UNIVERSIDAD AUTÓNOMA METROPOLITANA

AZCAPOTZALCO

Casa abierta al tiempo

División de Ciencias Básica e Ingeniería

Licenciatura en Ingeniería en Computación

PROYECTO TECNOLOGICO

COMPARTICIÓN DE IMÁGENES USANDO ESTEGANOGRAFÍA Y AUTÓMATAS CELULARES

ELABORADO POR:

SASHA GONZÁLEZ MARTÍNEZ

208305375

Trimestre 2014 Primavera

Julio de 2014

Asesor: Germán Téllez Castillo

Profesor Asociado

Departamento de Sistemas

CBI | INGENIERÍA EN COMPUTACIÓN

COMPARTICIÓN DE IMÁGENES USANDO ESTEGANOGRAFÍA Y AUTÓMATAS CELULARES

ALUMNA | SASHA GONZÁLEZ MARTÍNEZ

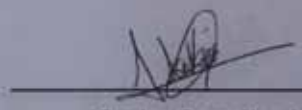
MATRÍCULA | 208305375

ASESOR| GERMÁN TÉLLEZ CASTILLO

Yo, GERMÁN TÉLLEZ CASTILLO, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

M. en C. Germán Téllez Castillo

Yo, SASHA GONZALEZ MARTINEZ doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Sasha González Martínez

Agradecimientos

A mi familia.

Dedicada con un profundo agradecimiento y admiración a mi madre, por todo el apoyo, sobre todo por la confianza y libertad que me dio para decidir mí camino.

A mis hermanas y hermano que siempre me apoyaron a lo largo de toda la carrera.

A mi asesor.

Un agradecimiento singular debo al profesor M. en C. Germán Téllez Castillo que como asesor de este proyecto me ha orientado, apoyado y corregido en mi labor con un interés y una entrega que ha sobrepasado, con mucho todas las expectativas que como alumna, deposité en su persona.

Todo este trabajo ha sido posible gracias a ellos.

Resumen

En este proyecto terminal se presenta un nuevo criptosistema gráfico para cifrar imágenes basadas en autómatas celulares reversibles con memoria.

Su principal característica es que las imágenes original y cifrada están definidas por la misma paleta de colores y que la imagen recuperada es idéntica a la imagen original, es decir, no hay pérdida de resolución ni de definición en todo el protocolo, al contrario de lo que ocurre en la mayor parte de los criptosistemas gráficos presentados hasta la fecha.

Contenido

Tabla de imágenes.

CAPÍTULO I. PROYECTO

Antecedentes.

Cifrar la información es de vital importancia para salvaguardar y mantener la confidencialidad, integridad y viabilidad de la información, así como minimizar la vulnerabilidad del sistema y la información contenida en él. En este proyecto se obtiene un sistema que basado en autómatas celulares nos permita cifrar imágenes mediante esteganografía.

Las técnicas para compartir imágenes secretas han atraído la atención en los últimos años [1-4]. Sin embargo existen problemas con estas técnicas; la primera de ellas es una pérdida intencional o accidental de la imagen, que puede ocurrir si sólo se accede a una parte de los datos. El segundo problema es, además de mantener a los adversarios alejados del contenido de la imagen, es el que la imagen pueda ser transferida a dichos adversarios.

Los autómatas celulares son sistemas dinámicos en donde el espacio, el tiempo y el conjunto de valores que ocupa son discretos. Los autómatas celulares son herramientas de modelación para sistemas complejos. El autómata celular genera su dinámica en una retícula en donde cada localidad de la retícula se le llama célula; cada célula toma un valor de un conjunto finito de valores llamados estados; existe una función de evolución que asigna a cada célula un estado tomando en cuenta el valor que tiene la célula y los valores que tienen sus células vecinas. La función de evolución es una función estocástica.

La esteganografía es una técnica que permite entregar mensajes camuflados dentro de un objeto contenedor, de forma que no se detecte su presencia y pasen inadvertidos; se ha empleado a lo largo de la historia y en particular durante la II Guerra Mundial.

La autenticación es el proceso de detectar y comprobar la identidad de una entidad de seguridad mediante el examen de las credenciales del usuario y la validación de las mismas consultando a una autoridad determinada. La información obtenida durante la autenticación puede ser utilizada directamente por el código.

En el diseño de criptosistemas se han usado frecuentemente sistemas dinámicos. No obstante, no han sido muchos los protocolos basados en sistemas dinámicos que se han propuesto específicamente para el cifrado de imágenes. El principal problema que presentan es que son difíciles de implementar computacionalmente debido a la diferencia entre la aritmética definida por el sistema dinámico usado y la aritmética discreta de la computadora. Además, la imagen descifrada suele presentar una pérdida de resolución que, aunque la hace reconocible, no es exactamente igual a la original. Recientemente se ha propuesto el uso de autómatas celulares en protocolos criptográficos para imágenes, cuya principal característica es que se recupera la imagen original sin pérdida alguna de resolución.

Objetivos generales.

Diseñar e implementar un algoritmo basado en autómatas celulares que permitan cifrar una imagen bmp usando esteganografía.

Objetivos particulares.

- Diseñar un autómata celular reversible.
- Crear una llave publica y una privada.
- Implementar en lenguaje Java el algoritmo diseñado.
- Diseñar e implementar una interfaz gráfica para el algoritmo anteriormente diseñado.

Justificación.

En este sistema se usa una imagen bmp y no una JPEG debido a que en el proceso de codificación de una imagen JPEG no es reversible es decir que no se puede recuperar después del descifrado; ya que en la imagen JPEG hay pérdida de bits.

Dado que se cifrará una imagen digital la cuál es un ente discreto se usa en este proyecto terminal un autómata celular el cuál es una herramienta discreta; una ventaja de esto, es que el diseño de un autómata celular así como sus reglas de evolución no es muy complejo. Esto es, las reglas de evolución que rigen la dinámica de un autómata celular pueden ser expresadas por un conjunto de funciones matemáticas discretas; esta característica se utilizará para discretizar el proceso de cifrado de la imagen. Otra ventaja de usar autómatas celulares para llevar a cabo este proyecto terminal es que se pueden expresar dinámicas complejas con un conjunto de ecuaciones simples.

En este proyecto terminal diseñamos un algoritmo que basado en autómatas celulares nos permite evitar la distorsión a la imagen original. Empleando un autómata celular obtenemos resultados comparables con los algoritmo de cifrado por desplazamiento.

CAPÍTULO II. MARCO TEÓRICO

Autómatas celulares.

El desarrollo de los autómatas celulares AC, comenzó alrededor de 1943 cuando JOHN VON NEUMANN empezó a considerar la posibilidad de generación de vida artificial, tratando de que un autómata se copiara a sí mismo. Bajo sugerencia de su colega STANISLAW MARCIM ULAM, VON NEUMANN utilizó patrones sobre una cuadrícula en el plano, las cuales evolucionan según una regla de transformación fija. De esta forma el problema de auto reproducción mecánica, quedaba reducido a la búsqueda de ciertas configuraciones que, con la aplicación de una regla de evolución , dieran lugar a copias idénticas.

Muchos AC interesantes han surgido desde entonces; algunos como juegos de computadora, que gracias a las facilidades computacionales y a las diversas TESELACIONES del plano, es posible aplicar reglas locales que dan lugar a vistosos cambios en las configuraciones; tal es el caso del llamado Juego de la Vida presentado por el matemático británico JOHN HORTON CONWAY, en la columna MATHEMATICAL GAMES de SCIENTIFIC AMERICAN, en octubre de 1970.

EDWARD FREDKIN en 1960, formuló el concepto de mecánica de la información, en analogía con la mecánica cuántica. Su formulación se basa en el supuesto de que el mundo físico proporciona constantemente información y puede, por consiguiente, modelarse como un gran AC de tres dimensiones. En 1965, JOHN HOLLAND utilizó AC para resolver problemas de adaptación y optimización. HEDLUND (1969) y RICHARDSON (1972) estudian los AC como sistemas dinámicos de corrimiento. Actualmente los AC se están aplicando a diferentes áreas del conocimiento: física, biología, química, matemáticas y ciencias de la computación, entre otros.

