



Instituto Politécnico Nacional
Escuela Superior de Computo
ESCOM-IPN



05-2002

REPORTE TÉCNICO PREVIO

ESTEGANOGRAFÍA APLICADA

Mendoza Rodarte Saúl.

Instituto Politécnico Nacional Campus Zacatenco.
Escuela Superior de Cómputo
E-MAIL: siloe18@hotmail.com

Reyes Figueroa Arturo.

Instituto Politécnico Nacional Campus Zacatenco.
Escuela Superior de Cómputo.
E-MAIL: rysarthur@msn.com

RESUMEN

La Esteganografía es una técnica que nos permite ocultar información dentro de otra información diferente. Podemos "esconder" mensajes ó archivos dentro de imágenes, archivos de sonido, documentos de texto, etc. Esta técnica ha sufrido un importante impulso en los últimos tiempos que permiten entreverla como una de las opciones con más futuro para proteger la confidencialidad de la información.

En este trabajo desarrollamos una herramienta que nos permita ocultar nuestra información dentro de otra información diferente, y "esconder" mensajes ó archivos dentro de imágenes, donde ésta sea de fácil manejo para los usuarios finales y responder así a las exigencias de seguridad y confidencialidad de la información.

DIRECTOR:

Ing. Arturo Pruneda Martínez

Vo. Bo._____

RESUMEN	1
1. INTRODUCCION	3
2. DESARROLLO DE LA HERRAMIENTA	5
3. DISEÑO DEL SISTEMA	7
4. PROTOTIPO	11
Ocultamiento de la información	11
5. CONCLUSION DEL PROTOTIPO	14
6. SISTEMA FINAL	15
Consideraciones de la eficiencia	15
Técnica: Sustitución del bit menos significativo	15
Eficiencia	16
Desarrollo del Sistema Esteganografico	17
Componentes frente a bibliotecas	17
Componente OLE	17
Incorporación de componentes Visual Basic	18
7. STEGANOGRAPHIC	19
Apéndice A	27
Pseudo-código de Xtegan Ver 1.0.00 prev	27
Pseudo-código Librería	30
Apéndice B	35
Código Fuente de Xtegan 1.0.00 prev	35
Codigo Fuente de librería Xtegan 1.0.00 prev	36
Apéndice C	41
Codigo fuente de KernelS	41
Apéndice D	45
Codigo Fuente de KernelE	45
Apéndice E	48
Codigo Fuente de Steganographic	48
Apéndice F	60
Articulo de Sistema Esteganográfico	60

1. INTRODUCCION.

La seguridad de un sistema de cómputo es la habilidad que tiene el sistema para lograr proteger información, a pesar de las acciones de algún enemigo, quizá bien informado y con medios adecuados para corromper el sistema.

La Esteganografía es una técnica que nos permite ocultar información ó datos dentro de otra información diferente.

Para quien crea que este proceso es muy lioso, que el arte con el cual podemos encriptar un mensaje es complicado, puede acudir a programas escritos con este menester. Uno de ellos fue escrito por Ron Rivest, que realizó un sistema al que denominaron "Chaffing and Winnowing" y que consistía en enviar de forma segura mensajes en clave, intercalando tal cantidad de basura, que el atacante se veía incapaz de descifrar dicho mensaje.

Aunque piensen que solo puede aplicarse al texto no es así, pues se podría incluso realizar una imagen en la que los píxeles menos significativos son sustituidos por el mensaje en cuestión que deseemos incrustar dentro de la imagen. Incluso se podría utilizar el mismo método para archivos de sonido, no impidiendo el poder grabar unos 40 MB de información clandestina en un CD de música.

La humanidad lleva utilizando este método desde antes del inicio de la computación, aunque con nuestros computadores podemos alcanzar niveles de complejidad muy elevados a la hora de camuflar un mensaje, pues la potencia de calculo y los algoritmos que podremos utilizar para estos menesteres son realmente grandiosos, aunque también gracias a estas tecnologías, algún día podamos encontrar algún mensaje oculto en algún libro perdido, que nos revele algún que otro secreto inconfesable.

La Confidencialidad de la información se refiere a que ésta, esté accesible para lectura solamente por partes autorizadas; de forma que cualquiera que intente interceptarla no pueda tener acceso al contenido de los datos.

Comencemos por definir que la palabra Esteganografía que en castellano no aparece en el diccionario de la Real Academia, pero en cambio, no nos ofrece ninguna palabra que pueda sustituirla. El término "Esteganografía" viene del griego STEGOS, que significa "cubierta", por lo que Esteganografía significaría "escritura oculta" o "escritura encubierta".

En la Esteganografía puede aplicarse cualquier método para ocultar un mensaje, pues es en un 99% imaginación y por tanto no tiene límites.

Hay que dejar clara la diferencia entre la criptografía y la Esteganografía "estricta". La criptografía modifica los datos para que no sean legibles, a diferencia de la Esteganografía, que simplemente los toma y los oculta entre otros datos. Sin embargo, hoy en día, con las computadoras, ambas técnicas son combinables, consiguiéndose una seguridad aún mayor

Es evidente que un mensaje cifrado es identificado rápidamente por él sin sentido de su formato, en cambio si ponemos ese mismo mensaje dentro de una imagen, o de otro texto se garantiza que no vayamos paseando nuestros datos por el mundo con un letrero de "cifrado". Ello nos otorga discreción y anonimato. También existe la posibilidad de que el tráfico de la información pudiera ser tratado de forma masiva para capturar cosas de interés. Esto se suele hacer mediante el "monitoreo" de nuestro tráfico para capturar palabras clave; Palabras que si las hacemos invisibles en principio no llamarán la atención. Además los constantes rumores sobre puertas traseras en los programas más populares de cifrado pueden hacer aconsejable el uso de la Esteganografía para dar seguridad realmente potente.

No hay duda de que, si la criptografía puede tener usos delictivos, la Esteganografía puede tenerlos aún más claros. Sin embargo, bien usada puede convertirse en algo muy útil. La

Esteganografía se convierte en una útil herramienta para proteger nuestros datos, tanto combinada con la criptografía, como por separado.

Existen algunas herramientas que manejan algunas técnicas de ocultamiento de información de las cuales encontramos:

S-Tools

S-Tools, escrito por Andrew Brown, es un programa para Windows que permite cifrar y ocultar datos en archivos .wav ó en imágenes en formato .bmp o .gif.

Nota: Este programa es freeware, así que puede distribuirse libremente, si bien hay que tener en cuenta que, dado que incluye la implementación de diversos algoritmos criptográficos, podría estar sujeto a determinadas restricciones a la exportación. Su uso en Francia podría ser ilegal bajo la Ley 90-1170 de dicho país, que prohíbe el uso de criptografía. Asimismo, podría entrar en conflicto con la EAR (Regulación del Tráfico Internacional de Armas) americana.

Es seguramente el más cómodo al ser para Windows, integra la encriptación en el mismo programa, y permite ocultar los datos en archivos más "generales" que las anteriores versiones.

En cuanto a los algoritmos criptográficos, se dispone de cuatro algoritmos de clave secreta: IDEA, DES, Triple DES y MDC. IDEA es por ahora el mejor y más fuerte de los cuatro. En cuanto a DES, sería preferible no utilizarlo, dado que se le han descubierto demasiadas debilidades para seguir considerándolo seguro.

Texto

Texto, que a pesar de su nombre no es un programa español, ha sido escrito por Kevin Maher, y es un programa que transforma archivos codificados con uuencode ó archivos cifrados con PGP y ASCII armor en archivos de texto que contienen frases en inglés.

Texto sustituye los caracteres ASCII por palabras en inglés que obtiene de un archivo llamado words. Después utiliza estas palabras según las estructuras de frases contenidas en un archivo llamado structs, creando así el texto en inglés. Las palabras en mayúsculas son etiquetas que Texto sustituye por las palabras seleccionadas del archivo words.

Debido a que en el inglés también hay algunas estructuras irregulares, a veces algunas frases contienen errores gramaticales. No son demasiado graves como para hacer sospechar del texto, dado que el inglés es un idioma bastante "práctico" y relativamente simple si lo comparamos por ejemplo con nuestras lenguas latinas. Es más, estos errores hacen incluso que el texto parezca más humano, como si fuera escrito por alguien que comete faltas, y más aún, unidos estos errores a las extrañas frases, los textos producidos dan la impresión de ser escritos por alguien que padece alguna demencia o está drogado, lo que puede ayudar a no tenerlos en consideración y no examinarlos.

Asimismo, también puede modificarse el archivo words y sustituir las palabras. La condición es no utilizar palabras acabadas en "s" o en "ing", ni repetir palabras. El orden también importa, así que cambiar el actual orden de palabras de words también resultará. Eso sí, si modificamos words, debemos pasarle el nuevo archivo a la persona con la que nos comunicamos, si no, no podrá extraer los datos. En cambio, no hace falta pasarle el archivo structs aunque lo modifiquemos.

Por cierto, por si alguien lo está pensando. Y... ¿utilizar archivos en español? La idea es buena, pero el programa está pensado para el idioma inglés. Habría que meterse a modificar el código, y hay un importante problema: la mencionada "complejidad" de nuestro rico idioma, que hace que el escribir un programa que construya estructuras gramaticales en español relativamente correctas sea una dura tarea. El gran problema que tiene este programa: El texto obtenido es DIEZ VECES mayor que el archivo original. La solución que recomienda Kevin Maher es utilizar más palabras, una para cada dos símbolos, en vez de una para cada uno. Modificar el código es simple, pero esto requiere 4096 palabras de cada clase en el archivo words, algo un tanto complejo (es más, ¿hay 4096 adverbios en inglés?). De media debería conseguirse que los archivos pasaran a ser cinco veces más grandes en vez de diez veces.

2. DESARROLLO DE LA HERRAMIENTA

Con el desarrollo de este trabajo esperamos obtener una herramienta capaz de ocultar información (texto) en una imagen; así también desarrollar una documentación precisa acerca de la Esteganografía y sus aplicaciones, que sirva para establecer bases y recomendaciones en trabajos futuros en esta área.

Consideramos las acciones que el usuario tendría que hacer para interactuar con el sistema, en primera instancia es el usuario quien determina el origen de la información a ocultar, ya sea señalando el lugar de la información (archivo) ó si éste escribirá directamente la información a ocultar, posteriormente el usuario deberá indicar la imagen donde será ocultada la información con estos datos el sistema deberá ser capaz de ocultar la información proporcionada en la imagen.

Cabe mencionar que el sistema desarrollaría dos actividades importantes: la primera es ocultar una información en otra y la segunda extraer la información original del medio transportador (imagen).

Para la segunda etapa el usuario tendrá que indicar el origen (ruta del archivo) del medio transportador, y al proporcionar una clave específica además de elegir la acción el sistema deberá ser capaz de extraer la información oculta en el medio transportador.

Para que este sistema cumpla con los niveles de seguridad que la Esteganografía proporciona se tomarán en cuenta ciertas características las cuales son, que no exista variación entre la imagen original y la obtenida por medio de ésta técnica de ocultamiento, segundo que la imagen resultante ocupe el mismo espacio en disco es decir que la imagen sea del mismo tamaño, en caso de existir variaciones en la imagen estas sean imperceptibles al ojo humano.

Y finalmente de acuerdo a un estudio previo de herramientas esteganográficas existentes, se identificó las características que debía tener el software hacia el usuario final. Donde lo más importante será proporcionar una interfaz con el usuario de fácil manejo, donde no se involucren cuestiones técnicas que deben ser ajenas para éste último.

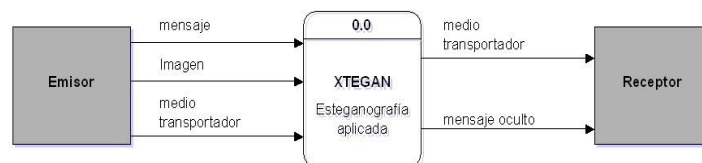


Figura 1

*Diagrama de Contexto
Esteganografía Aplicada*

En la estructura general del sistema, podemos identificar tres actores, el emisor, el sistema y el receptor.

El emisor. Este usuario final es aquel que por alguna razón tiene la necesidad de mantener segura su información, consideremos el caso de que desea enviar información importante a otra persona, las acciones implicadas son: proporcionar al sistema la fuente tanto de la información a ocultar como de la imagen que deba llevar la información oculta.

El sistema. El sistema esteganográfico recibirá como únicas entradas el mensaje o archivo y la imagen, el sistema deberá ser capas de ocultar la información del emisor con una imagen. Entregara como único resultado una nueva imagen, imagen que deberá cumplir con las características ya señaladas en los requerimientos del sistema.

El receptor. Este usuario también final, al recibir el archivo de imagen, podrá ingresarlo al sistema esteganográfico y así el sistema deberá extraer la información oculta.

En el diagrama siguiente se muestra como a pesar de existir dos procesos distintos una sola herramienta deberá de realizar ambos, ocultamiento y extracción.

Así pues entenderíamos el diagrama de la Figura 2 como sigue:

- Si al sistema le proporciono una información ó mensaje y una imagen, el sistema deberá entregarme una imagen con información oculta.
- Si al sistema le proporciono una imagen el sistema deberá entregarme el mensaje oculto.

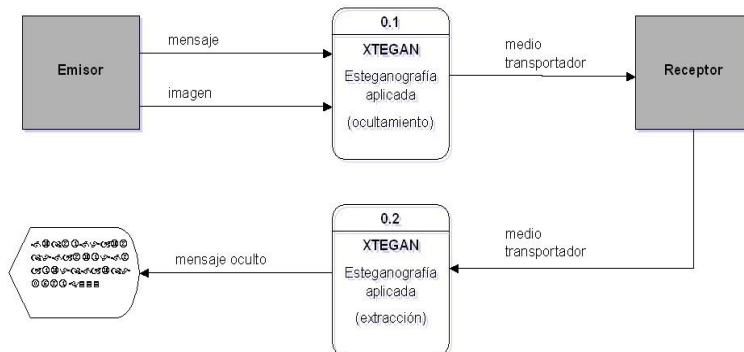


Figura 2

Diagrama Lógico
Esteganografía Aplicada

En la Figura 2 podemos observar el diagrama lógico y las etapas involucradas en el proceso de ocultamiento y extracción de la información a partir de las entradas al sistema, la imagen, el masaje ó archivo con la información a ocultar y como el receptor al ingresar la imagen generada ó medio transportador entra al sistema y el mismo sistema quien extrae la información oculta en el medio transportador.

3. DISEÑO DEL SISTEMA

Diagrama de Nivel Cero

Figura 3

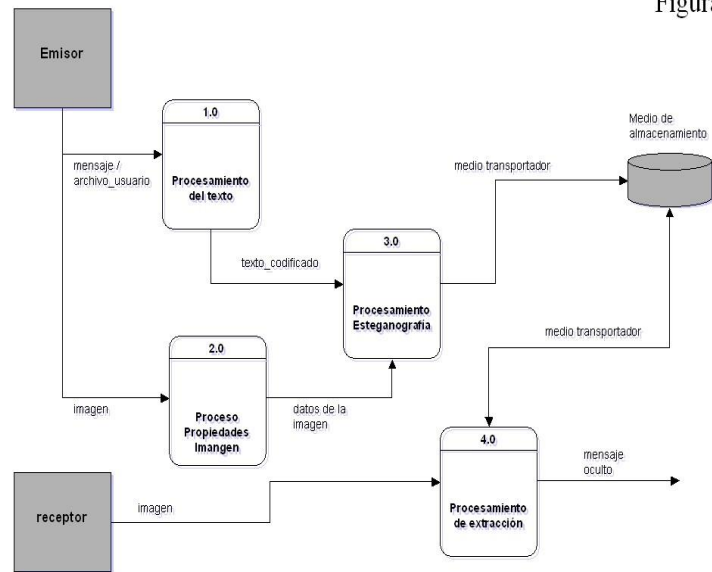


Diagrama de Flujo de Datos de Nivel Cero
Esteganografía Aplicada

En la Figura 3 observamos más claramente el funcionamiento del sistema propuesto. Empecemos por identificar cada uno de los elementos y las características de estos así como las entradas y las salidas de los procesos involucrados.

Como podemos observar en la Figura 3, el sistema esteganográfico se divide en cuatro principales procesos:

Procesamiento del texto.

Obtención de las propiedades de la imagen.

Procesamiento Esteganográfico.

Procesamiento de Extracción.

Diagrama de primer nivel "Procesamiento del Texto"

Figura 4

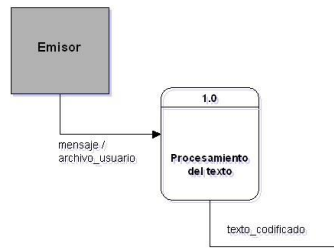


Diagrama de primer nivel "Procesamiento del Texto"

(Diagrama hijo del proceso 1.0) Esteganografía Aplicada

En la Figura 4 observamos dos tipos de entrada. En realidad es solo una, pero es el usuario quien define de donde es el flujo, que puede ser por un archivo ya existente ó que el usuario proporcione directamente el texto, el contenido de este último será procesado y como única salida se generara un registro temporal que contendrá el código designado a cada uno de los caracteres que forman el texto proporcionado por el usuario, esto es, el Procesamiento del Texto no es sino un proceso de codificación.

