ejército alemán el cual tenía en su poder la máquina ENIGMA construida por el ingeniero electromecánico Arthur Scherbius y la máquina Lorenz SZ 40 que utilizaba circuitos de teletipo para aplicar cifrado de flujo a las comunicaciones militares de alto nivel (López, 2019). A esto se suman los trabajos de Claude Shannon y John Von Newmann quienes sentaron las bases de la teoría de la información y la computación (Shannon, 1948) (Shannon, 1949) (von Neumann, 1993). Desde ese momento, se ha podido evidenciar un crecimiento vertiginoso en los recursos dedicados a la investigación y desarrollo en la

criptografía y la esteganografía que actualmente se sitúan en el marco de las ciencias de la computación y las telecomunicaciones (Singh, 2002).

Cabe resaltar que la principal diferencia entre estas dos disciplinas consiste en que la criptografía se ocupa de la protección del contenido de la información que se transmite bajo condiciones de riesgo e inseguridad, mientras que la esteganografía trata de ocultar la propia existencia de los mensajes con el fin de no levantar sospechas de terceros que quieran interceptar la comunicación entre dos o más partes (Singh, 2002). Este planteamiento intenta mostrar que un mensaje encriptado no es necesariamente invisible, luego independientemente del criptosistema que se use, el hecho de que un tercero identifique la existencia del criptograma es la base para un intento de criptoanálisis o de búsqueda de vulnerabilidades en los protocolos o algoritmos que se manejen (López, 2019). Por ello, se considera que la combinación de esteganografía y criptografía puede ser la clave a la hora de diseñar un sistema confiable para la protección de la información transmitida en canales y dispositivos analógicos y/o digitales (López, 2019).

6.1 Criptografía

Antes de la invención de los computadores y los dispositivos electromecánicos que hacen parte de la cotidianidad, la criptografía consistía en algoritmos relativamente sencillos que sustituían los caracteres de un mensaje o los transponían entre sí y los más sofisticados eran los que involucraban ambos procedimientos. Ahora los criptosistemas son más complejos debido al avance en ciencia y tecnología, pero los principios generales se mantienen, ya que muchos sistemas de cifrado todavía combinan técnicas de sustitución y transposición (Maiorano, 2009), la diferencia radica en que, en el ámbito de la informática y las máquinas de cómputo, no se manipulan caracteres sino secuencias de dígitos binarios (bits).

Las técnicas criptográficas convencionales que han surgido desde la construcción de los primeros computadores incluyen procedimientos basados en transposición y superposición, sistemas electro-mecánicos basados en rotores (la máquina ENIGMA y los dispositivos SIGABA y PURPLE son algunos ejemplos) (López, 2019), redes de Feistel empleadas en criptosistemas de cifrado por bloques como DES (Data Encryption Standard), Lucifer, FEAL (Fast Data Encipherment Algorithm), CAST y Blowfish entre otros (Guo, 2019), algoritmos AES e IDEA (International Data Encryption Algorithm), generadores de secuencias pseudo-aleatorias que usan álgebra modular, registros de desplazamiento retro-alimentados, cifrados simétricos y asimétricos, criptografía de curva elíptica, algoritmos RSA (Rivest, Shamir y Adleman), RC4 (Rivest Cipher 4) y de Diffie-Hellman y más recientemente criptografía usando cadenas de ADN (Yaghouti y Moattar, 2019), computación celular con membranas, autómatas celulares, teoría del caos y procesamiento computacional cuántico (Savchuk y Fesenko, 2019).

Otras aplicaciones de las técnicas criptográficas modernas, además de mantener la confidencialidad de la información, son las funciones hash o sumas de comprobación y las firmas digitales que corresponden a mecanismos de seguridad cuya función es permitir la verificación de la integridad y la autoría de los datos (documentos) compartidos en la red (Maiorano, 2019).

6.2 Sistemas Dinámicos y Teoría del Caos

La presencia de comportamiento caótico en sistemas dinámicos fue descubierta, en parte, gracias al desarrollo de los computadores y la informática. En 1961, el meteorólogo Edward Lorenz intentaba predecir el comportamiento del clima, para ello, necesitaba resolver numéricamente un conjunto de ecuaciones que modelaban el movimiento de partículas en la

atmósfera y se dio cuenta de que cada vez que ejecutaba su programa en el computador, obtenía resultados diferentes como solución al sistema de ecuaciones. Lo que ocurría era que su programa trabajaba con seis cifras decimales de precisión, mientras que él introducía como condición inicial sólo tres. Las tres últimas eran introducidas aleatoriamente por el computador en cada ejecución. Aunque Lorenz conocía esto, no pensaba que una variación de milésimas en las condiciones iniciales fuera a importar mucho en el resultado final. Fue así como se descubrió que el sistema de Lorenz tenía sensibilidad a la variación de las condiciones iniciales, lo que a su vez provocaba la evolución temporal imprevisible y caótica (Metzger, 1998).

Desde los tiempos de Isaac Newton, los científicos disponen de una teoría matemática capaz de predecir el comportamiento de un gran número de sistemas físicos. Conociendo su configuración inicial y aplicando una serie de reglas (leyes de la física), su comportamiento está totalmente determinado en un instante posterior. La teoría del caos advierte que, en algunos sistemas físicos, la evolución temporal es de carácter complejo y depende en gran medida de las condiciones iniciales hasta el punto de que no se pueda predecir con seguridad su evolución después de un lapso de tiempo específico (Metzger, 1998).

La teoría del caos se enmarca dentro del estudio de los sistemas dinámicos. Estos se definen a partir del conjunto de sus posibles configuraciones. Una vez se conoce el espacio de fases el cual se quiere estudiar, se necesita una ley que explique la evolución de éste. A partir de aquí se diferencian los sistemas dinámicos discretos de los continuos (Gómez, s.f.).