Un representante en la actualidad del estudio de los AC es Stephen Wolfram quien ha realizado investigaciones sobre el comportamiento cualitativo de los A.C. en una dimensión, con dos o tres estados, sobre configuraciones periódicas que se presentan en el A.C. Wolfram observó sus evoluciones para configuraciones iniciales aleatorias.

Así, dada una regla, el A.C. exhibe diferentes comportamientos para diferentes condiciones iniciales. Al observar estos diferentes comportamientos estableció una clasificación para los AC de una dimensión. Las clases son:

a) Clase I. La evolución lleva a una configuración estable y homogénea, es decir, todas las células terminan por llegar al mismo valor.

b) Clase II. La evolución lleva a un conjunto de estructuras simples que son estables o periódicas.

c) Clase III. La evolución lleva a un patrón caótico.

d) Clase IV. La evolución lleva a estructuras aisladas que muestran un comportamiento complejo (es decir, ni caótico, ni ordenado), este suele ser el tipo de comportamiento más interesante que un sistema dinámico puede presentar. La figura 1, muestra ejemplos de las cuatro clases.

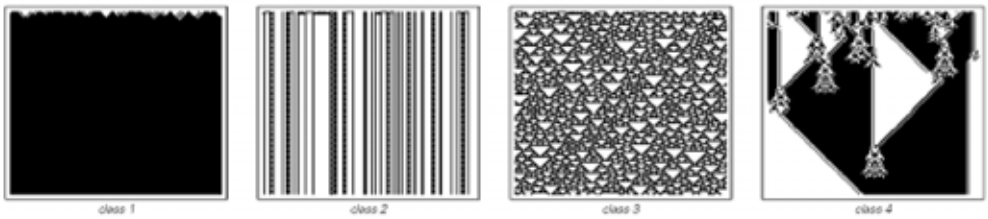


Figura 1. Ejemplos de las clases de los AC según Stephen Wolfram. De izquierda a derecha se observan las clasificaciones I a IV.

Descripción de un autómata celular.

Un AC consta de los siguientes elementos:

- Un enrejado, retícula, arreglo ó lattice regular de celdas o células.
- A cada celda se le asigna un valor, llamado estado; el conjunto de estados es finito.
- Cada celda tiene un conjunto finito de celdas vecinas, llamada vecindad de la célula. La relación de vecindad es uniforme.
- Una función de transición que es discreta y temporal y que indica cuál será el estado de una celda en el instante *t+1,* con base en su estado y los estados de su vecindad en el tiempo *t*. La función es la misma para todas las celdas.

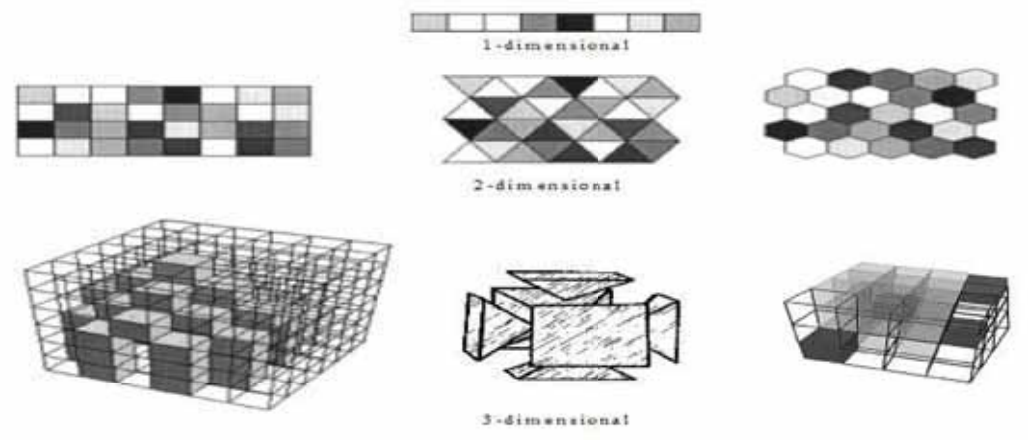
Conceptos.

Definición 1. Una retícula (o una lattice), es un arreglo regular de elementos de dimensión $d \in Z^{+}$; los elementos del lattice son llamados celdas o células. A cada célula se le asigna un valor de una familia de conjuntos finitos llamados conjuntos de estados. Ver figura 2.

Definición 2. Un lattice *L*, es homogéneo si todas sus celdas toman su valor a partir del mismo conjunto *S*.

Definición 3. Sea *L* un lattice homogéneo y $(r \epsilon L)$ una célula, el estado *de r* es un elemento $(s \epsilon S)$, esto es. $r \leftarrow s$.

La figura 2, muestra diferentes tipo de lattices.



El tiempo avanza en etapas discretas y la dinámica está dada por una regla explícita llamada función local. La función local es usada en cada etapa de tiempo sobre cada célula para determinar su nuevo estado a partir del estado actual de ciertas células, llamadas la vecindad de la célula, es decir, la función local toma los estados de la vecindad de la célula como argumento y devuelve como resultado el nuevo estado de la célula correspondiente. Las células cambian sus estados en etapas de tiempo discreto de acuerdo a la función local. Estos cambios de estado de las células podrían o no realizarse de forma sincronizada para todas las células del lattice, dependiendo de la naturaleza del problema que se modele. Si el lattice es homogéneo todas las células operan bajo la misma función local. *Observación:* La definición 1 implica que una lattice puede ser infinita, sin embargo, implementar esto en un programa de computadora es imposible, por esta razón, las lattices se consideran compuestas por un número finito de células, y se implementan siguiendo algunas condiciones de frontera, a saber:

Frontera periódica. Es una frontera en donde los bordes opuestos de una lattice se consideran conectados. Para una lattice de una dimensión, la frontera periódica permite visualizar geométricamente al lattice en dos dimensiones como una circunferencia.

Frontera abierta. Es una frontera en donde fuera de ella el lattice se considera que existen células con un valor fijo tomado de S.

Frontera reflectora. Es una frontera en donde los valores de las células en la frontera del lattice se consideran reflejados fuera de esta.

Sin frontera. Es una lattice que comienza con algún tamaño finito y que crece dinámicamente conforme se va requiriendo.

Definición 4. Sea L una lattice y sea $r \epsilon L$ una célula. Una vecindad de tamaño $n \epsilon Z^+$ para r, es un conjunto finito de células $N(r)= \{k_1,..., k_n\} \subset L$ tal que $r=k_j$ para algún j, si $r \epsilon N(r)$ o para ningún j en caso contrario.

Definición 5. Un Autómata Celular, AC es una TUPLA *(L, S, N, f)* donde:

1. L es una lattice de dimensión d, con $d \epsilon Z^+$. En el caso de una lattice finita, esta consiste de k células, y se le implementa con cierta condición de frontera.

2. S = {0, 1, 2,..., k-1} es un conjunto finito de estados.

3. N es un conjunto de vecindades definido por:

N = {N(r): $r \epsilon L$ es una célula y $N(r)$ es la vecindad de r de tamaño $n \epsilon Z^+ \ \forall r \epsilon L$}

4. $f: S^n \rightarrow S$ es una función llamada función de transición o función local. Esta función se aplica en cada paso de tiempo discreto sobre las células de L, tomando como argumentos los estados de las células de $N(r)$, y regresando como resultado el nuevo valor de r para el siguiente paso del tiempo.

Definición 6. Un AC A = (L, S, N, f) se dice que es homogéneo si y solamente si:

1. L es homogénea

2. f se aplica a cada paso discreto de tiempo sobre todas las células de L por igual

Si al menos se cumple 1, se dice que A es un AC de lattice homogénea. Al conjunto de estados de todas las células del AC se le conoce como configuración del AC.

Definición 7. Sea A = (L, S, N, f) un AC. Una configuración de A es una función $T_t: L \rightarrow S$ que asocia a cada célula del lattice L en el tiempo t, un estado de S. Dada una configuración, asignarle nuevos estados a todas las células para generar una nueva configuración, a través de la función de transición del AC, se conoce como función global.