Este proceso puede ser tan sencillo o tan difícil como la imaginación del programador se le permita, que va desde el simple uso del código ASCII hasta quizá el uso de una técnica criptográfica que proporcione una salida distinta del original.

Aquí el proceso medular de ésta tarea es convertir todo en números ya sea enteros o en representaciones binarias (1's y 0's), pues es a nivel binario donde trabajaremos con la imagen.

En esta etapa se presenta un almacenamiento temporal es un espacio en disco designado para almacenar por un tiempo corto no al texto, sino el resultado de codificar al texto, esto es, almacenar cierta información ya tratada para que el método esteganográfico la utilice y la oculte en la imagen.

Diagrama de primer nivel "Proceso Propiedades en la Imagen"

Figura 5

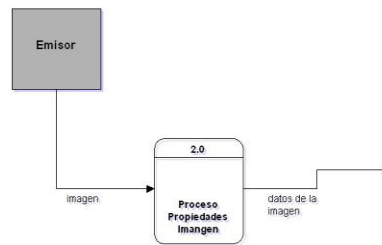


Diagrama de primer nivel "Proceso Propiedades de la Imagen"

(Diagrama hijo del proceso 2.6) **Esteganografía Aplicada**

La Figura 5, representa el proceso de obtener las propiedades de la imagen, estas son variadas, y dependen de la técnica esteganográfica a usar, pero lo más importante para toda técnica esteganográfica es conocer el tamaño como el espacio que ocupa en disco, las dimensiones, y los colores que utiliza la imagen a trabajar.

Este proceso recibe como entrada una imagen, la estudia y genera un registro (datos de la imagen) y la guarda por un tiempo relativo hasta que se genera la imagen o medio transportador.

Aquí observaremos que también existe un almacenamiento temporal de información ya que solo existirá hasta el momento de entregarle al usuario la nueva imagen creada, este contendrá la información recabada por el sistema, de las características de la imagen proporcionada o seleccionada por el usuario, generándose un registro el cual será la entrada del proceso esteganográfico; éste proceso será transparente para el usuario.

Diagrama del primer nivel "Procesamiento Esteganografía"

Figura 6

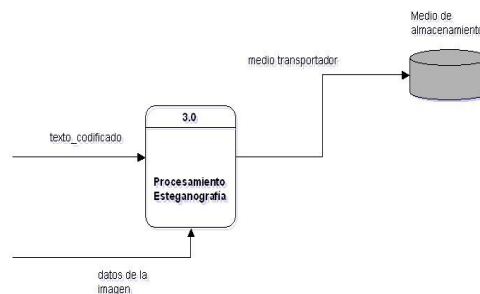


Diagrama de primer nivel "Procesamiento Esteganografía"

(Diagrama hijo del proceso 3.0) **Esteganografía Aplicada**

En el diagrama de la figura 6 observamos el proceso esteganográfico, aquí es donde interviene la implementación de la técnica esteganográfica seleccionada, sea cual sea la técnica, recibirá la codificación del mensaje original, los datos de la imagen es decir el registro de la imagen y nos dará como único resultado una imagen nueva, similar a la imagen original

En éste mismo diagrama mostramos el medio de almacenamiento donde se guardara el nuevo archivo generado tras el proceso de ocultamiento de información. Este almacén también lo podemos observar desde un punto de vista, como el sistema de archivos, ya que el resultado del proceso esteganográfico será un archivo, este es el mismo medio transportador o imagen generada.

También mostramos una salida más, que aparentemente no debe estar, pero existe por la simple selección que emitirá el usuario entre guardar la imagen nueva y quizá mostrar en pantalla el resultado, eso como una opción que tendrá disponible el usuario para su comodidad y pueda observar el resultado.

Diagrama de primer nivel "Procesamiento de Extracción"

Figura 7

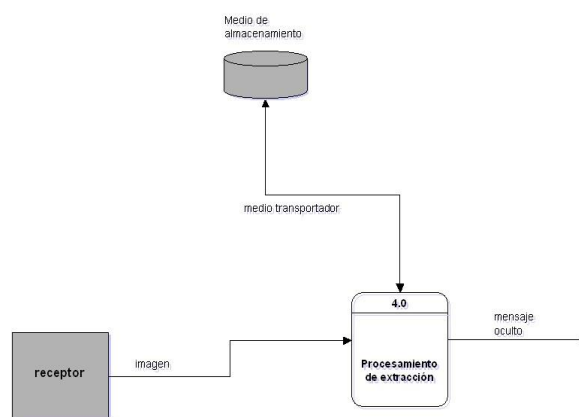


Diagrama de primer nivel "Procesamiento de Extracción"

(Diagrama hijo del proceso 4.0) Esteganografía Aplicada

En el diagrama de la parte superior (Figura 7), encontramos el Proceso de Extracción. Este proceso comprende las tareas que el sistema deberá realizar para extraer la información original de un medio transportador, como entrada será la imagen ó medio de transportador, el usuario que quiera extraer la información contenida deberá proporcionar una clave para con la cual extraerá la información.

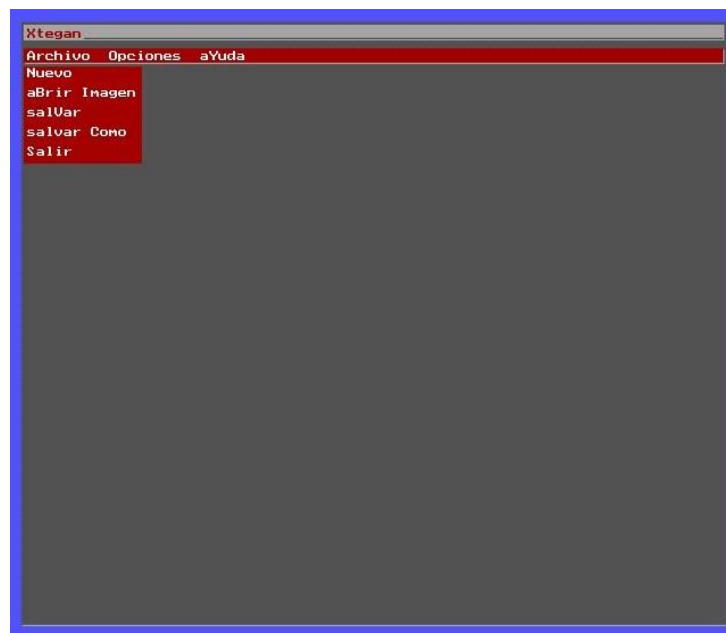
4. PROTOTIPO

El Primer Sistema llamado Xtegan es una propuesta experimental para observar y entender las opciones con las que debe contar el sistema a desarrollar.

Este primer sistema, se caracteriza principalmente por haber sido desarrollado en Lenguaje C. Inicialmente porque C es un lenguaje poderoso y flexible. Lo que se puede lograr con el C es muy extenso y muy poco limitado para los expertos del lenguaje. El lenguaje, por sí mismo, no pone límites. El C es un lenguaje portable. La portabilidad se aumenta con el estándar ANSI para el C (el juego de reglas para los compiladores C).

Como muestran estas características, el C es una alternativa excelente para haber desarrollado el "Primer Sistema".

Acerca del primer prototipo de sistema, pensamos en una interfaz grafica, de fácil manejo por el usuario, y las opciones del menú principal sean claras y cuente con cuadros de dialogo con información suficiente para saber cual será el siguiente paso de cada proceso.



Esta pantalla nos permite observar las opciones básicas del sistema.

Ocultamiento de la información.

La herramienta Esteganográfica propuesta, debe obtener la información a oculta de alguna forma, ya sea proporcionada por el usuario ó que este último la escriba directamente, sea cuál sea el origen, esta información deberá ser codificada de alguna manera, el objetivo es que el sistema pueda manipular la información que se precisa ocultar.

Una forma sencilla es asignar un código específico a un carácter en particular.

Carácter	A	B	C	...	y	z
código DEC	0	1	2	...	55	56
código BIN	00000000	00000001	00000010	...	00110111	00111000

De esta manera obtendremos la codificación de mensajes como “ABz” de la siguiente manera:

“0000000000000001000111000”.

Consideramos ahora, las características de la imagen a ser tratada, desde el punto de vista más básico un archivo es un conjunto de información binaria, con un formato en particular, basados en esa idea, un archivo de imagen también esta formado de bits con un formato específico, consideremos el archivo como arreglos o conjuntos de 8 bits, la que contienen estos es la información de cada uno de los píxeles que conforman la imagen.

Considerando estas características resulta muy sutil que exista la posibilidad de manipular el menos el bit menos significativo de los arreglos binarios.

Ahora si deseamos ocultar un carácter “y” dentro de un arreglo como el siguiente:

0000110000011000001100000010010000110111001111101000000010111110

Obtendríamos algo así:

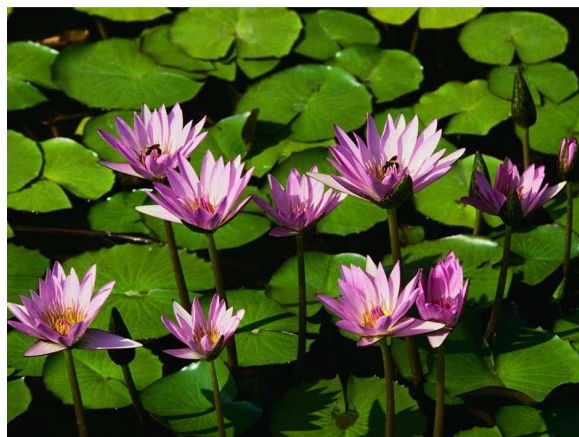
Original	Con cambios
00001100	00001100
00011000	00011000
00110000	00110000
00100100	00100100
00110111	00110111
00111110	00111110
10000000	10000000
10111110	10111110

Y la cadena binaria resultante queda así:

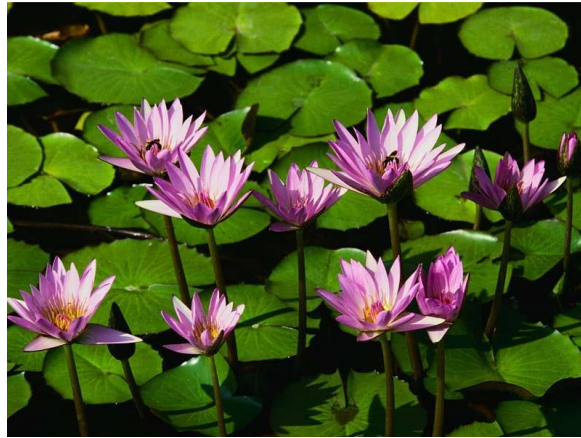
00001100000110000011000100100100011011000111111000000010111111

Estos cambios no repercuten seriamente en la imagen original así como en sus características más importantes, al menos no a simple vista, ya que lo que único que hacemos es cambiar el color original, y así convertirlo a un tono mas claro ó más oscuro.

El siguiente ejemplo entre dos imágenes una original y la otra ya transportando un mensaje “hola mundo cruel ya nunca te veré”.



Esta es la imagen original, la cual usaremos como medio transportador.



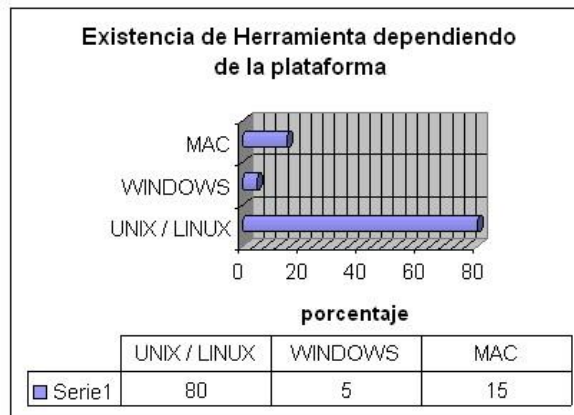
Esta imagen ya está portando un mensaje oculto, observando ambas imágenes, observamos que no existe diferencia a simple vista del proceso al que estuvo sujeta esta imagen.

Aunque la versión final sea desarrollada **tentativamente** en Visual C++, el desarrollar este prototipo en ANSI C nos permitirá generar código lo suficientemente manipulable, para los fines que hemos planteado.

Justificación de usar *visual C++*

Ya que es una versión mejorada de C y C++ pero esto no justifica su uso... mas bien la justificación de desarrollar una herramienta a partir de un lenguaje específico se elabora a partir de entender las características que debe cumplir el nuevo sistema y a otros criterios técnicos como la factibilidad y la gestión del proyecto.

Una de las etapas del análisis del sistema fue emprender una investigación a cerca de las herramientas esteganográficas existentes en el mercado, con este estudio encontramos que al menos el 80% de las herramientas y sistemas existentes en esta área de la seguridad, son sistemas basados para plataformas Unix / Linux (ver figura abajo)



Y el resto como observamos en la Figura se encuentra dividido entre las herramientas para MAC y Windows, este último representa la plataforma en la que existe el menor desarrollo de herramientas esteganográficas; razón por la cual la plataforma de desarrollo elegida es Windows, implica generar una herramienta mas dentro de las pocas existentes (solo dos) para esta plataforma.

Una vez determinada la Plataforma se entiende la respuesta de porque se utiliza Visual C++ como el Lenguaje de Desarrollo de la herramienta propuesta.

5. CONCLUSION DEL PROTOTIPO

La herramienta esteganográfica a desarrollar, nos permitirá, contar con un transporte de información más seguro, ya que la información podrá pasar desapercibida, por los ojos de cualquier persona ajena al destinatario, en forma de imagen, sin despertar la sospecha de que ocultamos información, aunque el ocultar información dentro de otra, ó en específico una información dentro de una imagen, aún es considerado un arte, el desarrollo de un algoritmo capaz de implementar este proceso resulta benéfico por las cuestiones de seguridad que se verán implicadas, proporcionando confidencialidad e integridad a la información a tratar.

6. SISTEMA FINAL

Consideraciones de la eficiencia

Como sabemos hay varios métodos para cifrar información; así, debemos conocer diversas consideraciones de eficiencia relacionadas entre si, las cuales a menudo están en conflicto, para elegir con inteligencia cual método de programación es el mas apropiado para un problema en particular.

Tres, son las consideraciones más importantes:

- El tiempo que debe dedicar el programador para codificar un programa en particular.
- La cantidad de tiempo de maquina necesario para ejecutar el programa.
- La cantidad de espacio necesario para el programa.

El problema de ocultar la información contenida en un archivo, dentro de una imagen puede ser tan sofisticado o tan simple como se vea desde el diseño atendiendo los requisitos de espacio y tiempo. A menudo los métodos sencillos son peores o solo un poco mejores que métodos más sofisticados pero generalmente menos eficientes. Asimismo si el programa de ocultamiento solo se va a ejecutar una vez y hay tiempo y espacio de maquina suficientes en los cuales ejecutarlo, seria ridículo dedicarle muchos días a investigar los mejores métodos para obtener un resultado específico. En este caso la cantidad de tiempo dedicado al programa se debe dirigir a la técnica a desarrollar, en este caso la técnica de ocultamiento. *“El tiempo de programación nunca es una excusa valida para utilizar un programa incorrecto”*.

Esto nos lleva exclusivamente a dos consideraciones de eficiencia: el espacio y el tiempo. Al igual que en la mayoría de las aplicaciones de computadora, con frecuencia el programador debe optimizar uno de estos dos conceptos a costa del otro.

Observemos la técnica y mas adelante explicaremos la eficiencia del sistema.

Técnica: Sustitución del bit menos significativo.

Las herramientas de Plano de bits abarcan métodos que aplican inserción de LSB (bit menos significativo) y manipulación del ruido. Estos acercamientos son comunes en Esteganografía y son relativamente fáciles de aplicar en imagen y audio. Una cantidad sorprendente en información puede esconderse en un espacio pequeño y el impacto no es perceptible a la imagen que lo lleva. Herramientas de la muestra usadas en este grupo incluyen StegoDos, S-tools, Mandelsteg etc. La estructura de la imagen usada en tales métodos de la Esteganografía típicamente es pérdida y los datos pueden manipularse directamente y pueden recuperarse. Algunos de estos programas aplican condensación y encriptación además de los servicios del Esteganografía. Estos servicios proporcionan mejor seguridad de los datos ocultos. Aun así, los métodos del plano de bits son bastante quebradizos y vulnerables a corrupción debido a los cambios pequeños al portador.