Un sistema dinámico discreto se define así: dado $X \subset \mathbb{R}^n$ un conjunto no vacío y

$$f : X \to X \tag{1}$$

una función que relaciona estados mediante la expresión

$$X_{k+1} = f(X_k) \tag{2}$$

La pareja (f, X) es un sistema dinámico y el conjunto X es llamado espacio de fases.

La ley que define la evolución, relaciona los puntos del espacio de fases de manera discreta. Si el sistema empieza en una configuración X_0, tras k pasos se encontrará en el estado $f_k(X_0)$, donde X_0 es la condición inicial y el conjunto $\{X_0, f(X_0), f_2(X_0), \dots\}$ es la órbita de X_0.

Un sistema dinámico continuo se define así: dado $X \subset \mathbb{R}^n$ un conjunto no vacío y

$$\nu : X \rightarrow X \tag{3}$$

un campo vectorial que relaciona los estados nuevos del sistema mediante la ecuación diferencial

$$\frac{dy}{dx} = \nu(x(t)) \tag{4}$$

La pareja (ν, X) es un sistema dinámico y el conjunto X es llamado espacio de fases.

6.3 Tipos de Atractores

En teoría de sistemas dinámicos, así como en la física, un atractor es un conjunto de valores numéricos hacia los cuales un sistema tiende a evolucionar, para una gran variedad de condiciones iniciales. La trayectoria que adopta el sistema a lo largo del tiempo y que pasa lo suficientemente cerca del atractor, permanece en su órbita aun cuando existan ligeras perturbaciones. Si el conjunto de ecuaciones que describe el comportamiento de éste se modela en dos o tres dimensiones, el atractor puede ser representado gráficamente. En general, un atractor de un sistema dinámico puede ser un punto, un conjunto finito de puntos, una curva, una variedad topológica o un conjunto de puntos con estructura fractal conocido como atractor extraño (Martens y Nowicki, 2003).

Los sistemas dinámicos pueden estudiarse a partir los de sistemas disipativos, ya que, en estos, sin la intervención de una fuerza externa que contrarreste la pérdida de energía, la evolución del sistema se detendría (esto puede ser causado, entre otras razones, por la fricción interna, pérdidas termodinámicas o pérdidas de material) (Valverde y Le Lay, 1980). La disipación energética y la fuerza externa tienden a equilibrarse, estableciendo en el sistema su comportamiento típico. El subconjunto del espacio de fases del sistema dinámico correspondiente al comportamiento típico es el atractor, también conocido como la sección de atracción.

Hasta la década de 1960, se pensaba que los atractores eran simples subconjuntos geométricos del espacio de fases, como puntos, líneas, superficies y regiones simples del espacio tridimensional (Milnor, 2006). Los atractores más complejos que no se pueden clasificar como subconjuntos o combinaciones simples (por ejemplo, con las operaciones de intersección y/o unión) de objetos geométricos fundamentales (líneas, superficies, esferas y toroides entre otros), se enmarcan dentro de los atractores extraños.

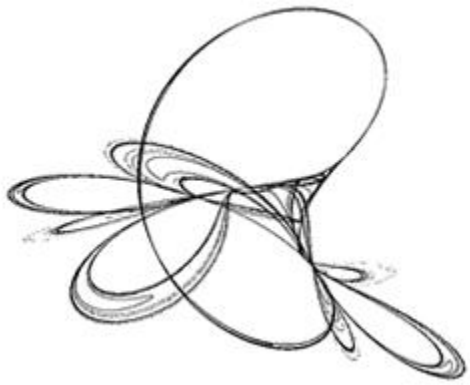
Existen diferentes tipos de atractores de acuerdo a la complejidad de sus estructuras (Strogatz, 1994):

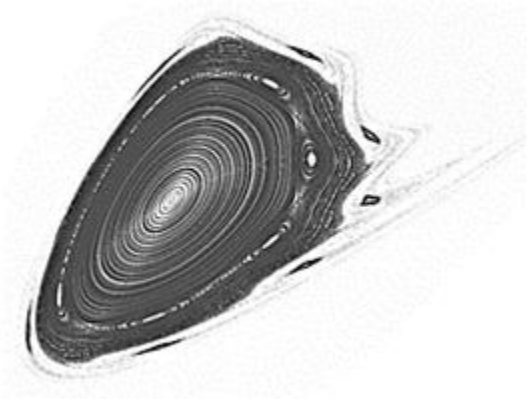
- De punto fijo: corresponde a un único punto al cual el sistema tiende a evolucionar hasta su estado final, como en el caso de la posición central inferior de un péndulo amortiguado o el fondo de un recipiente cóncavo que contiene una canica rodante.
- De finitos puntos: es un atractor que toma la forma de un conjunto finito de puntos que se visitan secuencialmente, en donde cada uno de estos puntos se llama punto periódico. El mapa logístico es un ejemplo en donde se presenta este tipo de estructura.

- De ciclo límite: corresponde a una órbita periódica en un sistema dinámico continuo que está aislado. Los ejemplos incluyen las oscilaciones de un reloj de péndulo (van Helden, 1995) y los latidos del corazón mientras el sujeto descansa.
- De límite toroidal: es el caso en donde hay más de una frecuencia en la trayectoria periódica del sistema a través del estado de un ciclo límite. Por ejemplo, en astrofísica, una frecuencia puede dictar la velocidad a la que un planeta orbita una estrella mientras que una segunda frecuencia describe las oscilaciones en la distancia entre los dos cuerpos. Si estas frecuencias forman un cociente irracional (es decir, son inconmensurables), la trayectoria ya no está cerrada y el ciclo límite se convierte en un atractor de límite toroidal.
- Atractores extraños: es el caso particular en el que el atractor posee una estructura fractal (dimensión no entera) (Strogatz, 1994). Suelen aparecer cuando la dinámica del sistema es caótica, aunque también existen atractores extraños no caóticos. Cuando un atractor extraño es caótico, exhibe una dependencia sensible de las condiciones iniciales y adicionalmente el sistema dinámico es localmente inestable pero globalmente estable. Una vez que la trayectoria del sistema ingresa en el atractor, las órbitas de los puntos consecutivos cercanos divergen entre sí pero nunca se apartan de éste (Grebogi, Ott, y Yorke, 1987).