Definición 8. Sea A = (L, S, N, f) un AC. La función global es una función $F: L \rightarrow L$ que se aplica evaluando F sobre cada una de las células del conjunto de células del AC en el tiempo t, es decir, sobre una configuración T_t del AC en el tiempo t, y regresa nuevos valores para todas las células del AC, es decir, se pasa de la configuración T_t de A, a la configuración T_{t+1} de A, del tiempo t al $t + 1$.[5]

Autómata celular reversible.

Así como la teoría general de autómatas celulares se han tenido tres etapas importantes, en el caso de los reversibles, análogamente, se tienen tres épocas importantes:

La primera se presenta en los años 60's destacando en principio el trabajo de Edward F. Moor y las ideas del Jardín del Edén. Desde un enfoque de dinámica simbólica y topología Gustav A. Hedlund, en 1969, contribuye a la teoría de los autómatas celulares reversibles con un estudio que ha sido piedra angular dentro del campo. Hedlund logra un análisis muy detallado y profundo de las propiedades de los autómatas celulares reversibles destacando dos conceptos importantes; *Multiplicidad Uniforme* e *Indices de Welch* .

La segunda etapa importante la podemos encontrar a finales de los 70's gracias al trabajo de Serafino Amoroso y Yale N. Patt, los cuales dieron un primer algoritmo para detectar cuando un autómata celular lineal es reversible. Masakasu Nasu, retoma los resultados de Hedlund y les da un nuevo enfoque utilizando teoría de gráficas, en especial, dos herramientas: el diagrama de de Bruijn y las gráficas *Bundle* también llamadas diagramas de Welch.

Más reciente se tiene el trabajo de Jarkko Kari. El hace uso implícito de los análisis hechos por Hedlund y Nasu ofreciendo una nueva perspectiva acerca de las causas que hacen que un autómata celular lineal sea reversible y de las propiedades que en estos se presentan.

De lo anterior podemos destacar que los autómatas celulares lineales reversibles han seguido un proceso de estudio intenso a pesar del corto tiempo de desarrollo que se tiene de esta teoría en comparación con otras. En este proceso se han retomado trabajos anteriores para enriquecerlos y darles un nuevo enfoque como sucede con Nasu y Kari, o simplemente se ha vuelto a rehacer parte del estudio como es el caso de Amoroso y Patt con respecto al trabajo de Hedlund.

El conjunto de estados de todas las células en el instante *t* se denomina configuración en el instante *t* y se representa por el vector $C^{(t)}= (a_0^{(t)},\ldots,a_{n-1}^{(t)})\epsilon S^n$. En particular, $C^{(0)}$ es la configuración inicial. Si denotamos por C al conjunto de todas las configuraciones posibles del AC, se denomina función de transición global del AC a la transformación lineal Φ: $C \rightarrow C$, $C^{(t)} \rightarrow C^{(t+1)}$,que asigna a cada configuración su evolución en el tiempo. Si Φ es biyectiva entonces existe otro autómata celular, llamado inverso, cuya función global es Φ^{-1}. Cuando existe este AC inverso, se dice que el autómata celular es reversible y su evolución hacia atrás en el tiempo es posible. Se puede considerar que esta evolución también depende del estado de otras células en instantes de tiempo anteriores: t-1, t-2, etc.

En el ámbito de nuestro estudio, un autómata celular se dirá reversible si para cada posible configuración la regla de evolución especifica uno y sólo un único sucesor. Esto es, dada una regla de evolución podemos construir una nueva con la cual podamos volver a generar las configuraciones que se habían producido anteriormente, ver figura 3.

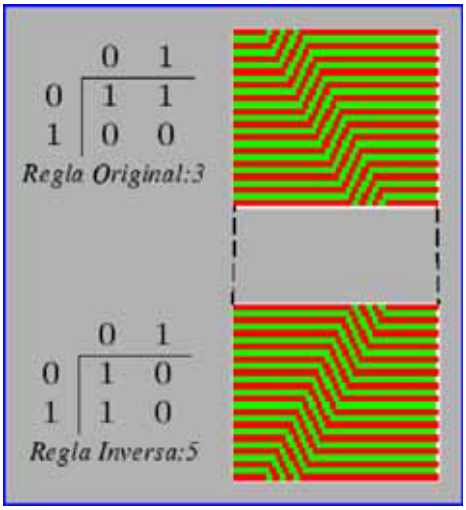


Figura 3: **Autómata ($2,\frac{1}{2}$) reversible, cuya regla original es 3 y regla inversa 5. De una configuración inicial, evoluciona a una configuración dada tal que aplicando la regla inversa se pueda retornar a la configuración original**

Propiedades de los Autómatas Celulares Lineales Reversibles

El problema de reversibilidad en autómatas celulares se puede plantear como un análisis del mapeo que existe del conjunto de configuraciones globales del autómata a si mismo. Si dicho mapeo es biyectivo entonces la evolución del autómata es reversible, ver figura 4.

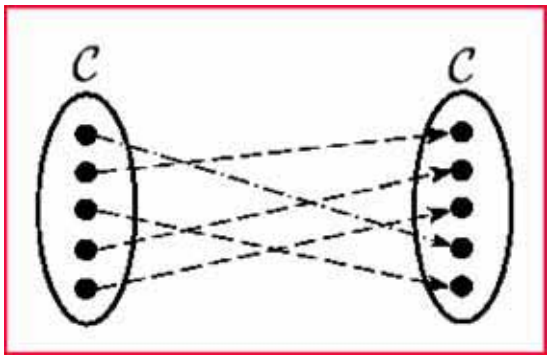


Figura 4: El mapeo biyectivo entre configuraciones globales define un autómata celular reversible

Hay que hacer notar que desde el punto de vista de comportamiento local no se puede hablar de autómatas reversibles, ya que la regla de evolución mapea un conjunto de vecindades a un conjunto de estados, esto es; $\Phi : K^{2r+1} \rightarrow K$, el cual es evidente que no es un mapeo biyectivo para $r > 0$; sin embargo, el interés por este tipo de sistemas es que la dinámica de los mismos depende de las reglas de comportamiento local no reversibles las cuales inducen un comportamiento global que si es reversible.

La cuestión a investigar es de que forma el funcionamiento del autómata es capaz de conservar la información del sistema para que en un momento dado podamos hacer uso de la información y poder reconstruir las configuraciones

globales anteriores; con esta idea se pueden establecer dos propiedades importantes que deben tener estos sistemas:

- En un autómata celular reversible no existe Jardín del Edén.
- Cada configuración global tiene una única configuración de la cual precede [6].

Modelo de cifrado de imágenes usando Autómatas Celulares.

Sea I una imagen definida por n = r×s ≥ 128 pixeles y una paleta de c colores. Dicha imagen puede ser representada como una matriz, M, de orden n = r×s, con coeficientes en Z_c, donde $c = 2^b$ y b = 1, 8, 24, para imágenes en blanco y negro, escala de grises y en color, respectivamente. El coeficiente (i, j) de la matriz M representa el color que posee el pixel (i, j) de la imagen I. Esta representación matricial da lugar, si concatenamos las sucesivas filas de la matriz M, a una secuencia de n enteros $P = (p_0,...,p_{n-1})$, que denominaremos representación secuencial de la imagen I.

El criptosistema propuesto consta de tres módulos.

En el primer modulo (modulo de instalación) se construye un autómata celular reversible y las evoluciones del autómata celular son usadas para producidor la imagen Stego[1].
Las evoluciones del autómata celular inverso serán usadas para recuperar la imagen original es decir la imagen sin el mensaje oculto. De este modo al insertar la función local de autómata celular reversible se podrá recuperar la imagen original. El usuario (D) crea un conjunto de llaves públicas y privadas que después serán usadas para adicionarle una firma a los datos con el propósito de la autenticación.

En el segundo modulo (modulo de inserción) el usuario produce una imagen STEGO insertando los datos obtenidos en las fases previas. La inserción es de tal forma que, primero la calidad visual de los resultados será buena y segundo será difícil reconocer cualquier dato en la imagen STEGO.