El proceso de ocultamiento consiste en escoger un subconjunto $\{j_1, \dots, j_m\}$ de elementos de la tapa y realizando el funcionamiento de substitución $cji\ mi$ en los intercambios del LSB de cji por mi (los mi pueden ser 1's o 0's). También puede que en una imagen el funcionamiento de la substitución cambia más de un bit de la tapa, por ejemplo guardando dos bits del mensaje en los dos menos significantes en una tapa-elemento. En el proceso de extracción, se extraen los LSB de los tapa-elementos seleccionados y se alinean para reconstruir el mensaje confidencial. Este esquema básico se presenta en algoritmos 1.1 y 1.2

Para poder descifrar el mensaje confidencial, el receptor debe tener acceso a la sucesión de índices de los elementos usada en el proceso ocultamiento. En el caso más simple, el remitente usa todos los tapa-elementos para el traslado de información y empieza en el primer elemento. Desde que el mensaje confidencial normalmente tendrá menos bits que el $l(c)$, el proceso ocultamiento terminará mucho tiempo antes del extremo del elemento de la tapa inalterado.

Esto puede sin embargo, llevar a un problema de seguridad serio: la primera parte de la tapa tendrá propiedades estadísticas diferentes que la segunda parte, ninguna modificación tenida ha sido hecha. Por encima viene este problema, por ejemplo; en el programa del dominio público el Disimulo de PGM agranda el mensaje confidencial con azar bit - para que el $I(c) = el I(m)$ - en un esfuerzo por crear un cambio igual al principio en aleatoriedad y el extremo de la tapa. El proceso ocultamiento cambia muchos más elementos así que se requerirá la transmisión del secreto. Por consiguiente la probabilidad que un agente externo sospechará aumentos de comunicación confidenciales.

Proceso de ocultamiento

for $l=1, \dots, l(c)$ **do**

$si \leftarrow ci$

end for

for $i=1, \dots, l(m)$ **do**

compute index j_i where to store i_{th} message bit

$Sji \leftarrow Cji \leftrightarrow mi$

(1.1)

For $i=1, \dots, l(M)$ **do**

Compute index Ji where the i_{th} message bit is stored.

$M_i \leftarrow LSB$

end for

(1.2)

Un acercamiento más sofisticado es el uso de un generador de número pseudo- aleatorio para extender el mensaje confidencial encima de la tapa más bien de manera del azar; un acercamiento popular es el método de intervalo de azar.

Proceso de ocultamiento: método del intervalo aleatorio

for $i = 1 \dots l(c)$ **do**

$Si \leftarrow Ci$

end for

Generate random sequence Ki using seed k

$n \leftarrow K1$

for $i = 1, \dots, l(c)$ **do**

$Sn \leftarrow Cn \leftrightarrow mi$

$n \leftarrow n+ki$

end for.

Eficiencia

En la sección anterior observamos la presencia de ciclos "for" ello es porque requiere operaciones de búsqueda así como de comparaciones iterativas. Así pues estos procesos se llevan a cabo i-ocasiones. Consideremos cómo k-iteraciones para n-caracteres, con lo que obtenemos $0 \leq i < k < n$

Entendamos pues, que n es el número de caracteres a ocultar contenidos dentro de un texto y k como el elemento en particular a ocultar. En este caso en particular hay $n-1$ ciclos y $n-1$ comparaciones en cada ciclo, por tanto el numero total de comparaciones es $(n-1)*(n-1)=n^2-2n+1$, los cual es exactamente **$O(n^2)$** . Por su puesto la cantidad de comparaciones dependerá del orden original del archivo. Sin embargo la cantidad de intercambios, es decir, el cambio de bits menos significativos LSB no puede ser mayor que la cantidad de comparaciones. Es probable que la cantidad de intercambios ocupe más tiempo de la ejecución del programa que la cantidad de comparaciones. Por lo tanto si deseamos ocultar un archivo que contiene 10,000 caracteres, el número de comparaciones será de 99, 980,001.

Significaría que el proceso es ineficiente con respecto al número de iteraciones que tiene que llevar a cabo. Sin embargo observemos el comportamiento de la velocidad.

Veamos como afecta la velocidad de este proceso. Para un carácter en particular se realizan $n-1$ iteraciones. Puesto que ya hemos encontrado un k -carácter, en el siguiente ciclo se realizarán $n-2$ iteraciones. Si este proceso lo repetimos para k -número de caracteres obtendremos $(n-1)+(n-2)+(n-3)+\dots+(n-k)$ lo cual es igual a $(2kn-k^2-k)/2$.

Por lo que continuando con el ejemplo anterior un texto que contiene 10,000 elementos puede estar formado por un conjunto de k -caracteres (un alfabeto de 28 letras mas 5 caracteres especiales y 10 números).

Si $k=43$ y $n=10,000$ entonces $(2kn-k^2-k)/2 = 429054$ instrucciones. Si cada una de ellas se realiza en el orden de 1ns, el tiempo de ejecución será de 0,000429054 seg. Por lo que en términos de velocidad el algoritmo es eficiente.

Como podemos observar con el ejemplo anterior, se satisface la eficiencia en cuanto al tiempo pero no en la eficiencia en cuanto al número de iteraciones de la ejecución.

Desarrollo del Sistema Esteganografico.

Hasta este momento ya hemos habla del proceso de ocultamiento y extracción de la información contenida en una imagen, observamos la eficiencia del algoritmo y el tiempo de respuesta de este ultimo. El siguiente paso es el desarrollo de nueva interfaz, que cumpla con las características planteadas desde el inicio del proyecto, para ello no introduciremos en los conceptos propios del desarrollo de aplicaciones para Windows.

En secciones anteriores introdujimos la tentativa de desarrollar la aplicación en Visual C++, sin embargo dadas las características de este sistema, incursionar en la MFC de Visual C++ se convertía en una tarea sino complicada, si extremadamente engorrosa, ya que se basa en el paradigma orientado a objetos. Concluyamos que no sería cómodo desarrollar esta aplicación en este paradigma.

Componentes frente a bibliotecas

Las aplicaciones desarrolladas hasta hace poco estaban basadas exclusivamente por bibliotecas de objetos como la tan conocida MFC. Actualmente los desarrollos empiezan a incorporar *componentes software*; pero cuando no disponemos del componente adecuado no queda mas remedio que utilizar las bibliotecas tradicionales de objetos, es por eso que el proceso modular del desarrollo del Sistema Esteganografico se basa principalmente en el desarrollo de los componentes. Ello por que encontramos que los objetos de una biblioteca tradicional dependen del entorno como sucede en Visual C++, esto genera un inconveniente. En cambio, un componente tiene la ventaja de que es un elemento estándar, y no encontraremos problemas en las actualizaciones futuras, problemas que si se pueden presentar cuando las aplicaciones están basadas en una biblioteca de objetos concreta. Tal vez la única ventaja de un objeto de una biblioteca tradicional frente a un componente sea un ligero incremento en la velocidad de ejecución.

Componente OLE

Nuestro objetivo además de desarrollar los componentes era buscar una arquitectura destinada a la comunicación de objetos, independiente de plataformas y de lenguajes de programación. El modelo COM (Component Object Model). Modelo básico de componentes que permite a los mismos comunicarse independientemente del lenguaje y de la plataforma. COM es un modelo de componentes propietarios a diferencia de otros mas conocidos como el DCOM de CORBA basado en componentes distribuidos.

COM se preocupa de la estructura binaria de los componentes y DCOM de los protocolos de comunicación, por tanto el modelo COM sugiere ser nuestra mejor alternativa, sin embargo esta no actuara de manera única, ya que se requiere englobar en una sola aplicación distintos componentes cada uno con características propias.

Por lo que el desarrollo de esta aplicación además deberá hacerse basado en componentes OLE. OLE (**Object Linking and Embedding**) es un sistema de manipulación de objetos basado en COM, que ha ido creciendo hasta englobar casi todo. Además permite acceder a objetos fuera de la aplicación principal como si fueran propios.

Una de las características mas importantes del Sistema Esteganografico es que además de compartir una estructura de datos procesos tales como ocultamiento y extracción cuentan con una estructura de datos propia así que el funcionamiento de la aplicación final dependería exclusivamente de donde se encuentren ubicados los mismos, con ello concluimos que el nuevo paradigma de desarrollo orientado a los componentes es la mejor alternativa para el desarrollo de la aplicación.

Incorporación de componentes Visual Basic

Comencemos por explicar algunas cuestiones técnicas, el desarrollo del Sistema Esteganografico en un lenguaje en particular resulta difícil de llevarse a cabo es por eso que optamos por desarrollar los distintos módulos en distintos lenguajes de programación, no solo eso sino incluso en distintos compiladores para así generar los componentes deseados.

Visual Basic como lenguaje de desarrollo se presenta como la mejor opción para manipular los componentes ya desarrollados en Visual C++, C++ y Borland C++. Todo esto porque las distintas versiones de C++ manipulan los archivos aunque de manera similar los resultados son distintos.

Se presentaría la necesidad de establecer los mecanismos de comunicación entre los componentes así que Visual Basic presenta el ambiente de desarrollo más idóneo para este objetivo. De ahí su incorporación en el desarrollo del Sistema Esteganografico.

7. STEGANOGRAPHIC

Steganographic 1.02.27 es la nueva versión de **Xtegan 1.0.00 Prev.** Esta nueva versión se caracteriza porque cuenta con una interfaz grafica estándar para Windows con lo cual resulta una herramienta mas amigable que su antecesor, puesto que dispone de cuadros de dialogo informativos para cada evento que se presente dentro del sistema, asistentes tanto para ocultamiento como para la extracción de la información, un browser para búsqueda de información en línea así como la ayuda del sistema.

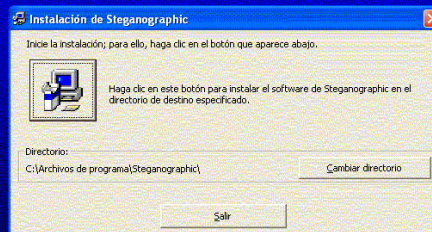
Comencemos por la instalación de la aplicación. Es un proceso sencillo para aquellos que ya están familiarizados con el ambiente Windows y de no ser así no existe mayor problema, ya que el asistente de instalación realizara todo por el usuario, este solo tendrá que seleccionar algunas opciones.

Inserte el disco en su PC en la unidad de CD. En el explorador seleccione la unidad de CD (D: comúnmente) observara un conjunto de archivos, seleccione Setup.exe y espere a que se cargue el asistente, observara la siguiente pantalla:



En la imagen anterior observamos la presentación de la instalación del sistema Steganographic.

Instalación de Steganographic

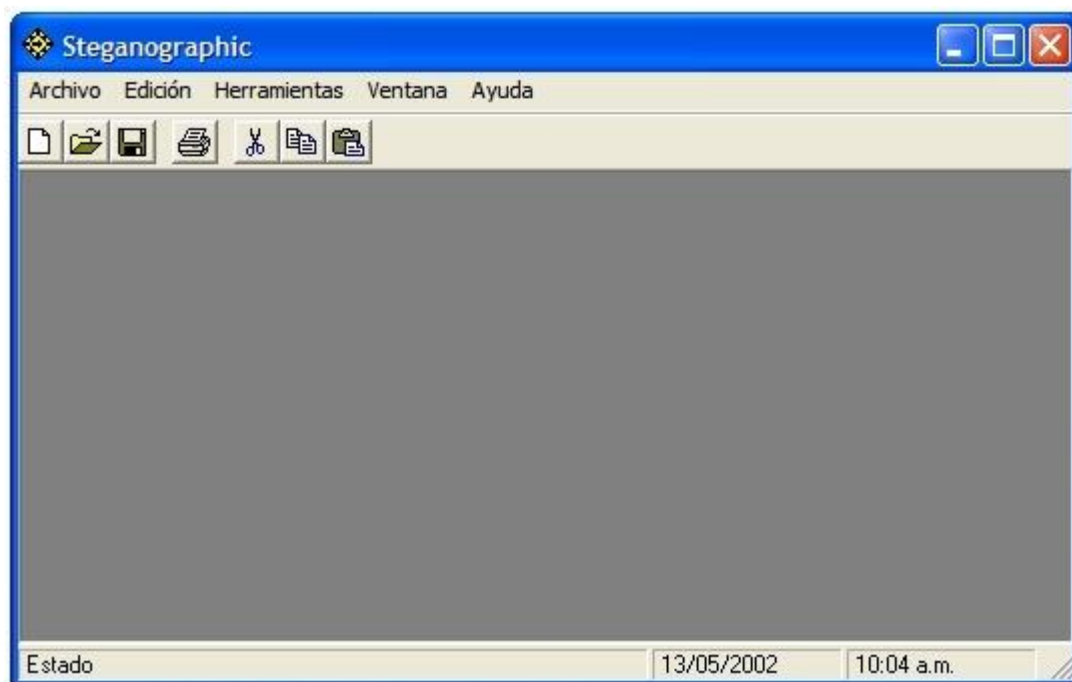


En la figura anterior podemos observar la segunda pantalla de la instalación del sistema en la cual nos presenta la opción de asignar una dirección a la carpeta que contendrá el sistema.

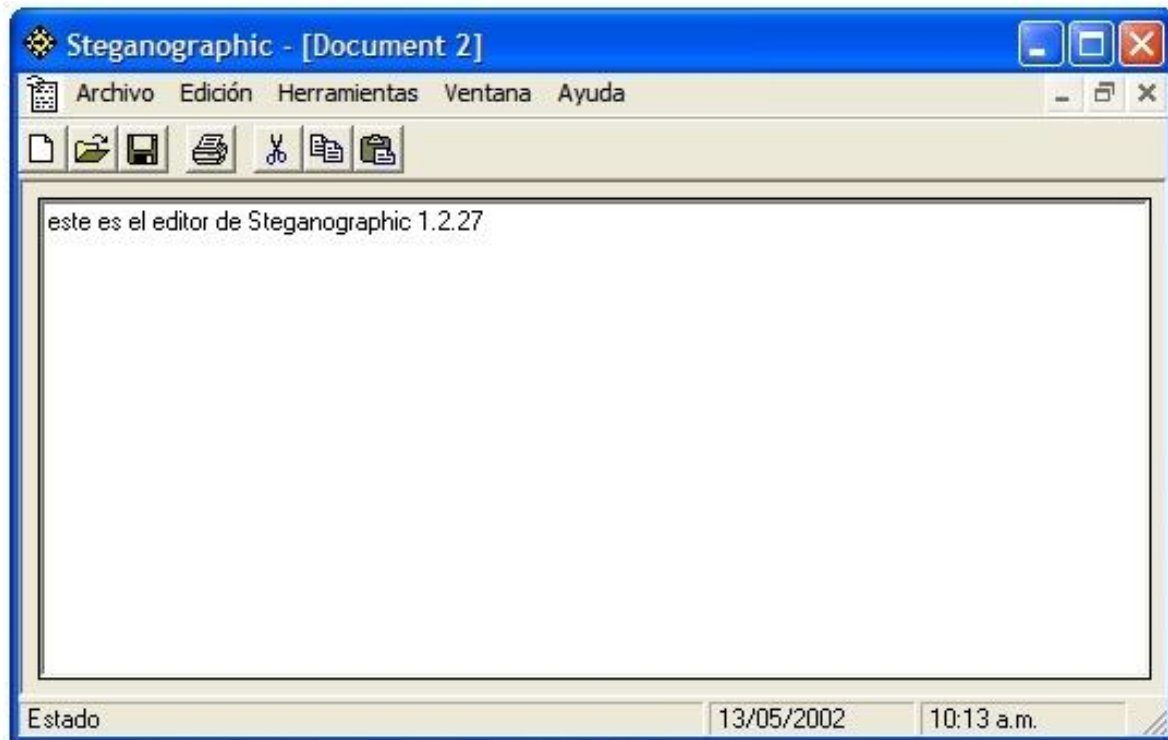
La instalación deberá finalizar sin mayor contratiempo después de lo cual podrá ejecutar Steganographic desde el menú Inicio/Programas, donde estará asignado un icono de acceso directo. Después de ejecutarlo aparecerá un dialogo de inicio de sesión donde deberá escribir su nombre de usuario acompañado de la clave correspondiente.



A continuación aparecerá la ventana principal de la aplicación.