El teorema de Poincaré-Bendixson muestra que un atractor extraño sólo puede presentarse en un sistema dinámico continuo de tres o más dimensiones (como en el caso del atractor de Lorenz). Sin embargo, tal restricción no se aplica a los sistemas discretos, los cuales pueden exhibir atractores extraños en dos o incluso una dimensión, como el sistema caótico de Tinkerbell o el mapa de Hénon (Milnor, 2006).

En las figuras 1 y 2 se presentan algunos ejemplos de atractores caóticos:

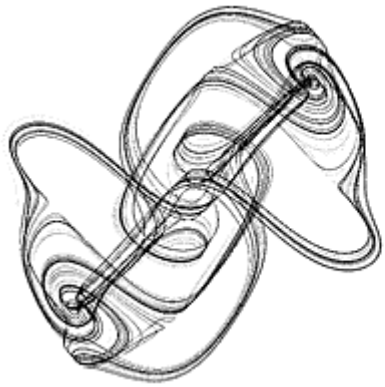


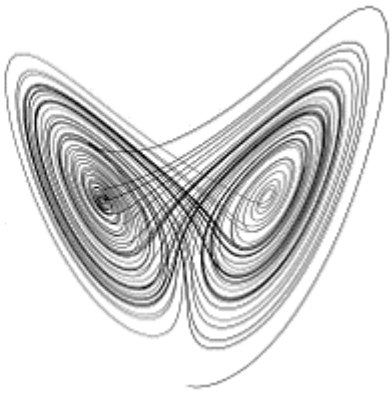


$$\begin{cases} x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} = 2x_n y_n + cx_n + dy_n \end{cases} \quad (5)$$

$$\begin{cases} x_{n+1} = x_n + y_{n+1} \\ y_{n+1} = y_n + \varepsilon x_n + kx_n(x_n - 1) + \mu x_n y_n \end{cases} \quad (6)$$

Figura 1. Sistemas caóticos discretos de Tinkerbell y Bogdanov respectivamente. Fuente: (Hirsch, Smale, y Devaney, 2004)





$$\begin{cases} \frac{dx}{dt} = \sin(y) - bx \\ \frac{dy}{dt} = \sin(z) - by \\ \frac{dz}{dt} = \sin(x) - bz \end{cases} \quad (7)$$

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(\rho - z) - y \\ \frac{dz}{dt} = xy - \beta z \end{cases} \quad (8)$$

Figura 2. Sistemas caóticos continuos de Thomas y Lorenz respectivamente. Fuente: (Hirsch et al., 2004)

6.4 Autómatas Celulares

Los autómatas celulares (AC) son sistemas computacionales discretos y abstractos que han demostrado ser útiles como modelos generales de complejidad, los cuales se pueden interpretar como sistemas dinámicos no lineales y tienen aplicación en una gran variedad de campos científicos. Los AC son, discretos espacial y temporalmente y están compuestos de un conjunto finito o numerable de unidades simples homogéneas llamadas células o celdas. En cada unidad de tiempo, las células adoptan uno de los estados definidos en un conjunto finito, evolucionando en paralelo, siguiendo funciones de actualización o reglas de transición dinámicas: la actualización del estado de una célula se logra teniendo en cuenta los estados de las células de su vecindario local (Berto y Tagliabue, 2017).

Los AC pueden calcular funciones y resolver problemas algorítmicos. A pesar de funcionar de una manera diferente a los sistemas basados en el concepto de máquina de Turing, con las reglas precisas, pueden emular una máquina de Turing universal y, por lo tanto, calcular, dada la tesis de Church-Turing, cualquier proceso computable (Weisstein, s.f.). Su principal característica radica en el comportamiento emergente complejo, comenzando por células simples siguiendo reglas locales elementales. Debido a esto, a partir de la década de 1950, los AC han atraído la atención de un número creciente de investigadores interesados en estudiar la formación y complejidad de patrones en un entorno puro y abstracto (Berto y Tagliabue, 2017).

La variedad de sistemas y modelos que se encuentran en la literatura sobre autómatas celulares es enorme y se puede generar prácticamente cualquier configuración desarrollada hasta el momento ajustando los cuatro parámetros que definen su estructura:

- Una cuadrícula de dimensión entera (n-dimensional) en donde se ubican las células. Aunque los componentes atómicos del sistema pueden tener formas diferentes, la importancia radica en la homogeneidad: todas las celdas son cualitativamente idénticas.
- Estados discretos. En cada paso de tiempo, las celdas pueden tener un solo estado.
- Interacciones locales. El comportamiento de cada celda depende solo de lo que sucede dentro de su vecindario local (que puede incluir o no a la propia celda).
- Dinámicas discretas. En cada paso de tiempo, las celdas actualizan su estado de acuerdo con una función de transición determinista.

La definición formal de los elementos que componen un AC se presenta a continuación (Straatman, Hagen, Power, Engelen y White, 2001):

$$A = (S, d, Q, N, \delta) \tag{9}$$

donde:

A = un autómata celular

S = el espacio de las celdas

d = la dimensión

Q = el conjunto de estados

N = el vecindario celular

δ = regla de transición de acuerdo al vecindario

Las características básicas de los autómatas celulares se centran en el establecimiento de una geometría que corresponda a la división del espacio del dominio en celdas de la misma forma (cuadros, polígonos, triángulos), dispuestos en una o varias dimensiones, de tal manera

que cada una de las reglas de evolución, al ser integradas dentro de un procesamiento, permiten el análisis y simulación del comportamiento de los estados del dominio (Weisstein, 2017).