Finalmente, en el tercer modulo (modulo de recuperación y verificación) en este modulo se recuperará la imagen con el mensaje oculto. Usando la clave generada por la llave pública y privada.

Modelo para construir el autómata celular reversible

- Sea r = 1, radio de la vecindad simétrica del autómata celular
- Selecciona un número aleatorio w_s
- $0<w_s<2^3$
- Construir la regla de evolución

$$a_j^{(t+1)} = (f_{ws}(v_j^T) + f_{ws+1}(v_j^{(t-1)}) + a_j^T) \pmod 2$$

donde $0 \leq j \leq 7$

[1] Imagen que resulta del proceso esteganográfico

CAPÍTULO III. DESARROLLO DEL PROYECTO.

Modelo.

El módulo de instalación:
Se implementarón las siguientes etapas para construir el autómata celular reversible:
1.- Se genera un conjunto de llaves públicas y privadas (PUD, PRD) respectivamente.
2.-Se construye un autómata celular reversible (m):
a) Selecciona el radio (r) de la vecindad del autómata, donde r= 1.
b) Selecciona un número aleatorio entre 0 y 2^{2r+1}; el cual llamaremos el número de la regla de evolución del autómata celular.
c) Teniendo el radio de la vecindad del autómata y el número de la regla de evolución del autómata se construye el autómata celular reversible (m).

En nuestro esquema consideramos un byte por cada píxel, por lo que el número de células en cada configuración de (m) es 8 y esto porque supondremos que r está entre uno y tres.

Módulo de inserción:
Insertamos en cada imagen los siguientes datos:

- Una secuencia única de números asignados a cada participante para asegurar un orden consecutivo de los participantes en la fase de recuperación.
- El número de la regla del autómata celular y el radio de la vecindad, para reconstruir el autómata celular (m).
- Las formas firmadas para cada participante.
- La cadena de autenticación correspondiente al participante para el propósito de autenticación.

Modulo de recuperación y verificación.
El procedimiento para recuperar la imagen se llevará a cabo de la siguiente manera:
1) Con la secuencia de números, el número de la regla del autómata celular, el radio y la cadena de autenticación de cada participante:
Se verificará si la secuencia de números es consecutiva.
2) Se puede verificar la información dada por el mismo participante de la siguiente forma:
PUD de P = PUD de P;
donde PUD = llave pública de usuario y P es el participante.

La entrada principal de la aplicación serán imágenes en formato bmp, sin importar si es a color o blanco y negro. La salida de la aplicación será la imagen que estará cifrada es decir la que contenga el mensaje oculto. Las dimensiones de la imagen bmp serán 1000x1000.

CAPÍTULO IV. SIMULACIÓN Y RESULTADOS.

En este capítulo se presentan una serie de simulaciones que nos permite mostrar que se alcanzaron los objetivos del proyecto.

En el sistema diseñado e implementado en este proyecto se debe ingresar una imagen bmp con dimensiones 1000 x 1000 pixeles como máximo, al cifrar la imagen no se muestra ningún cambio en la imagen ya que en eso se basa este proyecto en que al cifrar la imagen mediante esteganografía no se vea cambio entre la imagen original y la imagen Stego.
En la figura 5 se muestra la interfaz gráfica del sistema desarrollado.

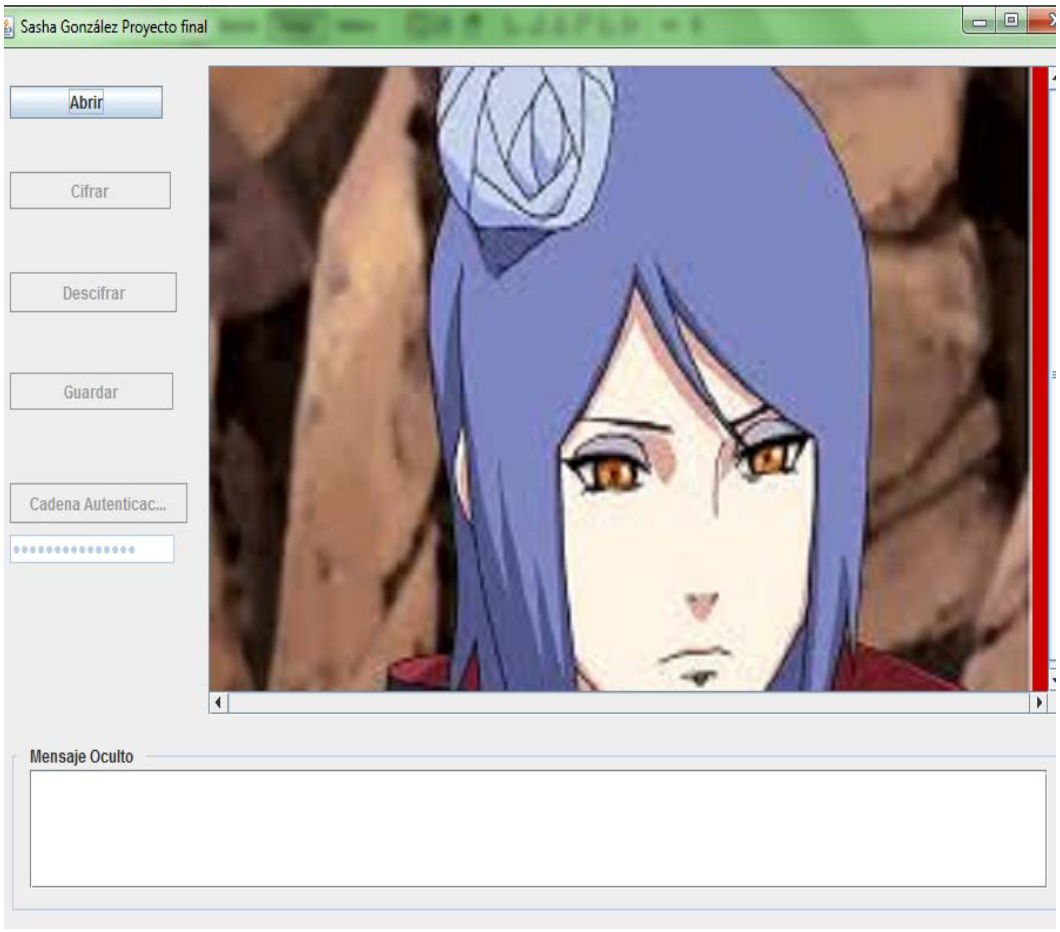


Figura 5. Interfaz del sistema

En la figura seis se muestra como con el boton abrir se elige la imagen a cifrar el programa solo acepta imágenes bmp.