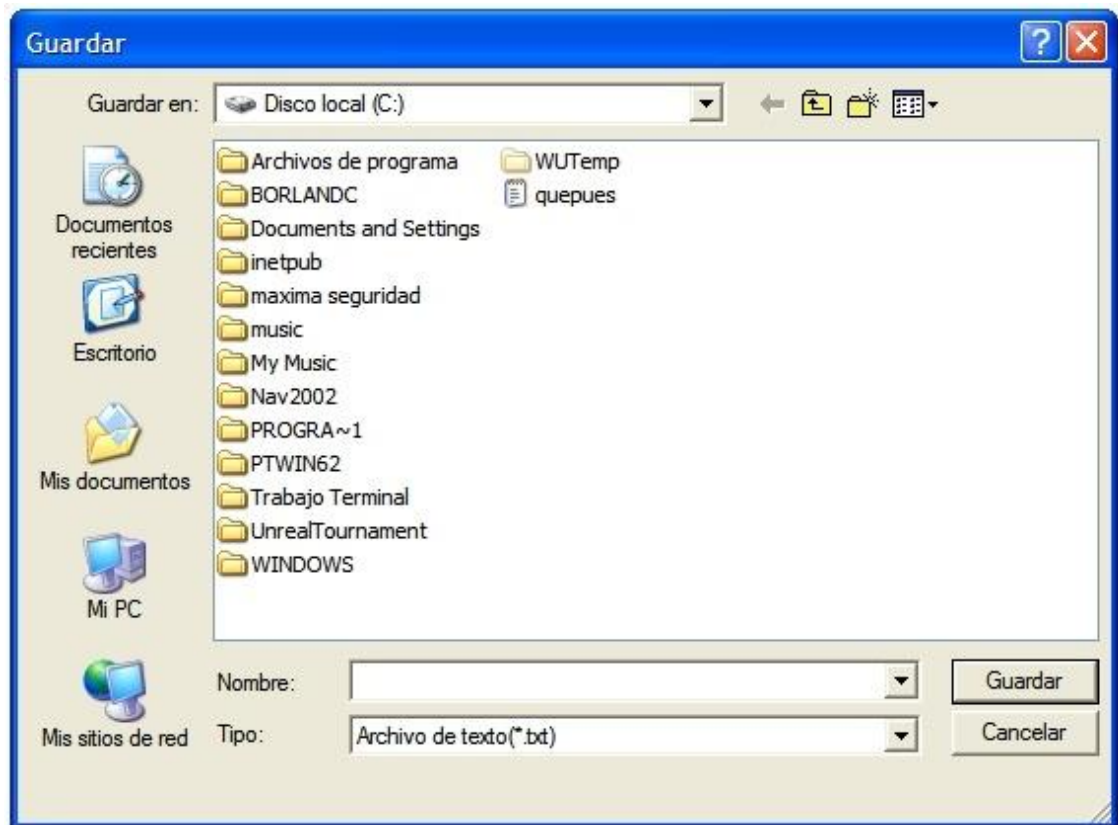
Una vez que este la ventana principal podemos comenzar a escribir la información que deseamos ocultar. Comenzando a escribir en una hoja tipo procesador de texto, como se muestra en la siguiente figura.



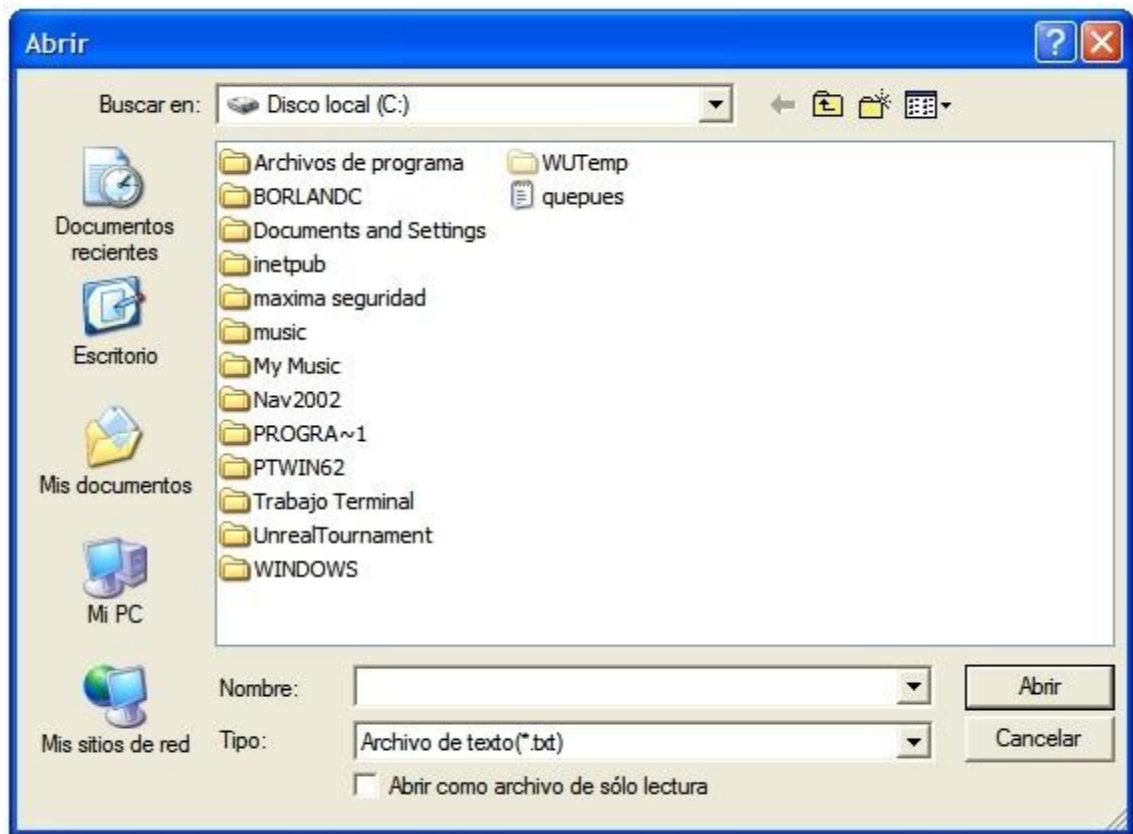
El sistema esteganografico **Steganographic 1.02.27** cuenta con algunas opciones dentro de su menú como lo son: archivo, edición, herramienta, ventana, y ayuda, Además de algunos iconos funcionales como los son: nuevo, abrir, guardar, imprimir, cortar, copiar y pegar.



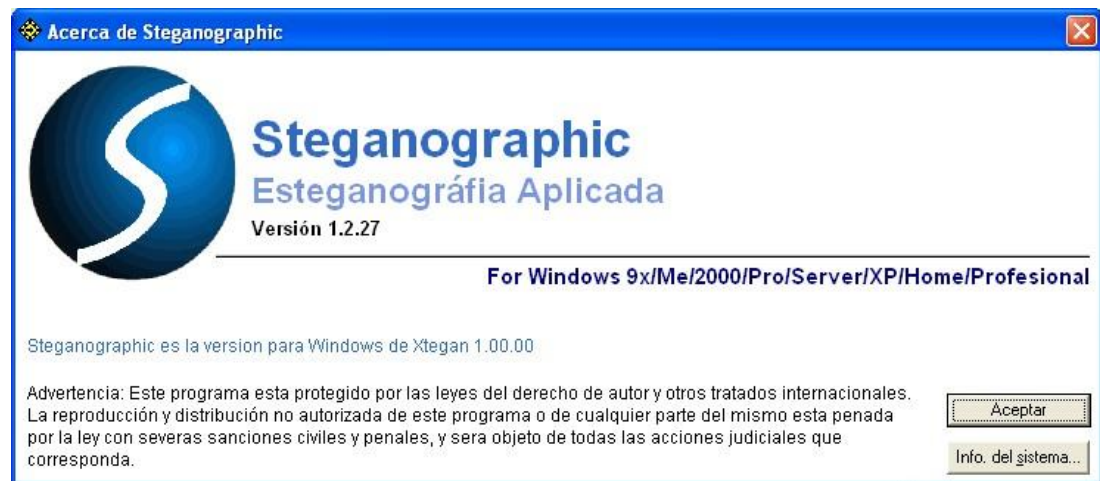
El sistema **Steganographic 1.02.27** tiene la opción de guardar el archivo que hemos creado el cual contiene la información a ser oculta. Cuando nosotros intentamos guarda un archivo aparece la ventana perteneciente a esta aplicación que es una ventan con la que el usuario esta demasiado familiarizado, esta ventana nos da la opción de guardar en la dirección que nosotros queramos y con el nombre que nosotros deseemos.



También cuenta con una opción para abrir un archivo ya existente y esta tiene también una ventana correspondiente la cual nos permite buscar la ubicación del archivo que nosotros queremos abrir.



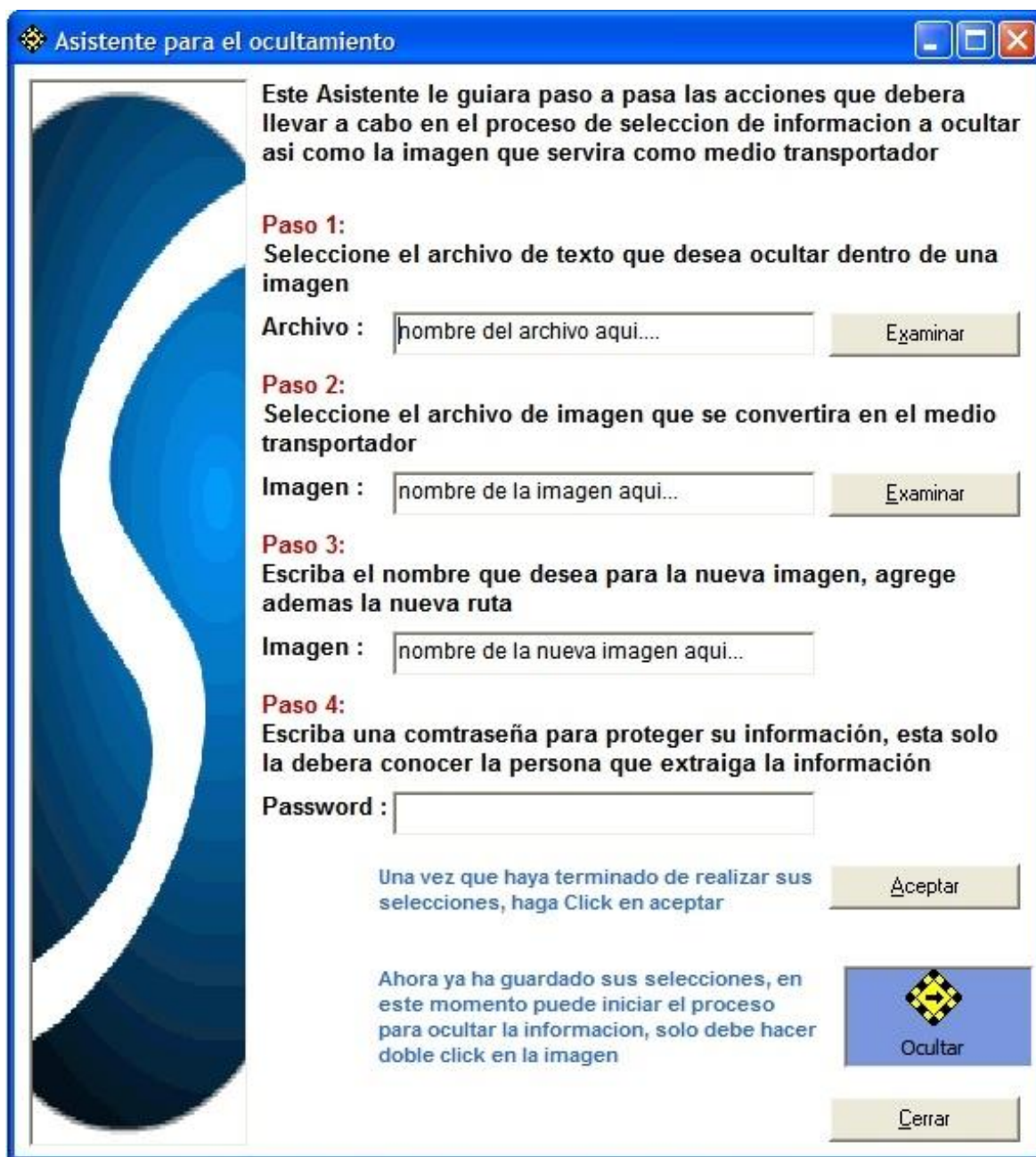
El sistema **Steganographic 1.2.27** cuenta también con una opción de referencia acerca del mismo, el cual contiene los datos de sistema como son el nombre, la versión y los sistemas operativos sobre los cuales puede funcionar.



Otra de las aplicaciones que tiene el sistema El sistema Steganographic 1.02.27 es la del explorador web con la cual podemos obtener información en línea mediante Internet, la ventana que despliega el sistema referente al explorador web es la siguiente:



El sistema cuenta también con dos asistentes que son la parte fundamental del mismo las cuales son: Asistente para ocultar y asistente para extraer



Asistente para el ocultamiento

Este Asistente le guiara paso a paso las acciones que debera llevar a cabo en el proceso de seleccion de informacion a ocultar asi como la imagen que servira como medio transportador

Paso 1:
Seleccione el archivo de texto que desea ocultar dentro de una imagen

Archivo :

Paso 2:
Seleccione el archivo de imagen que se convertira en el medio transportador

Imagen :

Paso 3:
Escriba el nombre que desea para la nueva imagen, agregue ademas la nueva ruta

Imagen :

Paso 4:
Escriba una contraseña para proteger su información, esta solo la debera conocer la persona que extraiga la información

Password :

Una vez que haya terminado de realizar sus selecciones, haga Click en aceptar

Ahora ya ha guardado sus selecciones, en este momento puede iniciar el proceso para ocultar la informacion, solo debe hacer doble click en la imagen

En la imagen anterior observamos precisamente el asistente para ocultar el cual nos pide como requisito que ingresemos el nombre y ruta del archivo de texto que deseemos ocultar, el nombre y la ruta de la imagen original y el nombre y ruta de la nueva imagen que será la que contendrá la información oculta.



La imagen de arriba es la ventana del asistente de extracción de la información de la imagen portadora. El único requisitos que esta pide es precisamente el nombre y ruta de la imagen o medio transportador que contiene la información que en un principio quisimos mantener segura.

Apéndice A.

Pseudo-código de Xtegan Ver 1.0.00 prev

```
// *****
// MAIN PRINCIPAL DE LA APLICACION XTEGAN
// VER 1.0 NOVIEMBRE DEL 2001
// *****

PRINCIPAL()
// *****
// declaracion de variables e inicializacion
// *****
    seleccion_menu;
    bandera=0;
    y,x;

// *****
// inicio del las librerias y del modo
// grafico de xtegan 1.0
// *****
    int gmode, gdriver = DETECT;
    initgraph(&gdriver,&gmode,"c:\\XTEGAN\\BG\\util");

// *****
// llamado del la pagina de presentacion
// *****
    INICIO()

// *****
// proceso de seleccion de opciones del menu
// principal.
// *****
    HACER{
        SEA (MENU())el caso{

// opcion de apertura del menu ARCHIVO
        caso 'a':
// retorno de la opcion seleccionada
            seleccion_menu=menu_archivo();

// opcion nuevo
            si(seleccion_menu=='n'){
                bandera=1;
                desplegar("Escriba el mensaje a ocultar: ");
                solicitar(cadena_mensaje_ocultar);
                seleccion_menu='b';
            }

// opcion apertura de imagen origen y destino
            si(seleccion_menu=='b'){
                char fuente[80], destino[80];
                si(bandera==1){
                    desplegar("nombre del archivo fuente(imagen): ");
                    solicitar("%s",fuente);
                    desplegar("nombre del archivo destino(imagen): ");
                    solicitar("%s",&destino);
                }
            }
        }

// *****
```

```

// llamado de la funcion ARCHIVO XTEG COPY
// es enviada la informacion de la informacion
// a ocultar, el origen y destino del medio
// transportador, incluye el proceso de codificacion
// *****
                                si(ARCHIVO_xteg_copy(fuente, destino)==0){
                                    desplegar("ocultamiento exitoso");
                                }
                                de lo contrario{
                                    desplegar(stderr,"error durante el
ocultamiento");
                                }
                                desplegar("press any key to continue...");
                                solicitar tecla();
                            }

                            bandera=0;
                        }
                    romper;

// *****
// retorno de la seleccion OPCION
// *****

                    caso 'o':
                        seleccion_menu=menu_opcion();
                        si(seleccion_menu=='e'){
                            char source[20];
                            limpiar pantalla();
                            desplegar("\nIndica el archivo fuente: ");
                            solicitar(source);
                            si(ARCHIVO_xtrac(source)==0)
                                puts(".....ok");
                            de lo contrario
                                fdesplegar(stderr,"Error durante la extraccion");
                            desplegar("\npress any key to continue...");
                            solicitar tecla();
                        }
                    romper;

// *****
// retorno de la seleccion AYUDA
// presentacion en demo de ABOUT
// *****

                    caso 'y':
                        seleccion_menu=menu_ayuda();
                        si(seleccion_menu=='d'){
                            desplegar("Instituto Politecnico Nacional");
                            desplegar("Escuela Superior de Computo");
                            desplegar("Xtegan ver 1.0 prev");
                            desplegar("Desarrollado por:");
                            desplegar("Mendoza Rodarte Saul");
                            desplegar("Reyes Figueroa Arturo");
                            desplegar("press any key to continue...");
                            solicitar tecla();
                        }
                    romper;

```

```
    }  
    delay(1000);  
  
    // *****  
    // ruptura del ciclo si es que la opcion de retorno  
    // obtenida por la seleccion es SALIDA  
    // *****  
    }mientras(seleccion_menu!='s');  
    cerrar ambiente grafico();  
}
```