De esta manera, durante las últimas décadas se han presentado importantes avances en las aplicaciones de los AC en diversos campos de la ciencia, en donde las reglas de transición pueden ser probabilísticas y tener en cuenta más de un paso de tiempo, ampliamente utilizados para representar la dinámica estocástica de los sistemas microfísicos. Otros ejemplos incluyen la actualización del estado de las celdas de forma asíncrona, diseño de la cuadricula para que contenga células no homogéneas siguiendo diferentes reglas de transición o conjuntos de estados infinitos (Berto y Tagliabue, 2017). En el campo de la criptografía, los AC han sido usados en la generación de secuencias de bits pseudo-aleatorias (Hernández, del Rey y Rodríguez 2002), encriptación de imágenes mediante mecanismos reversibles (Hernández, Hernández, Hoya, del Rey y Rodríguez, 2004) y sistemas de cifrado de llave publica (Martínez, s.f.), entre otras aplicaciones.

6.5 Esteganografía Digital y Marcas de Agua

Gracias a que los computadores y las redes de telecomunicaciones son cada vez más accesibles para el público en general, los enfoques creativos para almacenar, acceder y distribuir datos han generado muchos beneficios para la información multimedia digital, principalmente debido a propiedades como la transmisión sin distorsiones, el almacenamiento compacto, la fácil edición y por supuesto, la protección y disponibilidad de los archivos. A partir de esto, surge la esteganografía digital, que tiene como objetivo ocultar información en canales encubiertos y evitar la detección del mensaje que se quiera comunicar. Un caso particular es el de los sistemas esteganográficos digitales sobre imágenes, en donde el requisito fundamental es que la

estegoimágen sea perceptualmente indistinguible de la original para evitar levantar sospechas, es decir, la información oculta debe introducir un mínimo de modificaciones al objeto portador (Shih, 2017).

La esteganografía se puede dividir en dos tipos: lingüística y digital. Mientras que primero utiliza lenguaje natural escrito, la esteganografía digital, desarrollada con el advenimiento de los computadores, emplea archivos informáticos o datos multimedia digitales. Existen numerosos métodos y algoritmos que posibilitan el proceso esteganográfico de mensajes dentro de imágenes, archivos de audio y vídeo. A continuación, se describen algunos de ellos.

- Buscar y esconder: este algoritmo distribuye aleatoriamente el mensaje a través de la imagen. Utiliza una contraseña para generar una semilla al azar que luego se usa para elegir la primera posición (píxel). Se generan posiciones aleatoriamente hasta que se haya terminado de ocultar el mensaje. Este método presenta debilidades ya que al no verificar los píxeles en los que se incrustan los datos, podría haber áreas de mayor entropía en la imagen donde es más seguro alojar las partes del mensaje. Se usan técnicas de filtrado para encontrar estas zonas y mejorar la eficiencia y robustez del algoritmo al ser implementado (Umamaheswari, Sivasubramanian y Pandiarajan, 2010)
- Esteganografía en capas: mediante la esteganografía en capas se establece una relación lineal entre los elementos ocultos, en donde la codificación de la segunda palabra o letra de un mensaje depende de la primera (puede depender del último valor de la cifra, del último valor modificado, de la posición, etc.). Por lo que se establece un orden estricto de decodificación que impide obtener completamente el mensaje sin la primera parte, con lo cual únicamente se debe comunicar la clave para obtener esta parte y la pauta a seguir para encadenar los fragmentos (García, 2004).

- Ocultamiento a ciegas: esta es la forma más simple de ocultar información en una imagen. Comienza en la esquina superior de izquierda a derecha y de arriba a abajo píxel por píxel. A medida que se avanza, se cambian los bits menos significativos de los colores de los píxeles para que coincidan con el mensaje. Para recuperar el mensaje, se leen los bits menos significativos que comienzan en la parte superior izquierda. Este algoritmo es muy inseguro ya que resulta realmente fácil para cualquiera, leer los bits menos significativos en secuencia.
- Adición de ruido: además de modificar los bits necesarios para incrustar el mensaje en el objeto portador, se pueden modificar unos cuantos bits aleatorios del mensaje de forma que, si un posible atacante obtiene el archivo original, le será muy difícil descifrarlo si no conoce el sistema usado para la codificación.
- Ocultación en el bit menos significativo (LSB): este método es probablemente la forma más fácil de ocultar información en una imagen y, sin embargo, mantiene su eficacia. Funciona utilizando los bits menos significativos de cada píxel en una imagen portadora para ocultar los bits más significativos de un archivo que se desea incrustar (García, 2004). Los pasos que componen el algoritmo son: cargar tanto la imagen portadora como el archivo que se va a ocultar, elegir la cantidad de bits en los que desea ocultar el mensaje. Cuantos más se usen en la portadora, más se deteriorará. Posteriormente se crea la estegoimágen combinando los píxeles de la imagen con los del archivo. Si se decide, por ejemplo, usar 4 bits para la información que se quiere ocultar, quedarán cuatro bits para la portadora. Y finalmente, para recuperar los datos originales, solo se necesita saber cuántos bits se usaron para almacenar la imagen secreta. Se seleccionan los bits menos significativos según la secuencia de almacenamiento y se usan para crear una nueva

secuencia en donde los bits extraídos ahora se convierten en los bits más significativos (Umamaheswari et al., 2010).

Se pueden encontrar diversos soportes digitales para la ocultación de información, como por ejemplo archivos de imagen o sonido, videos, archivos ejecutables, páginas web, campos no usados de paquetes de redes (TCP/IP), espacio no utilizado en el disco duro, particiones ocultas o documentos HTML, XML, PDF, entre otros. En la figura 3 se muestra un esquema que explica la estructura general de un estegosistema:

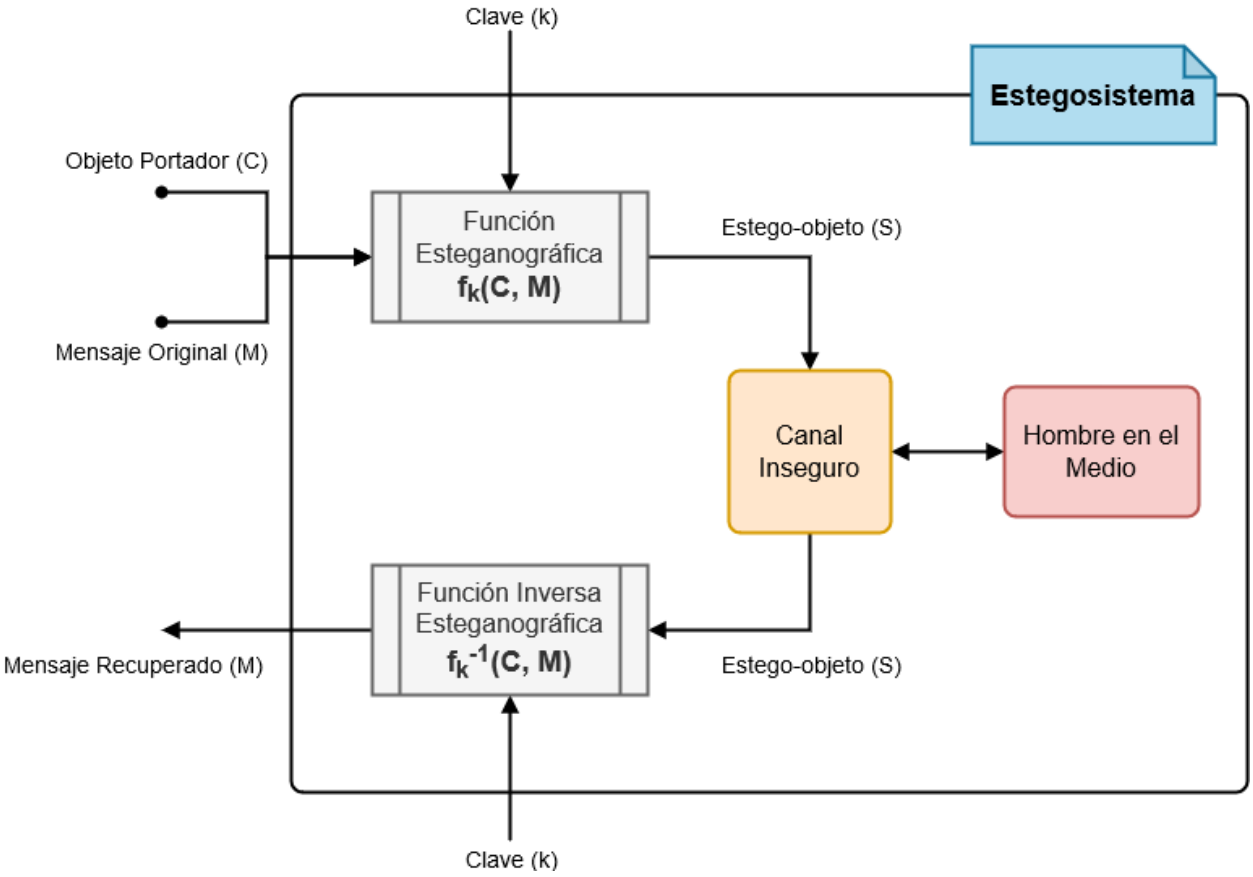


Figura 1.Estructura de un estegosistema . Fuente: elaboración propia

7. Alcances y Limitaciones

Con el desarrollo de este proyecto, se espera diseñar un criptosistema esteganográfico que se ejecute en un computador, con el objetivo de ocultar mensajes de texto en una imagen portadora seleccionados por el usuario. El proceso inverso se llevará a cabo en otro dispositivo de la misma naturaleza compartiendo la estegoimágen con el texto encriptado a través de correo electrónico u otro medio de comunicación apropiado.

Para la evaluación de los resultados, se harán las respectivas comparaciones de eficiencia algorítmica y seguridad respecto a los trabajos referenciados en este proyecto, usando métodos y pruebas propuestos por la comunidad científica, además, se ejecutarán sumas de verificación al inicio y al final del proceso de intercambio de información, con el objetivo de validar la integridad del mensaje usando un conjunto de funciones hash criptográficas. Así mismo, se utilizarán herramientas de desarrollo enfocadas en la computación científica.

Con respecto a las limitaciones de los resultados esperados, se destaca el hecho de que el formato de la imagen portadora deberá ser de compresión sin perdida para asegurar que los datos se mantengan sin alteraciones durante el envío (esto no implica que el archivo no pueda corromperse por otras razones), así mismo, es recomendable utilizar imágenes portadoras con numerosos cambios de contraste que impliquen la existencia de bordes, a fin de aumentar el espectro disponible para la ocultación de los datos. La resolución no tendrá un límite especifico, aunque se espera que entre mayor sea, más tiempo tome la ejecución del algoritmo. Por otra parte, la longitud del mensaje de texto podría verse limitada por la cantidad de memoria disponible para la generación de la secuencia cifrante usando el atractor caótico y por la cantidad de píxeles disponibles para su ocultamiento en la imagen portadora.

8. Metodología de la Investigación

En la figura 4 se muestran las etapas que componen el desarrollo de este proyecto:

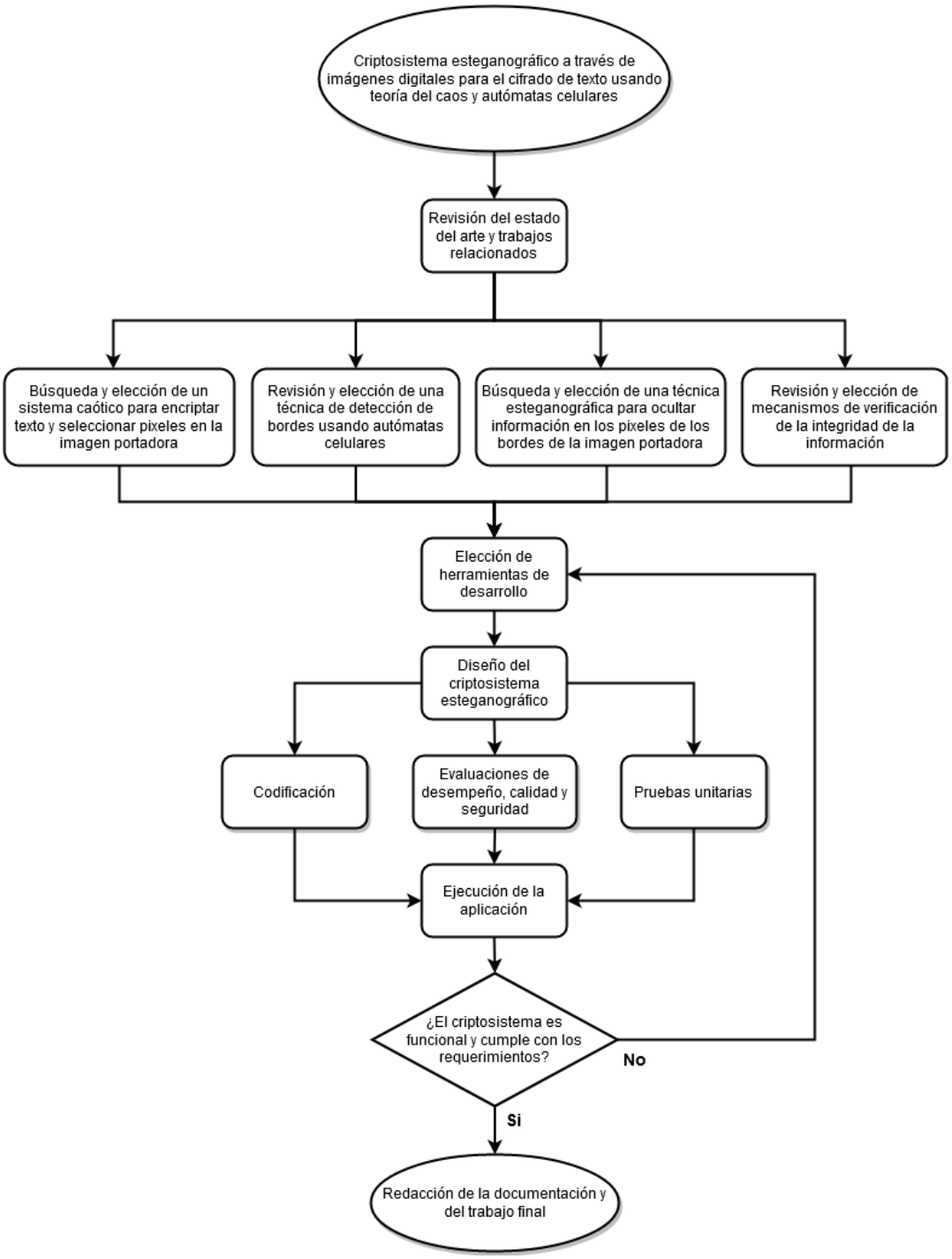


Figura 2. Diagrama de la metodología de la investigación. Fuente: elaboración propia

9. Cronograma de Actividades

El plan de actividades a seguir para este trabajo se muestra en la figura 5:

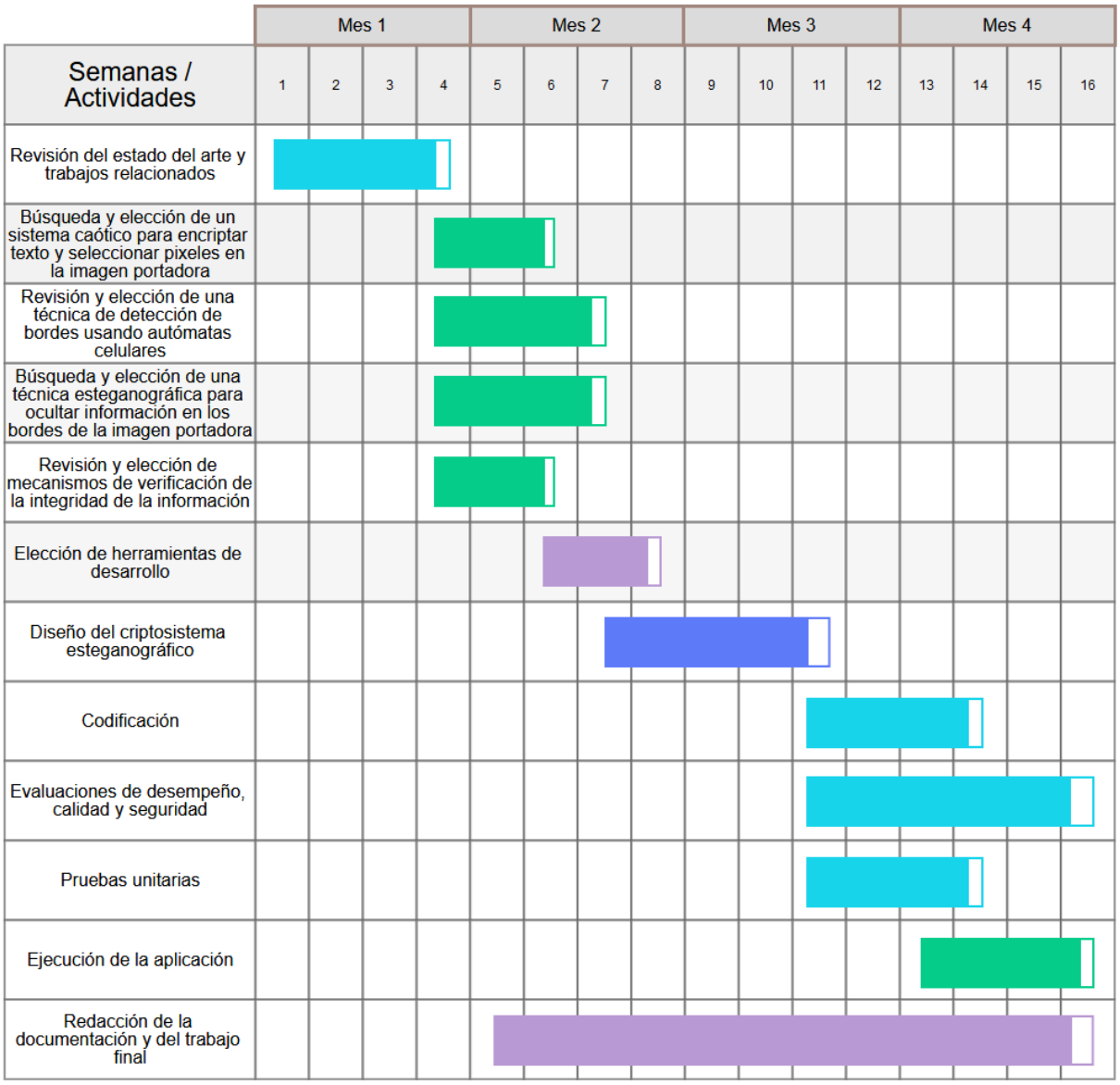


Figura 3. Cronograma de actividades. Fuente: elaboración propia

10. Recursos y Presupuesto

A continuación, se describe la función de los recursos humanos requeridos para la consecución del proyecto y los respectivos costos:

- Director de proyecto: tiene la responsabilidad de ayudar al estudiante a elegir el tema de la investigación, mostrarle cuáles deben ser los resultados que se esperan, plantear un programa de investigación coherente y con objetivos asumibles, monitorizar el progreso de la investigación y ofrecer asistencia técnica y ayuda en la resolución de problemas y en la búsqueda de información.
- Ingeniero de sistemas: es quien se encarga de diseñar, codificar, probar e implementar el criptosistema esteganográfico, basándose en la búsqueda y selección previa de herramientas conceptuales y tecnológicas examinadas en las etapas de revisión del estado del arte y planteamiento general del modelo, con la ayuda del director.
- Documentador: redacta toda la documentación del proyecto, tanto en la parte de desarrollo de software como en el proceso investigativo.
- Tester de software: tiene el papel de efectuar pruebas unitarias, de integración y de aceptación de forma paralela a los procesos de codificación e implementación.

Tabla 1. Costos correspondientes al talento humano. Fuente: elaboración propia

Rol	Número de personas	Salario mensual	Tiempo (semanas)	Total
Director de proyecto	2	$7.000.000	16	$28.000.000
Ingeniero de sistemas	1	$6.000.000	16	$24.000.000
Documentador	1	$3.500.000	12	$10.500.000
Tester de software	2	$3.800.000	6	$5.700.000

Los gastos generales se ven reflejados en la siguiente tabla:

Tabla 2. Costos generales del proyecto. Fuente: elaboración propia

Concepto	Descripción	Costo	Total
Equipos de computo	Alquiler de computadores con prestaciones que varían desde gama baja hasta gama alta	$350.000	$1.050.000
Papelería e impresiones	Impresión del documento del proyecto, diagramas, esferos y cuadernos entre otros	$400.000	$400.000
Transportes y gastos varios	Pasajes y alimentación	$1.300.000	$1.300.000

El presupuesto total del proyecto:

Tabla 3. Total de gastos. Fuente: elaboración propia

Concepto	Total
Salarios	$68.200.000
Gastos generales	$2.750.000
Total	$71.950.000

11. Referencias

Singh, S. (2002). The Code Book: The Secrets Behind Codebreaking. (1.a ed.). New York, Estados Unidos: Penguin Random House.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T. S. y Jung, K.-H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66. https://doi.org/10.1016/j.image.2018.03.012

López, M. J. (2019). Criptografía y Seguridad en Computadores. (5.a ed.). Jaén, España: Escuela Politécnica Superior de Jaén.

Shannon, C. E. (1948). A Mathematical Theory of Communication. The Bell System Technical Journal, 27, 379-423. Recuperado de http://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. The Bell System Technical Journal, 28(4), 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

von Neumann, J. (1993). First draft of a report on the EDVAC. IEEE Annals of the History of Computing, 15(4), 27-75. https://doi.org/10.1109/85.238389

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. y Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/comst.2015.2444095

Guo, C. (2019). Understanding the Related-Key Security of Feistel Ciphers From a Provable Perspective. IEEE Transactions on Information Theory, 65(8), 5260-5280. https://doi.org/10.1109/tit.2019.2903796

Yaghouti, A. y Moattar, M. H. (2019). Color image encryption based on hybrid chaotic system and DNA sequences. Multimedia Tools and Applications, 79(1-2), 1497-1518. https://doi.org/10.1007/s11042-019-08247-z

Savchuk, M. M. y Fesenko, A. V. (2019). Quantum Computing: Survey and Analysis. Cybernetics and Systems Analysis, 55(1), 10-21. https://doi.org/10.1007/s10559-019-00107-w

AO Kaspersky Lab. (s. f.). Press Releases & News. Pronostico de ciberseguridad para el 2020 en América Latina. Recuperado 20 de mayo de 2020, de https://latam.kaspersky.com/about/press-releases/2019_kaspersky-ofrece-pronostico-de-ciberseguridad-2020-para-america-latina

Casa Editorial El Tiempo. (2019, noviembre 20). El cibercrimen no descansa, estas son las proyecciones para el 2020. Recuperado 20 de mayo de 2020, de https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508

Mohammed, J. y Nayak, D. R. (2014). An efficient edge detection technique by two dimensional rectangular cellular automata. International Conference on Information Communication and Embedded Systems (ICICES2014), 1-4. https://doi.org/10.1109/icices.2014.7033847

Phadte, R. S. y Dhanaraj, R. (2017). Enhanced blend of image steganography and cryptography. 2017 International Conference on Computing Methodologies and Communication (ICCMC), 230-235. https://doi.org/10.1109/iccmc.2017.8282682

Setiadi, D. R. I. M. (2019). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. Journal of King Saud University - Computer and Information Sciences, 1-11. https://doi.org/10.1016/j.jksuci.2019.12.007

Saha, T., Sengupta, S. y Dasgupta, T. (2017). Chaotic cipher based spatial domain steganography with strong resistance against statistical attacks. 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), 365-370. https://doi.org/10.1109/icrcicn.2017.8234536