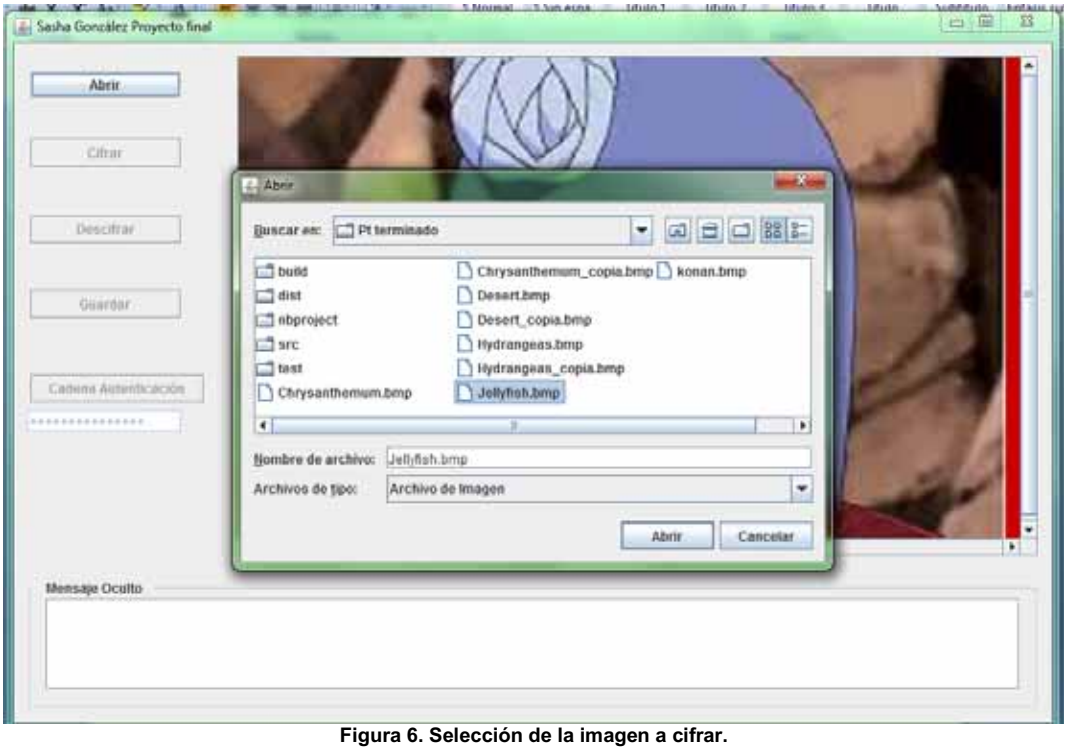


Figura 6. Selección de la imagen a cifrar.

La figura siete nos muestra que al elegir la imagen en formato bmp se activan los botones de cifrar y cadena de autenticación.

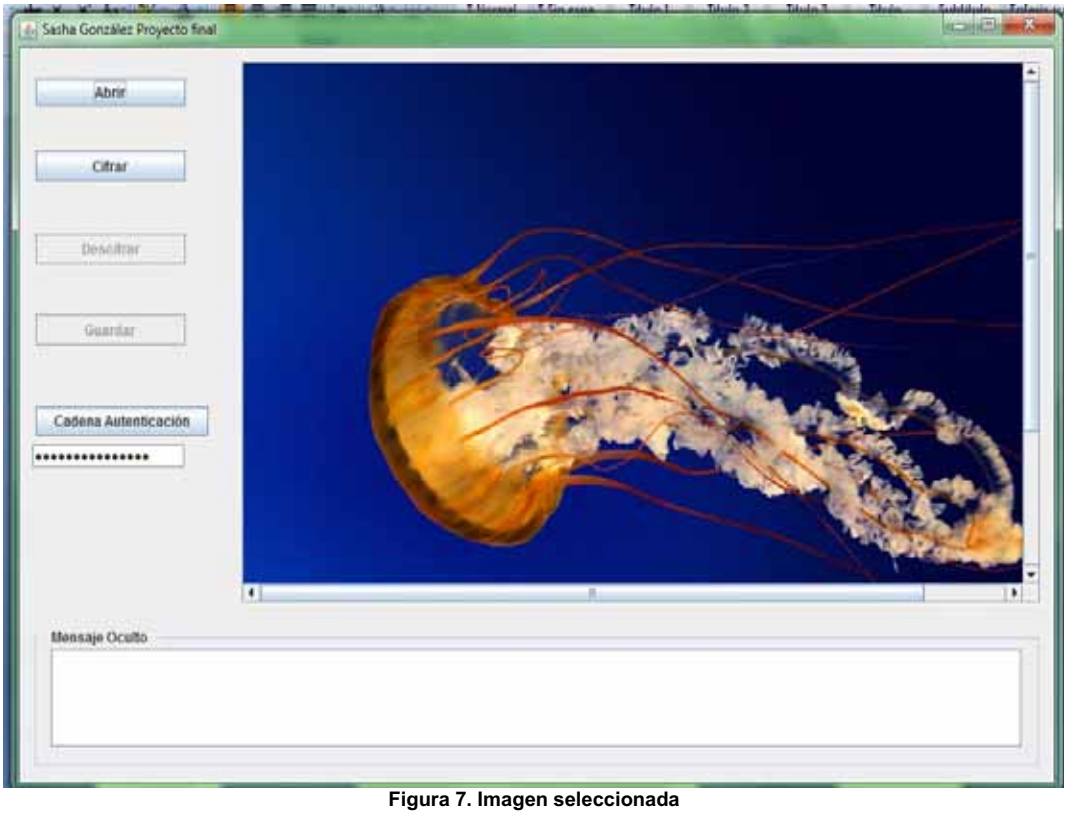


Figura 7. Imagen seleccionada

El siguiente paso es poner el mensaje que se quiera ocultar, como se muestra en la figura 8. Al presionar el botón cifrar se muestra un mensaje notificando que el mensaje se oculto exitosamente. Nótese que el botón guardar se activo.

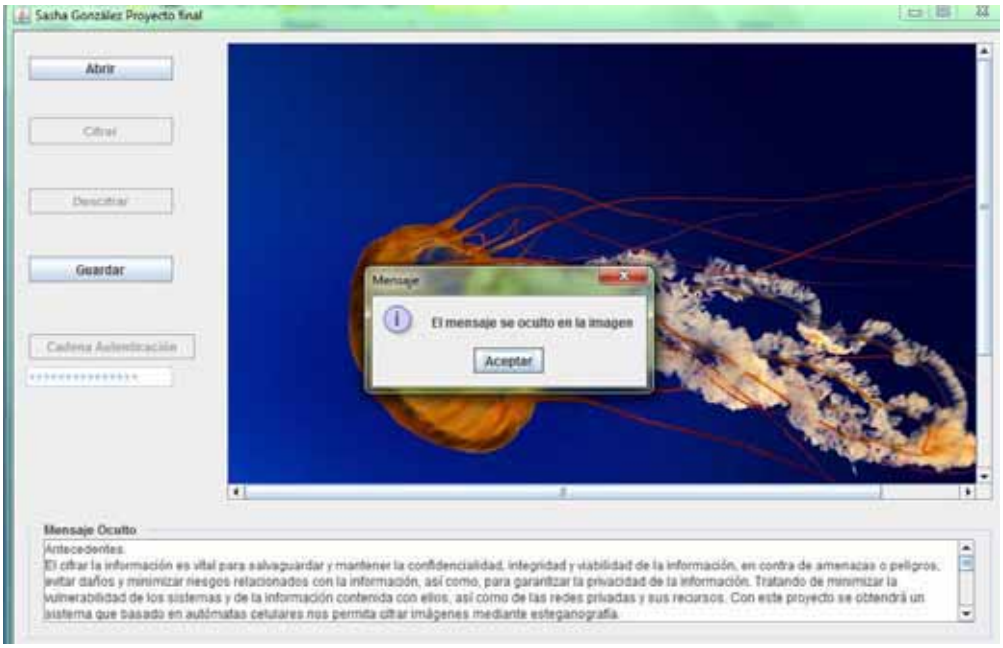
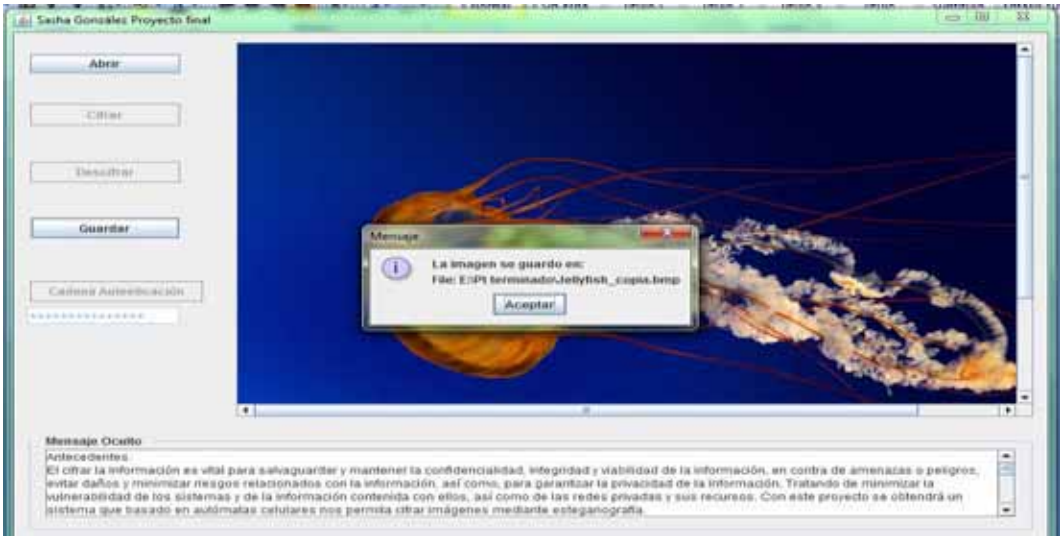


Figura 8. Mensaje oculto

La imagen Stego se debe guardar, cuando se presiona el botón guardar la imagen se guarda con el mismo nombre solo que se agrega "_ copia". Se muestra en la imagen nueve.