Pseudo-código Librería

```
// *****
// cadena de caracteres para
// la codificación de inparamación
// *****

caracter cadena[]="abcdefghijklmnopqrstuvwxyz ";

// *****
// buffer para almacenar
// el mensaje para ocultar
// *****
caracter cadena_mensaje_ocultar[80];

// *****
// proceso que genera la ventana a partir de
// las dimensiones indicadas por el usuario
// *****
void ventana(entero x, entero y, entero color, entero tamano, entero expansion){
    para(entero incremento=0; incremento<expansion; incremento++){
        setfillstyle(1,color);
        bar(x,y-incremento,x+tamano,y+incremento);
        setfillstyle(1,7);
        bar(x+tamano+1,y+1-incremento,x+tamano+1,y+1+incremento);
        setcolor(7);
        line(x+1,y+1+incremento,x+tamano,y+1+incremento);
        delay(100);
    }
}

// *****
// proceso que genera el boton a partir de
// las dimensiones indicadas por el usuario
// *****

void boton(entero x, entero y, entero color, entero tamano, entero expansion){
    para(entero incremento=0; incremento<expansion; incremento++){
        setfillstyle(1,color);
        bar(x,y-incremento,x+tamano,y+incremento);
        setfillstyle(1,7);
        bar(x+tamano+1,y+1-incremento,x+tamano+1,y+1+incremento);
        setcolor(7);
        line(x+1,y+1+incremento,x+tamano,y+1+incremento);
        delay(100);
    }
}

// *****
// llamado del main a la función inicio para
// presentación de Xtegan
// *****
void inicio(void){
    setbkcolor(8);
    settextstyle(0,0,1);
    setcolor(15);
```

```

desplegar(20,20,"Instituto Polit,cnico Nacional");
desplegar(20,30,"Escuela Superior de C&mputo");
desplegar(20,40,"XTEG ver 1.0 prev");
desplegar(20,50,"Mendoza Rodarte Saul");
desplegar(20,60,"Reyes Figueroa arturo");
desplegar(20,70,"Copyright (c) 2001");
delay(1500);
setcolor(15);
rectangle(100,300,525,320);
setcolor(1);
para(entero avance=0;avance<424;avance++){
    gotoxy(28,18);
    prenterof("cargando el sistema (%d %)",avance/4-5);
    line(101+avance,301,101+avance,319);
    delay(3);
}
delay(1500);
setfillstyle(1,8);
bar(100,200,525,320);
boton(500,435,4,100,10);
setcolor(15);
desplegar(514,432,"Continuar");
esperar tecla();
}

```

```

// *****
// presentacion de menu principal para seleccion
// de opciones de Xtegan
// *****
caracter menu(void){
    caracter opc='X';
    setbkcolor(9);
    setfillstyle(1,8);
    bar(10,10,getmaxx()-10,getmaxy()-10);
    setcolor(7);
    line(11,getmaxy()-9,getmaxx()-9,getmaxy()-9);
    line(getmaxx()-9,11,getmaxx()-9,getmaxy()-9);
    setfillstyle(1,7);
    bar(12,12,getmaxx()-12,23);
    setcolor(8);
    line(65,22,getmaxx()-13,22);
    setcolor(4);
    desplegar(15,15,"Xtegan");
    boton(12,35,4,614,6);
    setcolor(15);
    desplegar(15,32,"Archivo Opciones aYuda");
    opc=esperar tecla();

    regresar(opc);
}

```

```

// *****
// *****
// codigo de la funcion generadora de la codsiicacion
// recibe origen y destino del medio transportador
// *****
// *****

entero ARCHIVO_xteg_copy(caracter *oldname, caracter *newname){
    ARCHIVO *fold, *fnew;
    entero c;
    entero x=0;
    entero y;
    entero contador=0;
    si((fold=abrirArchivo(oldname, "rb"))==NULL)
        regresar -1;
    si((fnew=abrirArchivo(newname, "wb"))==NULL){
        cerrarArchivo (fold);
        regresar -1;
    }
    mientras(1){
        c=fgetc(fold);
        contador++;
        si(contador==2000){
            si(x<80){
                para(y=0;y<29;y++){
                    si(cadena_mensaje_ocultar[x]==cadena[y]){
                        c=y;
                    }
                }
                x++;
            }
            contador=0;
        }

        si(!feof(fold))
            fputc(c,fnew);
        else
            break;
    }
    cerrarArchivo(fnew);
    cerrarArchivo(fold);
    regresar 0;
}

// *****
// *****
// funcion para extraer el mensaje oculto de una imagen
// de xtegan, solo para imagenes tratadas con xtegan
// *****
// *****

entero ARCHIVO_xtrac(caracter *oldname1){
    ARCHIVO *fold1;
    entero c;
    entero contador=0;
    si((fold1=abrirArchivo(oldname1, "rb"))==NULL)
        regresar -1;

```

```

    mientras(1){
        c=fgetc(fold1);
        contador++;
        si(contador==2000){
            si(c>29)
                break;
            else
                prenterof("%c",cadena[c]);
            contador=0;
        }
        sifeof(fold1))
            break;
    }

    cerrarArchivo(fold1);
    regresar 0;
}

```

```

caracter menu_archivo(void){
    entero y;
    caracter opc_a;
    para(y=1;y<75;y++){
        setcolor(4);
        line(12,43+y,130,43+y);
        delay(3);
    }
    setcolor(15);
    desplegar(15,45,"Nuevo");
    desplegar(15,60,"* aBrir imagen");
    desplegar(15,75,"* salVar");
    desplegar(15,90,"* salvar Como");
    desplegar(15,105,"Salir");
    opc_a=esperar tecla();
    para(y=120;y>43;y--){
        setcolor(8);
        line(12,y,280,y);
        delay(3);
    }
    regresar(opc_a);
}

```

```

caracter menu_opcion(void){
    entero y;
    caracter opc_o;
    para(y=1;y<15;y++){
        setcolor(4);
        line(85,43+y,200,43+y);
        delay(3);
    }
    setcolor(15);
    desplegar(88,45,"Extraer");
    opc_o=esperar tecla();
    para(y=120;y>43;y--){
        setcolor(8);
        line(12,y,280,y);
        delay(3);
    }
}

```

```

        regresar(opc_o);
    }

    caracter menu_ayuda(void){
        entero y;
        caracter opc_y;
        para(y=1;y<15;y++){
            setcolor(4);
            line(165,43+y,265,43+y);
            delay(3);
        }
        setcolor(15);
        desplegar(167,45,"acerca De...");
        opc_y=esperar tecla();
        para(y=120;y>43;y--){
            setcolor(8);
            line(12,y,280,y);
            delay(3);
        }
        regresar(opc_y);
    }
}

```

Apéndice B.

Código Fuente de Xtegan 1.0.00 prev

```
#include <stdio.h>
#include <graphics.h>
#include <conio.h>
#include <dos.h>
#include <string.h>
#include "c:\\XTEGAN\\milib.h"

void main(void){
    char seleccion_menu;
    int flag=0;
    int y,x;
    int gmode, gdriver = DETECT;
    initgraph(&gdriver,&gmode,"c:\\XTEGAN\\BGI\\util");

    inicio();

    do{
        switch(menu()){
            case 'a':
                seleccion_menu=menu_archivo();
                if(seleccion_menu=='n'){
                    flag=1;
                    gotoxy(10,5);
                    printf("Escriba el mensaje a ocultar: ");
                    gotoxy(10,6);
                    gets(cadena_mensaje_ocultar);
                    seleccion_menu='b';
                }
                if(seleccion_menu=='b'){
                    char fuente[80], destino[80];
                    if(flag==1){
                        gotoxy(10,10);
                        printf("nombre del archivo fuente(imagen): ");
                        scanf("%s",fuente);
                        gotoxy(10,12);
                        printf("nombre del archivo destino(imagen): ");
                        scanf("%s",&destino);
                        if(file_xteg_copy(fuente, destino)==0){
                            gotoxy(10,14);
                            printf("ocultamiento exitoso");
                        }
                        else{
                            gotoxy(10,14);
                            fprintf(stderr,"error durante el
ocultamiento");
                        }
                    }
                    gotoxy(10,15);
                    printf("press any key to continue...");
                    getch();
                }

                flag=0;
                setfillstyle(1,9);
                bar(0,0,getmaxx(),getmaxy());
            }
        }
    }
}
```

```

        }
        break;

    case 'o':
        seleccion_menu=menu_opcion();
        if(seleccion_menu=='e'){
            char source[20];
            clrscr();
            printf("\nIndica el archivo fuente: ");
            gets(source);
            if(file_xtrac(source)==0)
                puts(".....ok");
            else
                fprintf(stderr,"Error durante la extraccion");
            printf("\npress any key to continue...");
            getch();
            setfillstyle(1,9);
            bar(0,0,getmaxx(),getmaxy());
        }
        break;
    case 'y':
        seleccion_menu=menu_ayuda();
        if(seleccion_menu=='d'){
            gotoxy(10,10); printf("Instituto Politecnico Nacional");
            gotoxy(10,11); printf("Escuela Superior de Computo");
            gotoxy(10,13); printf("Xtegan ver 1.0 prev");
            gotoxy(10,14); printf("Desarrollado por:");
            gotoxy(10,15); printf("Mendoza Rodarte Saul");
            gotoxy(10,16); printf("Reyes Figueroa Arturo");
            gotoxy(10,18); printf("press any key to continue...");
            getch();
        }
        break;
    }
    delay(1000);
}while(seleccion_menu!='s');
closegraph();
}

```

Codigo Fuente de librería Xtegan 1.0.00 prev

```

char cadena[]="abcdefghijklmnopqrstuvwxyz? ";

char cadena_mensaje_ocultar[80];

void ventana(int x, int y,int color, int tamano, int expansion){
    for(int incremento=0;incremento<expansion;incremento++){
        setfillstyle(1,color);
        bar(x,y-incremento,x+tamano,y+incremento);
        setfillstyle(1,7);
        bar(x+tamano+1,y+1-incremento,x+tamano+1,y+1+incremento);
        setcolor(7);
        line(x+1,y+1+incremento,x+tamano,y+1+incremento);
        delay(100);
    }
}

```

```

void boton(int x, int y, int color, int tamano, int expansion){
    for(int incremento=0; incremento<expansion; incremento++){
        setfillstyle(1,color);
        bar(x,y-incremento,x+tamano,y+incremento);
        setfillstyle(1,7);
        bar(x+tamano+1,y+1-incremento,x+tamano+1,y+1+incremento);
        setcolor(7);
        line(x+1,y+1+incremento,x+tamano,y+1+incremento);
        delay(100);
    }
}

void inicio(void){
    setbkcolor(8);
    settextstyle(0,0,1);
    setcolor(15);
    outtextxy(20,20,"Instituto Polit,cnico Nacional");
    outtextxy(20,30,"Escuela Superior de C#mputo");
    outtextxy(20,40,"XTEG ver 1.0 prev");
    outtextxy(20,50,"Mendoza Rodarte Saul");
    outtextxy(20,60,"Reyes Figueroa arturo");
    outtextxy(20,70,"Copyright (c) 2001");
    delay(1500);
    setcolor(15);
    rectangle(100,300,525,320);
    setcolor(1);
    for(int avance=0; avance<424; avance++){
        gotoxy(28,18);
        printf("cargando el sistema (%d %)",avance/4-5);
        line(101+avance,301,101+avance,319);
        delay(3);
    }
    delay(1500);
    setfillstyle(1,8);
    bar(100,200,525,320);
    boton(500,435,4,100,10);
    setcolor(15);
    outtextxy(514,432,"Continuar");
    getch();
}

char menu(void){
    char opc='X';
    setbkcolor(9);
    setfillstyle(1,8);
    bar(10,10,getmaxx()-10,getmaxy()-10);
    setcolor(7);
    line(11,getmaxy()-9,getmaxx()-9,getmaxy()-9);
    line(getmaxx()-9,11,getmaxx()-9,getmaxy()-9);
    setfillstyle(1,7);
    bar(12,12,getmaxx()-12,23);
    setcolor(8);
    line(65,22,getmaxx()-13,22);
    setcolor(4);
    outtextxy(15,15,"Xtegan");
    boton(12,35,4,614,6);
    setcolor(15);
    outtextxy(15,32,"Archivo  Opciones  aYuda");
}

```

```

        opc=getch();
        return(opc);
    }

int file_xteg_copy(char *oldname, char *newname){
    FILE *fold, *fnew;
    int c;
    int x=0;
    int y;
    int contador=0;
    if((fold=fopen(oldname, "rb"))==NULL)
        return -1;
    if((fnew=fopen(newname, "wb"))==NULL){
        fclose (fold);
        return -1;
    }
    while(1){
        c=fgetc(fold);
        contador++;
        if(contador==2000){
            if(x<80){
                for(y=0;y<29;y++){
                    if(cadena_mensaje_ocultar[x]==cadena[y]){
                        c=y;
                    }
                }
                x++;
            }
            contador=0;
        }

        if(!feof(fold))
            fputc(c,fnew);
        else
            break;
    }
    fclose(fnew);
    fclose(fold);
    return 0;
}

int file_xtrac(char *oldname1){
    FILE *fold1;
    int c;
    int contador=0;
    if((fold1=fopen(oldname1, "rb"))==NULL)
        return -1;
    while(1){
        c=fgetc(fold1);
        contador++;
        if(contador==2000){
            if(c>29)
                break;
            else
                printf("%c",cadena[c]);
        }
    }
}

```

```

        contador=0;
    }
    if(feof(fold1))
        break;
}

fclose(fold1);
return 0;
}

char menu_archivo(void){
    int y;
    char opc_a;
    for(y=1;y<75;y++){
        setcolor(4);
        line(12,43+y,130,43+y);
        delay(3);
    }
    setcolor(15);
    outtextxy(15,45,"Nuevo");
    outtextxy(15,60,"* aBrir imagen");
    outtextxy(15,75,"* salVar");
    outtextxy(15,90,"* salvar Como");
    outtextxy(15,105,"Salir");
    opc_a=getch();
    for(y=120;y>43;y--){
        setcolor(8);
        line(12,y,280,y);
        delay(3);
    }
    return(opc_a);
}

char menu_opcion(void){
    int y;
    char opc_o;
    for(y=1;y<15;y++){
        setcolor(4);
        line(85,43+y,200,43+y);
        delay(3);
    }
    setcolor(15);
    outtextxy(88,45,"Extraer");
    opc_o=getch();
    for(y=120;y>43;y--){
        setcolor(8);
        line(12,y,280,y);
        delay(3);
    }
    return(opc_o);
}

char menu_ayuda(void){
    int y;
    char opc_y;
    for(y=1;y<15;y++){

```

```
        setcolor(4);
        line(165,43+y,265,43+y);
        delay(3);
    }
    setcolor(15);
    outtextxy(167,45,"acerca De...");
    opc_y=getch();
    for(y=120;y>43;y--){
        setcolor(8);
        line(12,y,280,y);
        delay(3);
    }
    return(opc_y);
}
```

Apéndice C

Código fuente de KernelS

```
#include <stdio.h>
#include <conio.h>
#include <string.h>

char cadena[80];
int tamano;
char cadena_auxiliar[40];

// *****
// KERNELS es el proceso principal para el ocultamiento
// de informacion entro de una imagen
// solicita el archivo de texto, la imagen y el
// nombre de la imagen que se generara
// apartir de steganographic
// *****

int kernelS(char *Atexto, char *Aimagen, char *Atransporte)
{
    FILE *ftexto, *fimagen, *ftrans;
    FILE *auxiliar;

    int ct;
    int cp;
    int y;
    int contador=0;

    printf("\nKernelS© es parte de Steganographic 1.2.27");
    printf("\nCopyright Derechos Reservados 2002");
    printf("\nEscuela Superior de Computo");
    printf("\nInstituto Politecnico Nacional\n");
    printf("\nNota: este programa oculta informacion en una imagen,");
    printf("\n    por cuestiones de seguridad la informacion a desplegar");
    printf("\n    solo se mostrara en pantalla, de donde podra usar los metodos");
    printf("\n    de edicion de la linea de comandos de Windows...");
    getch();

    // *****
    // apertura del archivo de texto
    // *****

    if((ftexto=fopen(Atexto,"rb"))==NULL){
        printf("\nEl archivo1 %s no fue encontrado, verifique la ruta",Atexto);
        return -1;
    }
    else{
        // *****
        // apertura del archivo de imagen
        // *****

        if((fimagen=fopen(Aimagen,"rb"))==NULL){
            fclose (ftexto);
            printf("\nEl archivo2 %s no fue encontrado verifique la ruta",Aimagen);
            return -1;
        }
    }
}
```

```

        else{
// *****
// apertura del archivo de nuevo de imagen
// *****
            if((ftrans=fopen(Atransporte,"wb"))==NULL){
                fclose (ftexto);
                fclose (fimagen);
                printf("\nEl archivo3 %s no fue encontrado verifique la
ruta",Atransporte);
                return -1;
            }
        }
        if((auxiliar=fopen("c:\\archivos de
programa\\steganographic\\codigoSE.sys.txt","r"))==NULL){
            printf("Error 512, no se encontro el archivo de codigos");
            return -1;
        }
        else{
            fscanf(auxiliar,"%s",cadena_auxiliar);
            tamano=strlen(cadena_auxiliar);
        }
// *****
// proceso de ocultamiento de informacion
// dependiendo de la dencidad para ocultar
// contador es el indice que determina donde
// llevar a cabo el ocultamiento de datos
// a nivel binario
// *****
        while(1)
        {
            cp=fgetc(fimagen);
            contador++;
            if(contador==2000){
                if(!feof(ftexto)){
                    ct=fgetc(ftexto);
                    for(y=0;y<tamano+1;y++){
                        if((ct == cadena_auxiliar[y]) || (ct == ' ')){
                            cp=y;
                        }
                    }
                }
                contador=0;
            }
            if(!feof(fimagen))
                fputc(cp,ftrans);
            else
                break;
        }
        printf("\n\n");
    }
    return 0;
}

// *****
// MAIN de KernelS
// *****