Flores, A., García, E. E., Inzunza, E., López, O. R., Rodríguez-, E., Cárdenas, J. R., y Tlelo, E. (2019). Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. Nonlinear Dynamics, 96(1), 497-516. https://doi.org/10.1007/s11071-019-04802-3

Cem, M., y Elmasry, W. (2018). New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. Sādhanā, 43(5), 68. https://doi.org/10.1007/s12046-018-0848-4

Kumar, S., Singh, A., y Kumar, M. (2019). Information hiding with adaptive steganography based on novel fuzzy edge identification. Defence Technology, 15(2), 162-169. https://doi.org/10.1016/j.dt.2018.08.003

Kar, N., Mandal, K., y Bhattacharya, B. (2018). Improved chaos-based video steganography using DNA alphabets. ICT Express, 4(1), 6-13. https://doi.org/10.1016/j.icte.2018.01.003

Amrogowicz, S., Zhao, Y., y Zhao, Y. (2016). An edge detection method using outer Totalistic Cellular Automata. Neurocomputing, 214, 643-653. https://doi.org/10.1016/j.neucom.2016.05.092

Maiorano, A. (2009). CRIPTOGRAFÍA, Técnicas de Desarrollo para Profesionales (Spanish Edition) (1.a ed.). Ciudad de México, México: Alfaomega Grupo Editor (MX).

Metzger, R. J. (1998). El Atractor de Lorenz Geométrico. Revista del Instituto de Investigación de la Facultad de Ciencias Matemáticas de la U.N.M.S.M, 1(1), 82-90. https://doi.org/10.15381/pes.v1i1.8879

Gómez, J. J. (s. f.). Introducción a la Teoría del Caos (1.a ed.). Recuperado de http://ciencia-en-red.fisimur.org/fisica/Caos2.pdf

Keyvanpour, M. R., y Merrikh-Bayat, F. (2011). An Effective chaos-based image watermarking scheme using fractal coding. Procedia Computer Science, 3, 89-95. https://doi.org/10.1016/j.procs.2010.12.016

Martens, M., y Nowicki, T. J. (2003). Ergodic theory of one-dimensional dynamics. IBM Journal of Research and Development, 47(1), 67-76. https://doi.org/10.1147/rd.471.0067

Milnor, J. (2006). Attractor. Scholarpedia, 1(11), 1815. https://doi.org/10.4249/scholarpedia.1815

van Helden, A. (1995). The Galileo Project | Science | Pendulum Clock. Recuperado 20 de mayo de 2020, de http://galileo.rice.edu/sci/instruments/pendulum.html

Grebogi, C., Ott, E., y Yorke, J. A. (1987). Chaos, Strange Attractors, and Fractal Basin Boundaries in Nonlinear Dynamics. Science, 238(4827), 632-638. https://doi.org/10.1126/science.238.4827.632

Berto, F., y Tagliabue, J. (2017, agosto 22). Stanford Encyclopedia of Philosophy. Cellular Automata. Recuperado 20 de mayo de 2020, de https://plato.stanford.edu/entries/cellular-automata/

Weisstein, E. W. (s. f.). Cellular Automaton. Recuperado 20 de mayo de 2020, de https://mathworld.wolfram.com/CellularAutomaton.html

Shih, F. Y. (2017). Digital Watermarking and Steganography: fundamentals and techniques (2.a ed.). https://doi.org/10.1201/9781315121109

García, D. (2004). Análisis de Herramientas Esteganográficas [tesis de pregrado, Universidad Carlos III de Madrid]. Repositorio Institucional UC3M. https://e-archivo.uc3m.es/bitstream/handle/10016/7119/PFC_David_Garcia_Cano_2004_201033204919.pdf?sequence=1&isAllowed=y

Umamaheswari, M., Sivasubramanian, S., y Pandiarajan, S. (2010). Analysis of Different Steganographic Algorithms for Secured Data Hiding. IJCSNS International Journal of Computer Science and Network Security, 10(8), 1-7. Recuperado de http://paper.ijcsns.org/07_book/201008/20100825.pdf

Strogatz, S. H. (1994). Nonlinear Dynamics And Chaos: With Applications To Physics, Biology, Chemistry And Engineering (Studies in Nonlinearity) (1.a ed.). New York, Estados Unidos: CRC Press.

Hirsch, M. W., Smale, S., & Devaney, R. L. (2004). Differential Equations, Dynamical Systems, and an Introduction to Chaos (2.a ed., Vol. 1). Elsevier Gezondheidszorg.

Velarde, M. G., y Le Lay, V. F. (1980). Estructuras disipativas - Algunas nociones básicas. El Basilisco, 10, 8-13. Recuperado de http://www.fgbueno.es/bas/bas110.htm

Straatman, B., Hagen, A., Power, C., Engelen, G., y White, R. (2001). The Use of Cellular Automata for Spatial Modelling and Decision Support in Coastal Zones and Estuaria. Land Water Milieu Informatie Technologie, 1, 1-203. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.8949&rep=rep1&type=pdf

Hernández, L., del Rey, A., y Rodríguez, G. (2002). Aplicaciones de los autómatas celulares a la generación de bits. Boletín de la Sociedad Española de Matemática Aplicada, 21, 65-87. Recuperado de https://digital.csic.es/bitstream/10261/21270/1/ACgenbits.pdf

Hernández, L., Hernández, A., Hoya, S., del Rey, A., y Rodríguez, G. (2004). Cifrado de imágenes usando autómatas celulares con memoria. Recuperado de https://digital.csic.es/bitstream/10261/21257/1/Novatica2004.pdf

Martínez, J. M. Cifrado y Descifrado de Patrones usando Autómatas Celulares Reversibles [tesis de maestría, Instituto Politécnico Nacional]. Recuperado 20 de mayo de 2020, de https://pdfs.semanticscholar.org/bee8/d47f73b77caa5f34f72384fe37510ced45a4.pdf