El siguiente paso es abrir la imagen nuevamente pero esta vez se debe elegir la copia que se creo, como se muestra en la figura 10



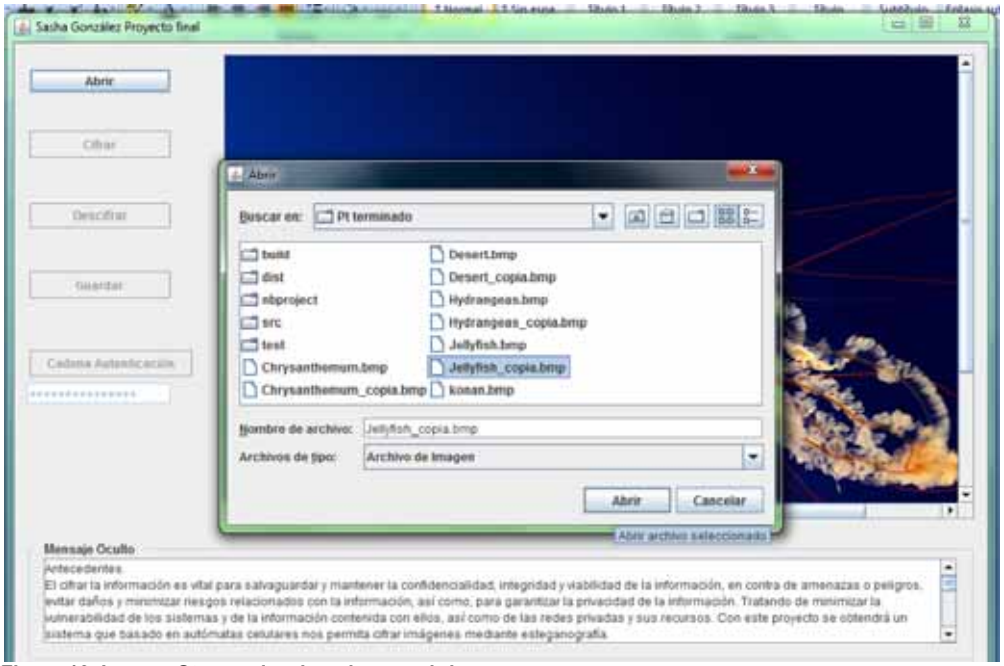


Figura 10. Imagen Stego seleccionada para abrir.

Cuando se abre esta imagen se activa el botón cadena de autenticación en este sistema la cadena es “PKCS#8X.509” esta clave es la que se obtiene del generador de llave pública y privada al concatenar estas dos claves se crea la cadena de autenticación. Nótese que en la figura once en el mensaje oculto aparece en blanco el espacio y el botón descifrar está inactivo si la contraseña es la correcta, entonces el botón descifrar se activa.

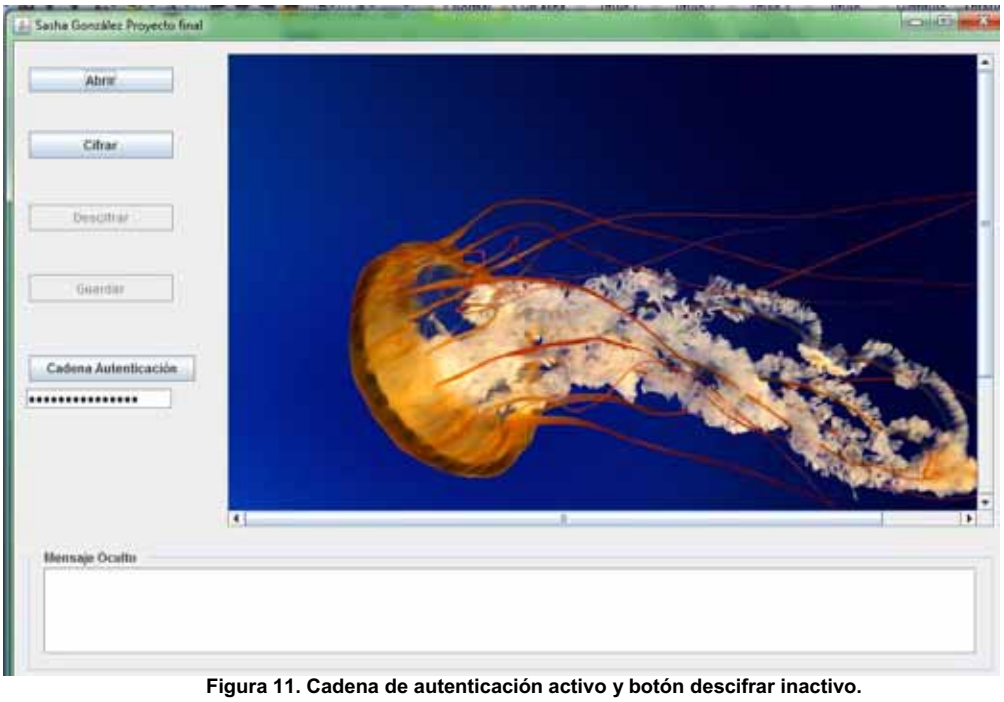


Figura 11. Cadena de autenticación activo y botón descifrar inactivo.

Si la contraseña es correcta se activara el botón descifrar Y APARECE UN MENSAJE notificando que se puede descifrar la imagen, pero si la contraseña es incorrecta el sistema arroja el mensaje notificando que la contraseña es incorrecta que intente nuevamente. Como se muestra en la figura 12 y 13 respectivamente.

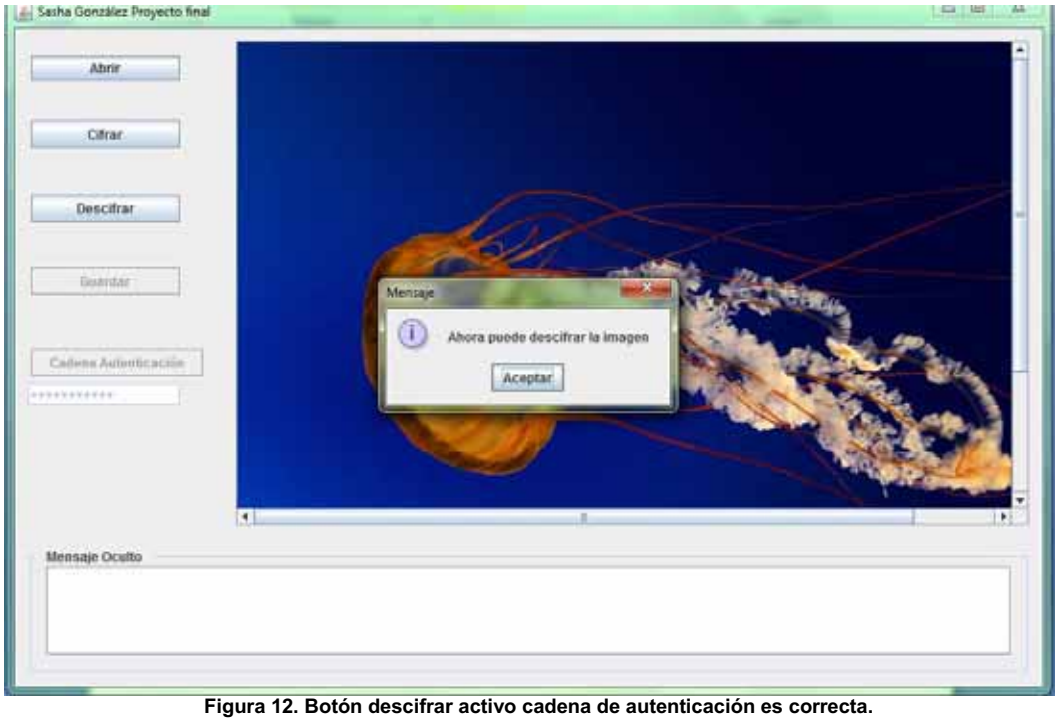


Figura 12. Botón descifrar activo cadena de autenticación es correcta.