```

```

void main(void){
    FILE *auxiliar;
    FILE *archivo1;
    FILE *archivo2;
    FILE *archivo3;

    int cArchivo;
    int contador1=1;
    int contador2=0;

    char imagen[40], transporte[40];

    int flag=0;
    char nombreArchivoTexto[80];

    // *****
    // apertura del archivo de intercambio
    // canal de comunicacion entre la aplicacion
    // y el componenete OLE
    // *****
    if((auxiliar=fopen("c:\\archivos de programa\\steganographic\\kerstg.dat","r"))==NULL)
        printf("\nArgumentos no validos, verifique.");
    else{
        fscanf(auxiliar,"%s",nombreArchivoTexto);
        fscanf(auxiliar,"%s",&imagen);
        fscanf(auxiliar,"%s",&transporte);
    }
    fcloseall();

    // *****
    // apertura del archivo de texto
    // determinacion del formato del archivo
    // y su posterior cambio a ascci
    // *****
    if((archivo1=fopen(nombreArchivoTexto,"r"))==NULL)
        printf("\nEl archivo %s no fue encontrado",nombreArchivoTexto);
    else{
        cArchivo=fgetc(archivo1);
        if(cArchivo == 123)
            flag=1;
        while(1){
            cArchivo=fgetc(archivo1);
            contador1++;
            iffeof(archivo1)
                break;
        }
    }
    fcloseall();

    if(flag==1){
        archivo2=fopen("c:\\archivos de programa\\steganographic\\auxiliar.stg","w");

        if((archivo1=fopen(nombreArchivoTexto,"r"))==NULL)
            printf("\nEl archivo %s no fue encontrado",nombreArchivoTexto);
        else{
            while(1){
                cArchivo=fgetc(archivo1);
                contador2++;
            }
        }
    }
}

```

```

                                if(!feof(archivo1)){
                                    if(contador2>115)
                                        if(contador2<(contador1-8))
                                            fputc(cArchivo,archivo2);
                                }
                                else
                                    break;
                            }
                        }
                    }
                }
            }
        }
        fcloseall();

        if(flag==0){
            archivo2=fopen("c:\\archivos de programa\\steganographic\\auxiliar.stg","w");

            if((archivo1=fopen(nombreArchivoTexto,"r"))==NULL)
                printf("\nEl archivo %s no fue encontrado",nombreArchivoTexto);
            else{
                while(1){
                    cArchivo=fgetc(archivo1);
                    if(!feof(archivo1))
                        fputc(cArchivo,archivo2);
                    else
                        break;
                }
            }
        }
        fcloseall();
        char password[20];
        archivo2=fopen("c:\\archivos de programa\\steganographic\\auxiliar.stg","r");
        archivo3=fopen("c:\\archivos de programa\\steganographic\\auxiliar2.stg","w");
        printf("\n\nIngresa password: ");
        scanf("%s",&password);
        fprintf(archivo3,"%s ",password);
        while(1){
            cArchivo=fgetc(archivo2);
            if(feof(archivo2))
                break;
            fputc(cArchivo,archivo3);
        }
        fcloseall();
        // *****
        // llamada al kernel del sistema
        // *****
        kernelS("c:\\archivos de programa\\steganographic\\auxiliar2.stg", imagen, transporte);
    }
}

```

Apendice D

Codigo Fuente de KernelE

```
#include <stdio.h>
#include <conio.h>
#include <string.h>

// *****
// declaracion de variables globales y de intercambio
// de informacion entre el main y kernelE
// *****
char cadena[80];
int tamano, longitud;
char cadena_auxiliar[40];

// *****
// variable que almacenara el password del usuario para
// el proceso de extraccion
// *****
char password[20];
char passaux[20];

int contador2=0;

// *****
// KernelE ver 1.2.27 proceso en el cual se extrae
// la informacion oculta en una imagen
// el usuario debera proporcionar el password
// *****

int kernelE(char *oldname1){
    FILE *fold1, *auxiliar;
    int c;
    int contador=0;

    // *****
    // apertura del archivo de intercambio de informacion
    // *****

    if((auxiliar=fopen("c:\\archivos de
programa\\steganographic\\codigoSE.sys.txt","r"))==NULL){
        printf("Error 512, no se encontro el archivo de codigos");
        return -1;
    }
    else{
        fscanf(auxiliar,"%s",cadena_auxiliar);
        tamano=strlen(cadena_auxiliar);
    }

    // *****
    // apertura del archivo de imagen a nivel binario
    // *****

    if((fold1=fopen(oldname1, "rb"))==NULL)
        return -1;
    // proceso de extraccion de informacion de la imagen
    while(1){
```

```

        c=fgetc(fold1);
        contador++;

// *****
// contador es el indice de dencidad para el ocultamiento
// de informacion en la imagen
// *****

        if(contador==2000){
            if(contador2<longitud)

// *****
// verificacion de password contenido en la imagen
// y el proporcionado por el usuario.
// *****

                passaux[contador2]=cadena_auxiliar[c];
                if(contador2==longitud){
                    if(strcmp(password,passaux))
                        break;
                }
                contador2++;

                if(c>tamano+1)
                    break;
                else{
                    if(contador2>longitud+1)
                        printf("%c",cadena_auxiliar[c]);
                }
                contador=0;
            }
            if(feof(fold1))
                break;
        }
        fclose(fold1);
        return 0;
    }

// MAIN del KernelE

void main(void){
    FILE *kernel;
    char transporte[40];
    printf("KernelE© es parte de Steganographic 1.2.27");
    printf("\nCopyright Derechos Reservados 2002");
    printf("\nEscuela Superior de Computo");
    printf("\nInstituto Politecnico Nacional\n");
    printf("\nNota: por cuestiones de seguridad la informacion a desplegar");
    printf("\n    solo se mostrara en pantalla, de donde podra usar los metodos");
    printf("\n    de edicion de la linea de comandos de Windows...");
    printf("\nPress any key to continue...");
    getch();
    printf("\n\n");

// *****
// ingreso del password por el usuario
// *****

```

```
printf("Ingrese el Password: ");
scanf("%s",&password);
longitud=strlen(password);
if((kernel=fopen("c:\\archivos de programa\\steganographic\\kerstg.dat","r"))==NULL){
    printf("Error, 512 no se encontro el archivo de datos");
}
else{
    fscanf(kernel,"%s",&transporte);
    kernelE(transporte);
    printf("\n\n");
}
getch();
fcloseall();
}
```

Apéndice E

Código Fuente de Steganographic

Código Modulo del sistema

```
Public fMainForm As frmMain

Sub Main()
    Dim fLogin As New frmLogin
    fLogin.Show vbModal
    If Not fLogin.OK Then
        'Fallo al iniciar la sesión, se sale de la aplicación
        End
    End If
    Unload fLogin

    frmSplash.Show
    frmSplash.Refresh
    Set fMainForm = New frmMain
    Load fMainForm
    Unload frmSplash

    fMainForm.Show
End Sub
```

Código de Formulario “Acerca De”

```
' Opciones de seguridad de clave del Registro...
Const KEY_ALL_ACCESS = &H2003F

' Tipos ROOT de claves del Registro...
Const HKEY_LOCAL_MACHINE = &H80000002
Const ERROR_SUCCESS = 0
Const REG_SZ = 1           ' cadena terminada en valor nulo Unicode
Const REG_DWORD = 4        ' número de 32 bits

Const gREGKEYSYSINFOLOC = "SOFTWARE\Microsoft\Shared Tools Location"
Const gREGVALSYSINFOLOC = "MSINFO"
Const gREGKEYSYSINFO = "SOFTWARE\Microsoft\Shared Tools\MSINFO"
Const gREGVALSYSINFO = "PATH"

Private Declare Function RegOpenKeyEx Lib "advapi32" Alias "RegOpenKeyExA" (ByVal hKey As Long, ByVal lpSubKey As String, ByVal ulOptions As Long, ByVal samDesired As Long, ByRef phkResult As Long) As Long

Private Declare Function RegQueryValueEx Lib "advapi32" Alias "RegQueryValueExA" (ByVal hKey As Long, ByVal lpValueName As String, ByVal lpReserved As Long, ByRef lpType As Long, ByVal lpData As String, ByRef lpcbData As Long) As Long

Private Declare Function RegCloseKey Lib "advapi32" (ByVal hKey As Long) As Long

Private Sub Form_Load()
    lblVersion.Caption = "Versión " & App.Major & "." & App.Minor & "." & App.Revision
    lblTitle.Caption = App.Title
End Sub

Private Sub cmdSysInfo_Click()
    Call StartSysInfo
```

```

End Sub

Private Sub cmdOK_Click()
    Unload Me
End Sub

Public Sub StartSysInfo()
    On Error GoTo SysInfoErr

    Dim rc As Long
    Dim SysInfoPath As String

    If GetKeyValue(HKEY_LOCAL_MACHINE, gREGKEYSYSINFO, gREGVALSYSINFO, SysInfoPath) Then
        ElseIf GetKeyValue(HKEY_LOCAL_MACHINE, gREGKEYSYSINFOLOC, gREGVALSYSINFOLOC, SysInfoPath) Then
            If (Dir(SysInfoPath & "\MSINFO32.EXE") <> "") Then
                SysInfoPath = SysInfoPath & "\MSINFO32.EXE"
            Else
                GoTo SysInfoErr
            End If
        Else
            GoTo SysInfoErr
        End If

        Call Shell(SysInfoPath, vbNormalFocus)

        Exit Sub
    SysInfoErr:
        MsgBox "La información del sistema no está disponible en este momento", vbOKOnly
End Sub

Public Function GetKeyValue(KeyRoot As Long, KeyName As String, SubKeyRef As String, ByRef KeyVal As String) As Boolean
    Dim i As Long                ' Contador de bucle
    Dim rc As Long                ' Código de retorno
    Dim hKey As Long              ' Controlador a una clave de Registro abierta
    Dim hDepth As Long            '
    Dim KeyValType As Long         ' Tipo de datos de una clave del Registro
    Dim tmpVal As String           ' Almacenamiento temporal para un valor de clave del Registro
    Dim KeyValSize As Long         ' Tamaño de variable de clave del Registro
    '-----
    ' Abrir RegKey bajo KeyRoot {HKEY_LOCAL_MACHINE...}
    '-----
    rc = RegOpenKeyEx(KeyRoot, KeyName, 0, KEY_ALL_ACCESS, hKey) ' Abrir la clave del Registro

    If (rc <> ERROR_SUCCESS) Then GoTo GetKeyError                ' Controlar error...

    tmpVal = String$(1024, 0)    ' Asignar espacio de variable
    KeyValSize = 1024            ' Marcar tamaño de variable

    '-----
    ' Obtener valor de clave del Registro...

```

```

'-----
rc = RegQueryValueEx(hKey, SubKeyRef, 0, KeyValType, tmpVal, KeyValSize) ' Get/Create
Key Value

If (rc <> ERROR_SUCCESS) Then GoTo GetKeyError      ' Controlar errores

tmpVal = VBA.Left(tmpVal, InStr(tmpVal, VBA.Chr(0)) - 1)
'-----
' Determinar el tipo de valor de clave para conversión...
'-----
Select Case KeyValType      ' Buscar tipos de datos...
Case REG_SZ                ' Tipo de datos String de clave del Registro
    KeyVal = tmpVal        ' Copiar valor String
Case REG_DWORD             ' Tipo de datos Double Word de clave del Registro
    For i = Len(tmpVal) To 1 Step -1
        ' Convertir cada bit
        KeyVal = KeyVal + Hex(Asc(Mid(tmpVal, i, 1)))
        ' Generar valor carácter a carácter
    Next
    KeyVal = Format$("&h" + KeyVal)
    ' Convertir Double Word a String
End Select

GetKeyValue = True          ' Operación realizada correctamente
rc = RegCloseKey(hKey)     ' Cerrar clave del Registro
Exit Function              ' Salir

GetKeyError:               ' Limpiar después de que se produzca un error...
KeyVal = ""                ' Establecer el valor de retonor a la cadena vacía
GetKeyValue = False        ' La operación no se ha realizado correctamente
rc = RegCloseKey(hKey)     ' Cerrar clave del Registro
End Function
Private Sub Text1_Change()

End Sub

```

Código del Asistente de ocultamiento.

```

Private Sub Command1_Click()
    dlgArchivoTxt.ShowOpen
    txtNombreAr.Text = dlgArchivoTxt.FileName
End Sub

Private Sub Command2_Click()
    dlgArchivoTxt.Filter = "Archivo de mapa de bits (*.bmp)|*.bmp"
    dlgArchivoTxt.ShowOpen
    txtNombreImagen.Text = dlgArchivoTxt.FileName
End Sub

Private Sub Command3_Click()
    Open "C:\archivos de Programa\Steganographic\kerstg.dat" For Output As #1
    Print #1, txtNombreAr.Text
    Print #1, txtNombreImagen.Text
    Print #1, txtNombreTransporte.Text
    Print #1, txtPass.Text

```

```

        Close #1
        MsgBox "Con la información proporcionada se a construido un canal de comunicacion..."
    End Sub

```

```

Private Sub ProgressBar1_MouseDown(Button As Integer, Shift As Integer, X As Single, Y As Single)

```

```

End Sub

```

```

Private Sub Command4_Click()
    Me.Hide
End Sub

```

Código del Asistente de Extracción

```

Private Sub Command1_Click()
    dlgArchivoTxt2.Filter = "Archivo de mapa de bits (*.bmp)|*.bmp"
    dlgArchivoTxt2.ShowOpen
    Text1.Text = dlgArchivoTxt2.FileName
End Sub

```

```

Private Sub Command2_Click()
    Me.Hide
End Sub

```

```

Private Sub Command3_Click()
    Open "c:\Archivos de Programa\Steganographic\kerstg.dat" For Output As #2
    Print #2, Text1.Text
    Print #2, Text2.Text
    Close #2
    MsgBox "La información proporcionada a sido verificada"
End Sub

```

```

Private Sub Label2_Click()

```

```

End Sub

```

Código del comando Nuevo Archivo

```

Private Sub Form_Load()
    Form_Resize
End Sub

```

```

Private Sub Form_Resize()
    On Error Resume Next
    rtfText.Move 100, 100, Me.ScaleWidth - 200, Me.ScaleHeight - 200
    rtfText.RightMargin = rtfText.Width - 400
End Sub

```

Codigo del Browser de Steganographic

```

Public StartingAddress As String
Dim mbDontNavigateNow As Boolean
Private Sub Form_Load()
    On Error Resume Next
    Me.Show
    tbToolBar.Refresh

```

```

Form_Resize

cboAddress.Move 50, lblAddress.Top + lblAddress.Height + 15

If Len(StartingAddress) > 0 Then
    cboAddress.Text = StartingAddress
    cboAddress.AddItem cboAddress.Text
    timTimer.Enabled = True
    brwWebBrowser.Navigate StartingAddress
End If

End Sub

Private Sub brwWebBrowser_DownloadComplete()
    On Error Resume Next
    Me.Caption = brwWebBrowser.LocationName
End Sub

Private Sub brwWebBrowser_NavigateComplete2(ByVal pDisp As Object, URL As Variant)
    On Error Resume Next
    Dim i As Integer
    Dim bFound As Boolean
    Me.Caption = brwWebBrowser.LocationName
    For i = 0 To cboAddress.ListCount - 1
        If cboAddress.List(i) = brwWebBrowser.LocationURL Then
            bFound = True
            Exit For
        End If
    Next i
    mbDontNavigateNow = True
    If bFound Then
        cboAddress.RemoveItem i
    End If
    cboAddress.AddItem brwWebBrowser.LocationURL, 0
    cboAddress.ListIndex = 0
    mbDontNavigateNow = False
End Sub

Private Sub cboAddress_Click()
    If mbDontNavigateNow Then Exit Sub
    timTimer.Enabled = True
    brwWebBrowser.Navigate cboAddress.Text
End Sub

Private Sub cboAddress_KeyPress(KeyAscii As Integer)
    On Error Resume Next
    If KeyAscii = vbKeyReturn Then
        cboAddress_Click
    End If
End Sub

Private Sub Form_Resize()
    On Error Resume Next
    cboAddress.Width = Me.ScaleWidth - 100
    brwWebBrowser.Width = Me.ScaleWidth - 100