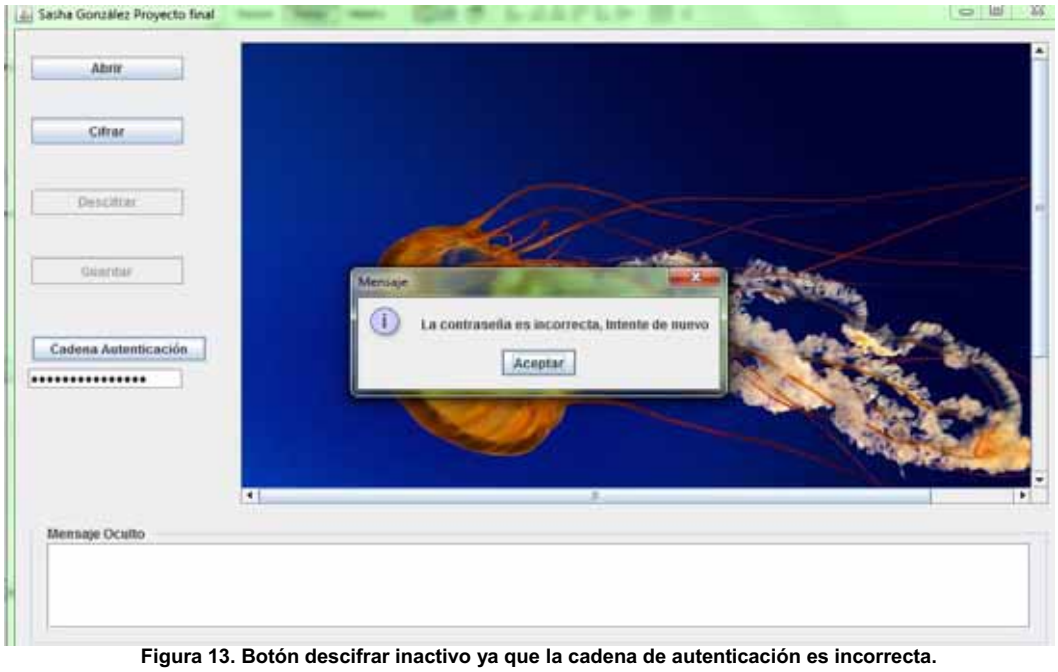


Figura 13. Botón descifrar inactivo ya que la cadena de autenticación es incorrecta.

Una vez que el botón descifrar se activa, la imagen se descifra como se muestra en la figura 14 y se muestra el mensaje oculto, en la sección de mensajes.

Figura 14.Imagen Stego descifrada.

El único modo que se tiene para comparar las imágenes (la que tiene el mensaje oculto y la que no tiene el mensaje) es revisando el peso de cada imagen.

En la figura 15 se muestra la imagen original y la imagen copia (la que contiene el mensaje oculto). Note que ambas imágenes son iguales. La imagen que se usa tiene una tamaño de 800 x 600 pixeles.

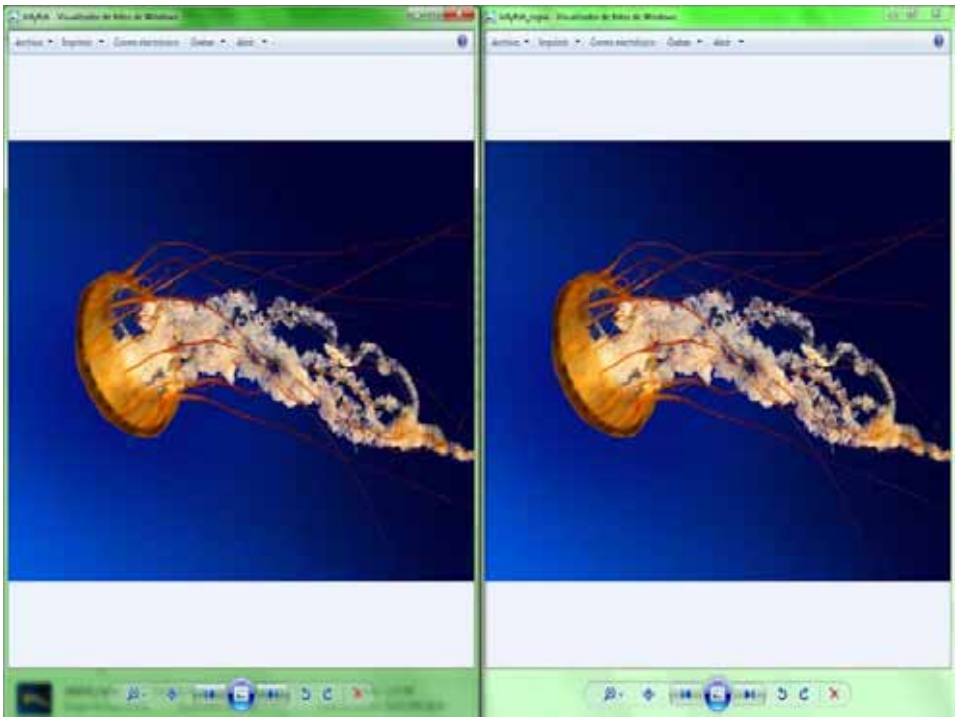


Figura 15. La imagen de la izquierda es la imagen original y la imagen de la derecha es la imagen Stego.

En la figura 16 se muestran las propiedades de cada una de las imágenes anteriores para que se note el cambio de peso entre cada imagen.

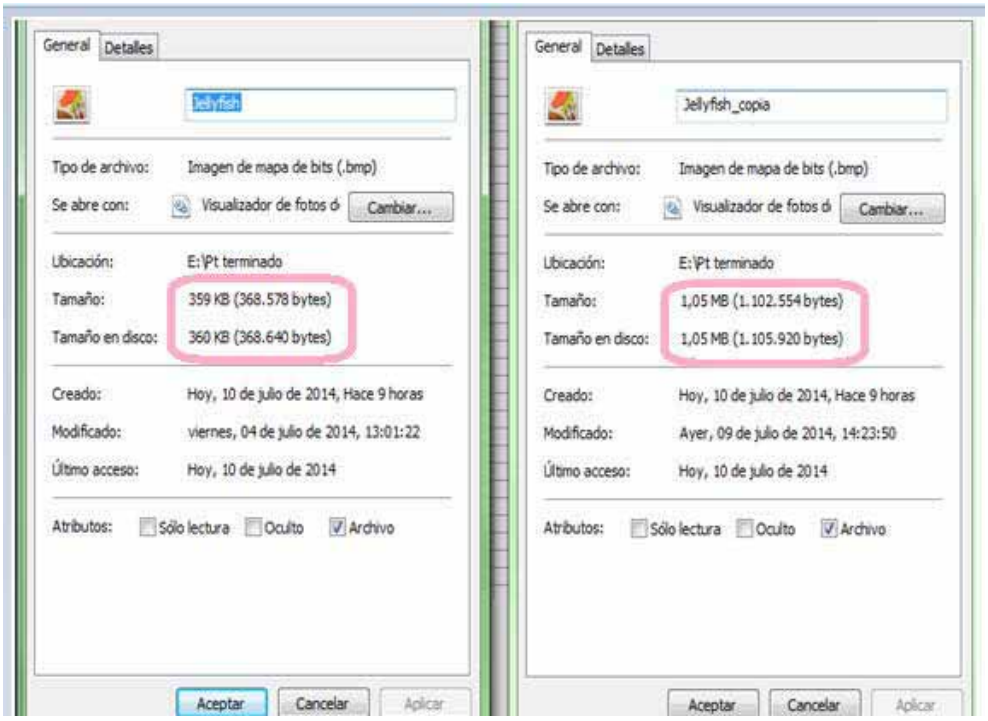


Figura 16. La imagen de la izquierda muestra las propiedades de la imagen original y la imagen de la derecha muestra las propiedades de la imagen Stego.