```

```

        brwWebBrowser.Height = Me.ScaleHeight - (picAddress.Top + picAddress.Height) - 100
    End Sub

```

```

Private Sub timTimer_Timer()
    If brwWebBrowser.Busy = False Then
        timTimer.Enabled = False
        Me.Caption = brwWebBrowser.LocationName
    Else
        Me.Caption = "Trabajando..."
    End If
End Sub

```

```

Private Sub tbToolBar_ButtonClick(ByVal Button As Button)
    On Error Resume Next

```

```

    timTimer.Enabled = True

```

```

    Select Case Button.Key
        Case "Atrás"
            brwWebBrowser.GoBack
        Case "Adelante"
            brwWebBrowser.GoForward
        Case "Actualizar"
            brwWebBrowser.Refresh
        Case "Inicio"
            brwWebBrowser.GoHome
        Case "Búsqueda"
            brwWebBrowser.GoSearch
        Case "Detener"
            timTimer.Enabled = False
            brwWebBrowser.Stop
            Me.Caption = brwWebBrowser.LocationName
    End Select

```

```

End Sub

```

Código de Inicio de Sesión

```

Private Declare Function GetUserName Lib "advapi32.dll" Alias "GetUserNameA" (ByVal lpbuffer
As String, nSize As Long) As Long

```

```

Public OK As Boolean
Private Sub Form_Load()
    Dim sBuffer As String
    Dim ISize As Long

    sBuffer = Space$(255)
    ISize = Len(sBuffer)
    Call GetUserName(sBuffer, ISize)
    If ISize > 0 Then
        txtUserName.Text = Left$(sBuffer, ISize)
    Else

```

```

        txtUserName.Text = vbNullString
    End If
End Sub

```

```

Private Sub cmdCancel_Click()
    OK = False
    Me.Hide
End Sub

```

```

Private Sub cmdOK_Click()
    If txtPassword.Text = "" Then
        OK = True
        Me.Hide
    Else
        MsgBox "La contraseña no es válida; vuelva a intentarlo", , "Inicio de sesión"
        txtPassword.SetFocus
        txtPassword.SelStart = 0
        txtPassword.SelLength = Len(txtPassword.Text)
    End If
End Sub

```

```

Private Sub txtUserName_Change()

End Sub

```

Código del menu principal

```

Private Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long,
ByVal wMsg As Long, ByVal wParam As Long, ByVal lParam As Any) As Long
Const EM_UNDO = &HC7
Private Declare Function OSWinHelp% Lib "user32" Alias "WinHelpA" (ByVal hwnd%, ByVal
HelpFile$, ByVal wCommand%, dwData As Any)

```

```

Private Sub MDIForm_Load()
    Me.Left = GetSetting(App.Title, "Settings", "MainLeft", 1000)
    Me.Top = GetSetting(App.Title, "Settings", "MainTop", 1000)
    Me.Width = GetSetting(App.Title, "Settings", "MainWidth", 6500)
    Me.Height = GetSetting(App.Title, "Settings", "MainHeight", 6500)
    LoadNewDoc
End Sub

```

```

Private Sub LoadNewDoc()
    Static IDocumentCount As Long
    Dim frmD As frmDocument
    IDocumentCount = IDocumentCount + 1
    Set frmD = New frmDocument
    frmD.Caption = "Document " & IDocumentCount
    frmD.Show
End Sub

```

```

Private Sub MDIForm_Unload(Cancel As Integer)
    If Me.WindowState <> vbMinimized Then
        SaveSetting App.Title, "Settings", "MainLeft", Me.Left
    End If
End Sub

```

```

        SaveSetting App.Title, "Settings", "MainTop", Me.Top
        SaveSetting App.Title, "Settings", "MainWidth", Me.Width
        SaveSetting App.Title, "Settings", "MainHeight", Me.Height
    End If
End Sub

Private Sub mnuAsistente_Click()
    frmAsistente.Show vbModal, Me
End Sub

Private Sub tbToolBar_ButtonClick(ByVal Button As MSComCtlLib.Button)
    On Error Resume Next
    Select Case Button.Key
        Case "Nuevo"
            LoadNewDoc
        Case "Abrir"
            mnuFileOpen_Click
        Case "Guardar"
            mnuFileSave_Click
        Case "Imprimir"
            mnuFilePrint_Click
        Case "Cortar"
            mnuEditCut_Click
        Case "Copiar"
            mnuEditCopy_Click
        Case "Pegar"
            mnuEditPaste_Click
    End Select
End Sub

Private Sub mnuHelpAbout_Click()
    frmAbout.Show vbModal, Me
End Sub

Private Sub mnuHelpSearchForHelpOn_Click()
    Dim nRet As Integer
    If Len(App.HelpFile) = 0 Then
        MsgBox "No se puede mostrar el contenido de la Ayuda. No hay Ayuda asociada a este proyecto.", vbInformation, Me.Caption
    Else
        On Error Resume Next
        nRet = OSWinHelp(Me.hwnd, App.HelpFile, 261, 0)
        If Err Then
            MsgBox Err.Description
        End If
    End If
End Sub

Private Sub mnuHelpContents_Click()
    Dim frmB As New frmBrowser
    frmB.StartingAddress = "http://www.geocities.com/esteganografia/ayuda.htm"
    frmB.Show
End Sub

Private Sub mnuWindowArrangeIcons_Click()

```

```

        Me.Arrange vbArrangeIcons
    End Sub

    Private Sub mnuWindowTileVertical_Click()
        Me.Arrange vbTileVertical
    End Sub

    Private Sub mnuWindowTileHorizontal_Click()
        Me.Arrange vbTileHorizontal
    End Sub

    Private Sub mnuWindowCascade_Click()
        Me.Arrange vbCascade
    End Sub

    Private Sub mnuWindowNewWindow_Click()
        LoadNewDoc
    End Sub

    Private Sub mnuViewWebBrowser_Click()
        Dim frmB As New frmBrowser
        frmB.StartingAddress = "http://www.geocities.com/esteganografia/"
        frmB.Show
    End Sub

    Private Sub mnuViewOptions_Click()
        frmOptions.Show vbModal, Me
    End Sub

    Private Sub mnuViewRefresh_Click()
        MsgBox "Agregar código 'mnuViewRefresh_Click'."
    End Sub

    Private Sub mnuViewStatusBar_Click()
        mnuViewStatusBar.Checked = Not mnuViewStatusBar.Checked
        sbStatusBar.Visible = mnuViewStatusBar.Checked
    End Sub

    Private Sub mnuViewToolbar_Click()
        mnuViewToolbar.Checked = Not mnuViewToolbar.Checked
        tbToolBar.Visible = mnuViewToolbar.Checked
    End Sub

    Private Sub mnuEditPasteSpecial_Click()
        MsgBox "Agregar código 'mnuEditPasteSpecial_Click'."
    End Sub

    Private Sub mnuEditPaste_Click()
        On Error Resume Next
        ActiveForm.rtfText.SelRTF = Clipboard.GetText
    End Sub

    Private Sub mnuEditCopy_Click()
        On Error Resume Next
        Clipboard.SetText ActiveForm.rtfText.SelRTF
    End Sub

```

```

Private Sub mnuEditCut_Click()
    On Error Resume Next
    Clipboard.SetText ActiveForm.rtfText.SelRTF
    ActiveForm.rtfText.SelText = vbNullString
End Sub

Private Sub mnuEditUndo_Click()
    MsgBox "Agregar código 'mnuEditUndo_Click'."
End Sub

Private Sub mnuFileExit_Click()
    Unload Me
End Sub

Private Sub mnuFileSend_Click()
    MsgBox "Agregar código 'mnuFileSend_Click'."
End Sub

Private Sub mnuFilePrint_Click()
    On Error Resume Next
    If ActiveForm Is Nothing Then Exit Sub

    With dlgCommonDialog
        .DialogTitle = "Imprimir"
        .CancelError = True
        .Flags = cdIPDReturnDC + cdIPDNoPageNums
        If ActiveForm.rtfText.SelLength = 0 Then
            .Flags = .Flags + cdIPDAllPages
        Else
            .Flags = .Flags + cdIPDSelection
        End If
        .ShowPrinter
        If Err <> MSComDlg.cdlCancel Then
            ActiveForm.rtfText.SelPrint .hDC
        End If
    End With
End Sub

Private Sub mnuFilePrintPreview_Click()
    MsgBox "Agregar código 'mnuFilePrintPreview_Click'."
End Sub

Private Sub mnuFilePageSetup_Click()
    On Error Resume Next
    With dlgCommonDialog
        .DialogTitle = "Configurar página"
        .CancelError = True
        .ShowPrinter
    End With
End Sub

Private Sub mnuFileProperties_Click()
    MsgBox "Agregar código 'mnuFileProperties_Click'."
End Sub

```

```

Private Sub mnuFileSaveAll_Click()
    MsgBox "Agregar código 'mnuFileSaveAll_Click'."
End Sub

Private Sub mnuFileSaveAs_Click()
    Dim sFile As String

    If ActiveForm Is Nothing Then Exit Sub

    With dlgCommonDialog
        .DialogTitle = "Guardar como"
        .CancelError = False
        .Filter = "Todos los archivos (*.*)|*.*"
        .ShowSave
        If Len(.FileName) = 0 Then
            Exit Sub
        End If
        sFile = .FileName
    End With
    ActiveForm.Caption = sFile
    ActiveForm.rtfText.SaveFile sFile

End Sub

Private Sub mnuFileSave_Click()
    Dim sFile As String
    If Left$(ActiveForm.Caption, 8) = "Document" Then
        With dlgCommonDialog
            .DialogTitle = "Guardar"
            .CancelError = False
            .Filter = "Archivo de texto(*.txt)|*.txt"
            .ShowSave
            If Len(.FileName) = 0 Then
                Exit Sub
            End If
            sFile = .FileName
        End With
        ActiveForm.rtfText.SaveFile sFile
    Else
        sFile = ActiveForm.Caption
        ActiveForm.rtfText.SaveFile sFile
    End If

End Sub

Private Sub mnuFileClose_Click()
    MsgBox "Agregar código 'mnuFileClose_Click'."
End Sub

Private Sub mnuFileOpen_Click()
    Dim sFile As String

    If ActiveForm Is Nothing Then LoadNewDoc

```

```

With dlgCommonDialog
    .DialogTitle = "Abrir"
    .CancelError = False
    .Filter = "Archivo de texto(*.txt)|*.txt"
    .ShowOpen
    If Len(.FileName) = 0 Then
        Exit Sub
    End If
    sFile = .FileName
End With
ActiveForm.rtfText.LoadFile sFile
ActiveForm.Caption = sFile

```

```
End Sub
```

```

Private Sub mnuFileNew_Click()
    LoadNewDoc
End Sub

```

Código de la presentación de inicio

```

Private Sub Form_Load()
    lblVersion.Caption = "Version " & App.Major & "." & App.Minor & "." & App.Revision
    lblProductName.Caption = App.Title
End Sub

```

```
Private Sub lblLicenseTo_Click()
```

```
End Sub
```

Apéndice F

Artículo de Sistema Esteganográfico

Presentado en el Congreso Estudiantil de Computación (CORE)
Marzo 2002.

SISTEMA ESTEGANOGRAFICO

Mendoza Rodarte Saúl.

Instituto Politécnico Nacional Campus Zacatenco.
Escuela Superior de Cómputo
E-MAIL: siloe18@hotmail.com

Reyes Figueroa Arturo.

Instituto Politécnico Nacional Campus Zacatenco.
Escuela Superior de Cómputo.
E-MAIL: rysarthur@hotmail.com

RESUMEN

La Esteganografía es una técnica que nos permite ocultar información dentro de otra información diferente. Podemos "esconder" mensajes ó archivos dentro de imágenes, archivos de sonido, documentos de texto, etc. Esta técnica ha sufrido un importante impulso en los últimos tiempos que permiten entreverla como una de las opciones con más futuro para proteger la confidencialidad de la información.

En este trabajo pretendemos desarrollar una herramienta que nos permita ocultar nuestra información dentro de otra información diferente, y "esconder" mensajes ó archivos dentro de imágenes, donde ésta herramienta sea de fácil manejo para los usuarios finales y responder así a las exigencias de seguridad y confidencialidad de la información.

1. INTRODUCCION.

La seguridad de un sistema de cómputo es la habilidad que tiene el sistema para lograr proteger información, a pesar de las acciones de algún enemigo, quizá bien informado y con medios adecuados para corromper el sistema.

La Esteganografía es una técnica que nos permite ocultar información ó datos dentro de otra información diferente.

La Confidencialidad de la información se refiere a que ésta, esté accesible para lectura solamente por partes autorizadas; de forma que cualquiera que intente interceptarla no pueda tener acceso al contenido de los datos.

Comencemos por definir que la palabra Esteganografía que en castellano no aparece en el diccionario de la Real Academia, pero en cambio,

no nos ofrece ninguna palabra que pueda sustituirla. El término "Esteganografía" viene del griego STEGOS, que significa "cubierta", por lo que Esteganografía significaría "escritura oculta" o "escritura encubierta".

En la Esteganografía puede aplicarse cualquier método para ocultar un mensaje, pues es en un 99% imaginación y por tanto no tiene límites. Aunque piensen que solo puede aplicarse al texto no es así, pues se podría incluso realizar una imagen en la que los píxeles menos significativos son sustituidos por el mensaje en cuestión que deseemos incrustar.

Hay que dejar clara la diferencia entre la criptografía y la Esteganografía "estricta". La criptografía modifica los datos para que no sean legibles, a diferencia de la Esteganografía, que simplemente los toma y los oculta entre otros datos. Sin embargo, hoy en día, con las computadoras, ambas técnicas son combinables, consiguiéndose una seguridad aún mayor

Es evidente que un mensaje cifrado es identificado rápidamente por él sin sentido de su formato, en cambio si ponemos ese mismo mensaje dentro de una imagen, o de otro texto se garantiza que no vayamos paseando nuestros datos por el mundo con un letrero de "cifrado". Ello nos otorga discreción y anonimato. También existe la posibilidad de que el tráfico de la información pudiera ser tratado de forma masiva para capturar cosas de interés. Esto se suele hacer mediante el "monitoreo" de nuestro tráfico para capturar palabras clave; Palabras que si las hacemos invisibles en principio no llamarán la atención. Además los constantes rumores sobre puertas traseras en los programas más populares de cifrado pueden hacer aconsejable el uso de la

Esteganografía para dar seguridad realmente potente.

No hay duda de que, si la criptografía puede tener usos delictivos, la Esteganografía puede tenerlos aún más claros. Sin embargo, bien usada puede convertirse en algo muy útil. La Esteganografía se convierte en una útil herramienta para proteger nuestros datos, tanto combinada con la criptografía, como por separado.

Existen algunas herramientas que manejan algunas técnicas de ocultamiento de información de las cuales encontramos:

S-Tools

S-Tools, escrito por Andrew Brown, es un programa para Windows que permite cifrar y ocultar datos en archivos .wav ó en imágenes en formato .bmp o .gif.

Nota: Este programa es freeware, así que puede distribuirse libremente, si bien hay que tener en cuenta que, dado que incluye la implementación de diversos algoritmos criptográficos, podría estar sujeto a determinadas restricciones a la exportación. Su uso en Francia podría ser ilegal bajo la Ley 90-1170 de dicho país, que prohíbe el uso de criptografía. Asimismo, podría entrar en conflicto con la EAR (Regulación del Tráfico Internacional de Armas) americana.

Es seguramente el más cómodo al ser para Windows, integra la encriptación en el mismo programa, y permite ocultar los datos en archivos más "generales" que los anteriores programas.

En cuanto a los algoritmos criptográficos, se dispone de cuatro algoritmos de clave secreta: IDEA, DES, Triple DES y MDC. IDEA es por ahora el mejor y más fuerte de los cuatro. En cuanto a DES, sería preferible no utilizarlo, dado que se le han descubierto demasiadas debilidades para seguir considerándolo seguro.

Texto

Texto, que a pesar de su nombre no es un programa español, ha sido escrito por Kevin Maher, y es un programa que transforma archivos codificados con uuencode ó archivos cifrados con PGP y *ASCII armor* en archivos de texto que contienen frases en inglés.

Texto sustituye los caracteres ASCII por palabras en inglés que obtiene de un archivo llamado words. Después utiliza estas palabras según las estructuras de frases contenidas en un archivo llamado structs, creando así el texto en inglés. Las palabras en mayúsculas son etiquetas que Texto sustituye por las palabras seleccionadas del archivo words.

Debido a que en el inglés también hay algunas estructuras irregulares, a veces algunas frases contienen errores gramaticales. No son demasiado graves como para hacer sospechar del texto, dado que el inglés es un idioma bastante "práctico" y relativamente simple si lo comparamos por ejemplo con nuestras lenguas latinas. Es más, estos errores hacen incluso que el texto parezca más humano, como si fuera escrito por alguien que comete faltas, y más aún, unidos estos errores a las extrañas frases, los textos producidos dan la impresión de ser escritos por alguien que padece alguna demencia o está drogado, lo que puede ayudar a no tenerlos en consideración y no examinarlos.