En las figuras 17 y, 18 se muestran otro ejemplo que usa nuestro algoritmo; para este caso la imagen tiene diferente tamaño.

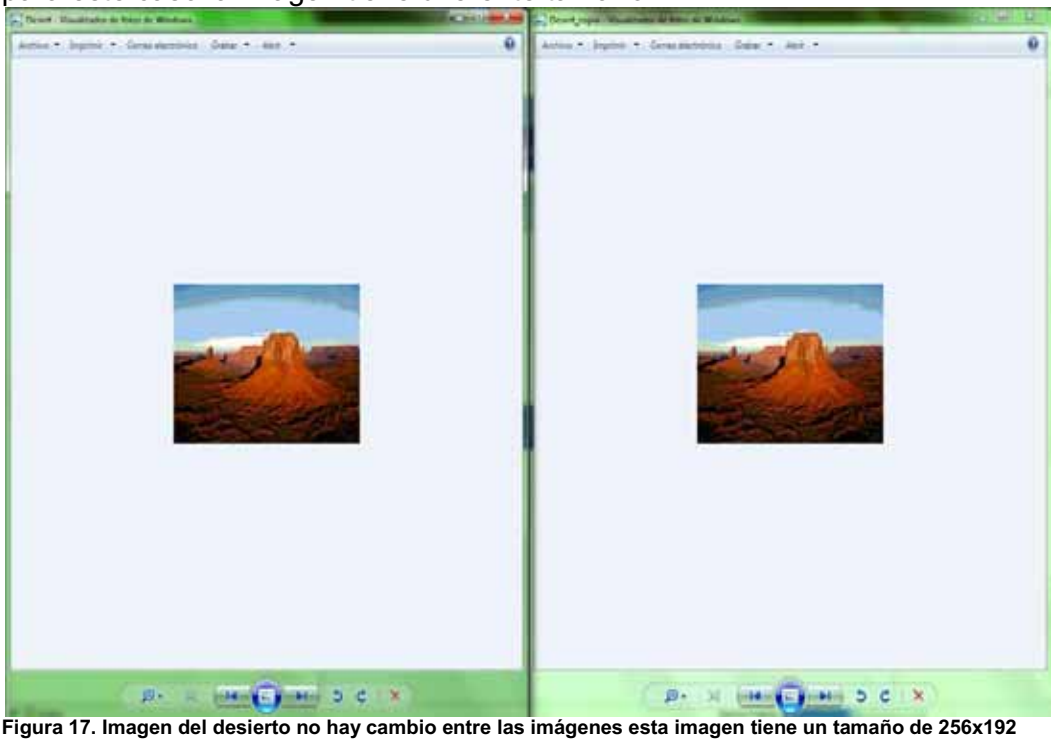


Figura 17. Imagen del desierto no hay cambio entre las imágenes esta imagen tiene un tamaño de 256x192 pixeles

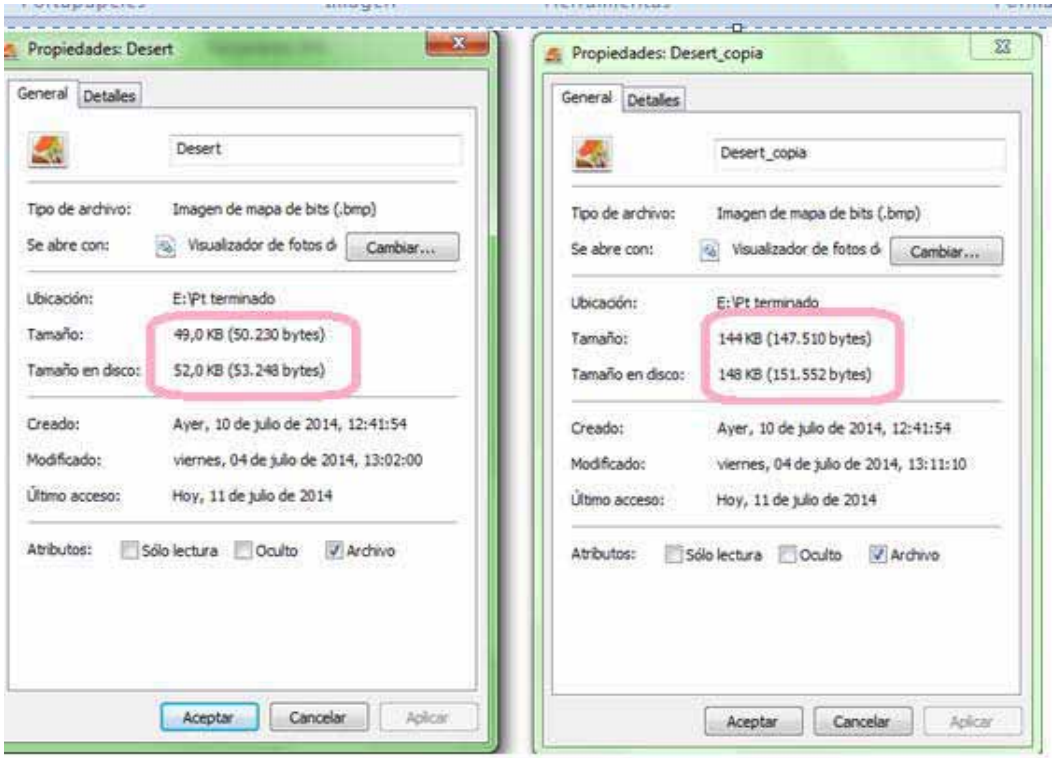


Figura 18. Se muestra las propiedades de las imágenes para que se vea el cambio de peso

CAPÍTULO V. CONCLUSIONES.

Los autómatas celulares pueden facilitar el estudio de diferentes fenómenos físicos, con este proyecto estudiamos e implementamos el cifrado de una imagen mediante esteganografía.

Su principal característica es que no se produce ninguna pérdida de resolución en la imagen recuperada, siendo por tanto ésta, exactamente igual a la original. La implementación en una computadora del algoritmo desarrollado no es complejo debido a las propiedades intrínsecas de los autómatas celulares.

En este proyecto terminal se ha desarrollado un sistema con el cual se puede cifrar una imagen bmp en la cual la salida de la aplicación es la misma imagen, sin pérdida de bits y por ende tampoco de información debido al formato usado para la imagen.

El único modo de saber que hay algo diferente en las imágenes es solo observando sus propiedades y mirar el tamaño de cada imagen.

Referencias.

[1] C. Lin, W. Tsai, “Secret image sharing with steganography and authentication,” *The Journal of Systems and Software*, vol. 73, pp. 405–414, 2004.

[2] C. Yang, T. Chen, K. Yu, C. Wang, “Improvements of image sharing withsteganography and authentication”, *The Journal of Systems and Software*, vol.80, pp. 1070–1076, 2007.

[3] C. Chang, Y. Hsieh, C. Lin, “Sharing secrets in stego images with authentication”,*Pattern Recognition*, vol. 41, pp. 3130–3137, 2008.

[4] S. Shyu, “Efficient visual secret sharing scheme for color images”, *PatternRecognition*, vol. 39, pp. 866–880, 2006.

[5] Jorge Omar Ávila Romero, “Simulación de tránsito vehicular dentro de una glorieta usando autómatas celulares”, pp.3-5, 2009.

[6] Enfoques de estudio en los Autómatas Celulares Lineales. “http://delta.cs.cinvestav.mx/~mcintosh/comun/tesismaestria/seck/node21.html”, Agosto 2001.

Documentos anexos

Anexo A - Manual del usuario