Asimismo, también puede modificarse el archivo words y sustituir las palabras. La condición es no utilizar palabras acabadas en "s" o en "ing", ni repetir palabras. El orden también importa, así que cambiar el actual orden de palabras de words también resultará. Eso sí, si modificamos words, debemos pasarle el nuevo archivo a la persona con la que nos comunicamos, si no, no podrá extraer los datos. En cambio, no hace falta pasarle el archivo structs aunque lo modifiquemos.

Por cierto, por si alguien lo está pensando. Y... ¿utilizar archivos en español? La idea es buena, pero el programa está pensado para el idioma inglés. Habría que meterse a modificar el código, y hay un importante problema: la mencionada "complejidad" de nuestro rico idioma, que hace que el escribir un programa que construya estructuras gramaticales en español relativamente correctas sea una dura tarea. El gran problema que tiene este programa: El texto obtenido es DIEZ VECES mayor que el archivo original. La solución que recomienda Kevin Maher es utilizar más palabras, una para cada dos símbolos, en vez de una para cada uno. Modificar el código es simple, pero esto requiere 4096 palabras de cada clase en el archivo words, algo un tanto complejo (es

más, ¿hay 4096 adverbios en inglés?). De media debería conseguirse que los archivos pasaran a ser cinco veces más grandes en vez de diez veces.

2. DESARROLLO DE LA HERRAMIENTA

Con el desarrollo de este trabajo esperamos obtener una herramienta capaz de ocultar información (texto) en una imagen; así también desarrollar una documentación precisa acerca de la Esteganografía y sus aplicaciones, que sirva para establecer bases y recomendaciones en trabajos futuros en esta área.

Consideramos las acciones que el usuario tendría que hacer para interactuar con el sistema, en primera instancia es el usuario quien determina el origen de la información a ocultar, ya sea señalando el lugar de la información (archivo) ó si éste escribirá directamente la información a ocultar, posteriormente el usuario deberá indicar la imagen donde será ocultada la información con estos datos el sistema deberá ser capaz de ocultar la información proporcionada en la imagen.

Cabe mencionar que el sistema desarrollaría dos actividades importantes: la primera es ocultar una información en otra y la segunda extraer la información original del medio transportador (imagen).

Para la segunda etapa el usuario tendrá que indicar el origen (ruta del archivo) del medio transportador, y al proporcionar una clave específica además de elegir la acción el sistema deberá ser capaz de extraer la información oculta en el medio transportador.

Para que este sistema cumpla con los niveles de seguridad que la Esteganografía proporciona se tomarán en cuenta ciertas características las cuales son, que no exista variación entre la imagen original y la obtenida por medio de ésta técnica de ocultamiento, segundo que la imagen resultante ocupe el mismo espacio en disco es decir que la imagen sea del mismo tamaño, en caso de existir variaciones en la imagen estas sean imperceptibles al ojo humano.

Y finalmente de acuerdo a un estudio previo de herramientas esteganográficas existentes, se identifico las características que debía tener el software hacia el usuario final. Donde lo más importante será proporcionar una interfaz con el usuario de fácil manejo, donde no se involucren

cuestiones técnicas que deben ser ajenas para éste último.

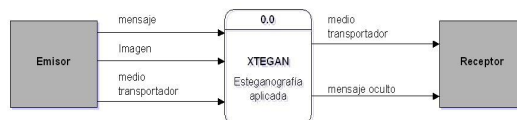


Figura 1

Diagrama de Contexto
Esteganografía Aplicada

En la estructura general del sistema, podemos identificar tres actores, el emisor, el sistema y el receptor.

El emisor. Este usuario final es aquel que por alguna razón tiene la necesidad de mantener segura su información, consideremos el caso de que desea enviar información importante a otra persona, las acciones implicadas son: proporcionar al sistema la fuente tanto de la información a ocultar como de la imagen que deba llevar la información oculta.

El sistema. El sistema esteganográfico recibirá como únicas entradas el mensaje o archivo y la imagen, el sistema deberá ser capaz de ocultar la información del emisor con una imagen. Entregará como único resultado una nueva imagen, imagen que deberá cumplir con las características ya señaladas en los requerimientos del sistema.

El receptor. Este usuario también final, al recibir el archivo de imagen, podrá ingresarlo al sistema esteganográfico y así el sistema deberá extraer la información oculta.

En el diagrama siguiente se muestra como a pesar de existir dos procesos distintos una sola herramienta deberá de realizar ambos, ocultamiento y extracción.

Así pues entenderíamos el diagrama de la Figura 2 como sigue:

- Si al sistema le proporciono una información ó mensaje y una imagen, el

sistema deberá entregarme una imagen con información oculta.

- Si al sistema le proporciono una imagen el sistema deberá entregarme el mensaje oculto.

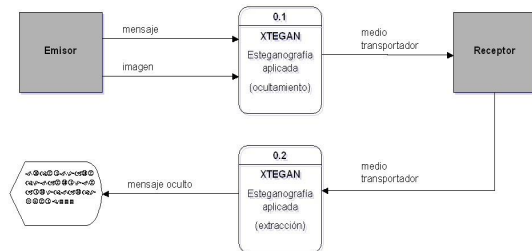


Figura 2

Diagrama Lógico
Esteganografía Aplicada

En la Figura 2 podemos observar el diagrama lógico y las etapas involucradas en el proceso de ocultamiento y extracción de la información a partir de las entradas al sistema, la imagen, el masaje ó archivo con la información a ocultar y como el receptor al ingresar la imagen generada ó medio transportador entra al sistema y el mismo sistema quien extrae la información oculta en el medio transportador.

Diagrama de Nivel Cero

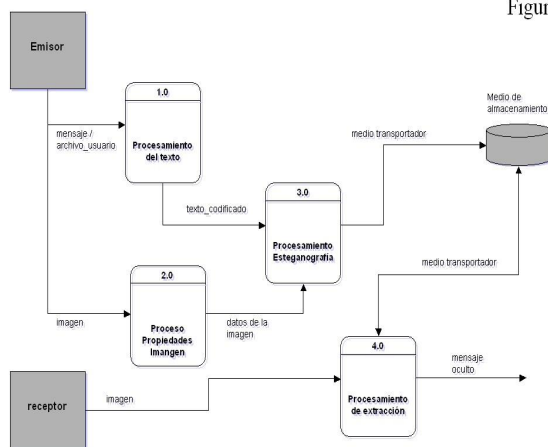


Diagrama de Flujo de Datos de Nivel Cero
Esteganografía Aplicada

En la Figura 3 observamos más claramente el funcionamiento del sistema propuesto. Empecemos por identificar cada uno de los elementos y las características de estos así como las entradas y las salidas de los procesos involucrados.

Como podemos observar en la Figura 3, el sistema esteganográfico se divide en cuatro principales procesos:

- Procesamiento del texto.
- Obtención de las propiedades de la imagen.
- Procesamiento Esteganográfico.
- Procesamiento de Extracción.

Diagrama de primer nivel "Procesamiento del Texto"

Figura 4

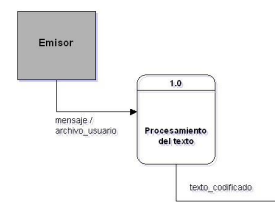


Diagrama de primer nivel "Procesamiento del Texto"
(Diagrama tipo del proceso 1.0) Esteganografía Aplicada

En la Figura 4 observamos dos tipos de entrada. En realidad es solo una, pero es el usuario quien define de donde es el flujo, que puede ser por un archivo ya existente ó que el usuario proporcione directamente el texto, el contenido de este último será procesado y como única salida se generara un registro temporal que contendrá el código designado a cada uno de los caracteres que forman el texto proporcionado por el usuario, esto es, el Procesamiento del Texto no es sino un proceso de codificación.

Este proceso puede ser tan sencillo o tan difícil como la imaginación del programador se le permita, que va desde el simple uso del código ASCII hasta quizá el uso de una técnica criptográfica que proporcione una salida distinta del original.

Aquí el proceso medular de ésta tarea es convertir todo en números ya sea enteros o en representaciones binarias (1's y 0's), pues es a nivel binario donde trabajaremos con la imagen.

En esta etapa se presenta un almacenamiento temporal es un espacio en disco designado para almacenar por un tiempo corto no al texto, sino el resultado de codificar al texto, esto es, almacenar

cierta información ya tratada para que el método esteganográfico la utilice y la oculte en la imagen.

Figura 6

Diagrama de primer nivel "Proceso Propiedades en la Imagen"

Figura 5

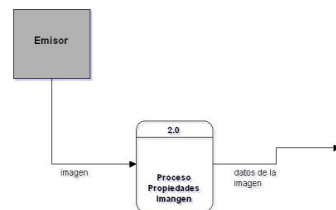


Diagrama de primer nivel "Proceso Propiedades de la Imagen"
(Diagrama hijo del proceso 2.0) Esteganografía Aplicada

La Figura 5, representa el proceso de obtener las propiedades de la imagen, estas son variadas, y dependen de la técnica esteganográfica a usar, pero lo más importante para toda técnica esteganográfica es conocer el tamaño como el espacio que ocupa en disco, las dimensiones, y los colores que utiliza la imagen a trabajar.

Este proceso recibe como entrada una imagen, la estudia y genera un registro (datos de la imagen) y la guarda por un tiempo relativo hasta que se genera la imagen o medio transportador.

Aquí observaremos que también existe un almacenamiento temporal de información ya que solo existirá hasta el momento de entregarle al usuario la nueva imagen creada, este contendrá la información recabada por el sistema, de las características de la imagen proporcionada o seleccionada por el usuario, generándose un registro el cual será la entrada del proceso esteganográfico; éste proceso será transparente para el usuario.

Diagrama del primer nivel "Procesamiento Esteganografía"

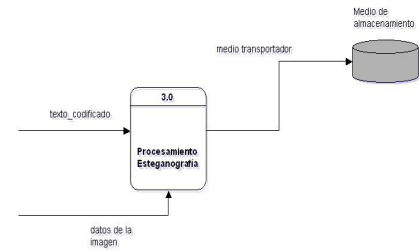


Diagrama de primer nivel "Procesamiento Esteganografía"
(Diagrama hijo del proceso 3.0) Esteganografía Aplicada

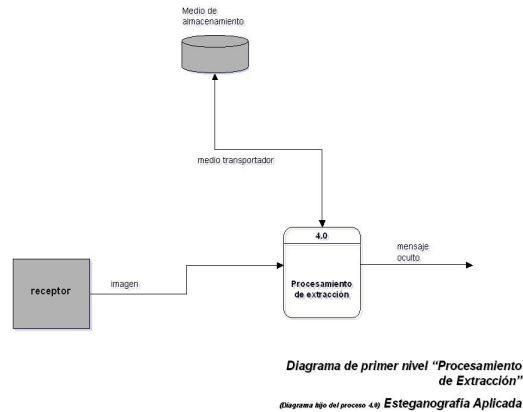
En el diagrama de la figura 6 observamos el proceso esteganográfico, aquí es donde interviene la implementación de la técnica esteganográfica seleccionada, sea cual sea la técnica, recibirá la codificación del mensaje original, los datos de la imagen es decir el registro de la imagen y nos dará como único resultado una imagen nueva, similar a la imagen original

En éste mismo diagrama mostramos el medio de almacenamiento donde se guardara el nuevo archivo generado tras el proceso de ocultamiento de información. Este almacén también lo podemos observar desde un punto de vista, como el sistema de archivos, ya que el resultado del proceso esteganográfico será un archivo, este es el mismo medio transportador o imagen generada.

También mostramos una salida más, que aparentemente no debe estar, pero existe por la simple selección que emitirá el usuario entre guardar la imagen nueva y quizá mostrar en pantalla el resultado, eso como una opción que tendrá disponible el usuario para su comodidad y pueda observar el resultado.

Diagrama de primer nivel "Procesamiento de Extracción"

Figura 7



En el diagrama de la parte superior (Figura 7), encontramos el Proceso de Extracción. Este proceso comprende las tareas que el sistema deberá realizar para extraer la información original de un medio transportador, como entrada será la imagen ó medio de transportador, el usuario que quiera extraer la información contenida deberá proporcionar una clave para con la cual extraerá la información.

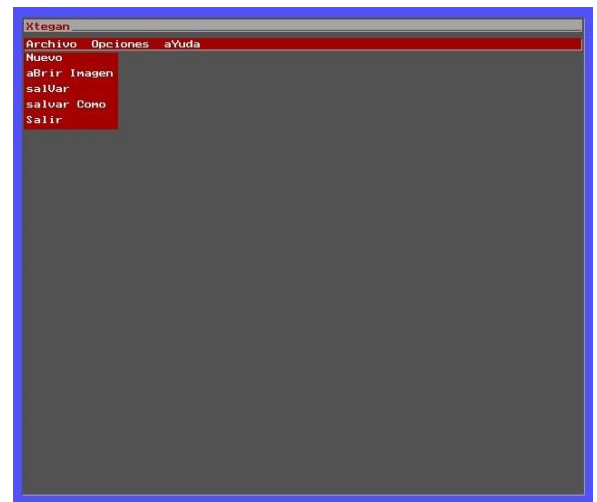
4. AVANCES REALIZADOS

El Primer Sistema llamado Xtegan es una propuesta experimental para observar y entender las opciones con las que debe contar el sistema a desarrollar.

Este primer sistema, se caracteriza principalmente por haber sido desarrollado en Lenguaje C. Inicialmente porque C es un lenguaje poderoso y flexible. Lo que se puede lograr con el C es muy extenso y muy poco limitado para los expertos del lenguaje. El lenguaje, por sí mismo, no pone límites. El C es un lenguaje portable. La portabilidad se aumenta con el estándar ANSI para el C (el juego de reglas para los compiladores C).

Como muestran estas características, el C es una alternativa excelente para haber desarrollado el "Primer Sistema".

Acerca del primer prototipo de sistema, pensamos en una interfaz grafica, de fácil manejo por el usuario, y las opciones del menú principal sean claras y cuente con cuadros de dialogo con información suficiente para saber cual será el siguiente paso de cada proceso.



Esta pantalla nos permite observar las opciones básicas del sistema.

Ocultamiento de la información.

La herramienta Esteganográfica propuesta, debe obtener la información a oculta de alguna forma, ya sea proporcionada por el usuario ó que este último la escriba directamente, sea cuál sea el origen, esta información deberá ser codificada de alguna manera, el objetivo es que el sistema pueda manipular la información que se precisa ocultar.

Una forma sencilla es asignar un código específico a un carácter en particular.

Carácter	A	B	C	...	y	Z
código DEC	0	1	2	...	55	56
código BIN	0000 0000	0000 0001	0000 0010	...	0011 0111	0011 1000

De esta manera obtendremos la codificación de mensajes como "ABZ" de la siguiente manera:

"00000000000000001000111000".

Consideramos ahora, las características de la imagen a ser tratada, desde el punto de vista más básico un archivo es un conjunto de información binaria, con un formato en particular, basados en esa idea, un archivo de imagen también esta formado de bits con un formato específico, consideremos el archivo como arreglos o conjuntos de 8 bits, la que contienen estos es la información de cada uno de los píxeles que conforman la imagen.

Considerando estas características resulta muy sutil que exista la posibilidad de manipular el menos el bit menos significativo de los arreglos binarios.

Ahora si deseamos ocultar un carácter “y” dentro de un arreglo como el siguiente:

```
0000110000011000001100000010010000110111
0011111101000000010111110
```

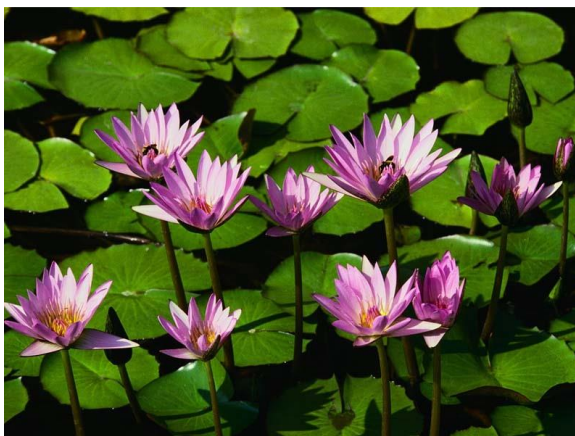
Obtendríamos algo así:

Original	Con cambios
00001100	00001100
00011000	00011000
00110000	00110000
00100100	00100100
00110111	00110111
00111110	00111111
10000000	10000000
10111110	10111111

Y la cadena binaria resultante queda así:
00001100000110000011000100100100110110
00111111100000010111111

Estos cambios no repercuten seriamente en la imagen original así como en sus características más importantes, al menos no a simple vista, ya que lo que único que hacemos es cambiar el color original, y así convertirlo a un tono mas claro ó más oscuro.

El siguiente ejemplo entre dos imágenes una original y la otra ya transportando un mensaje “hola mundo cruel ya nunca te veré”.



Esta es la imagen original, la cual usaremos como medio transportador.



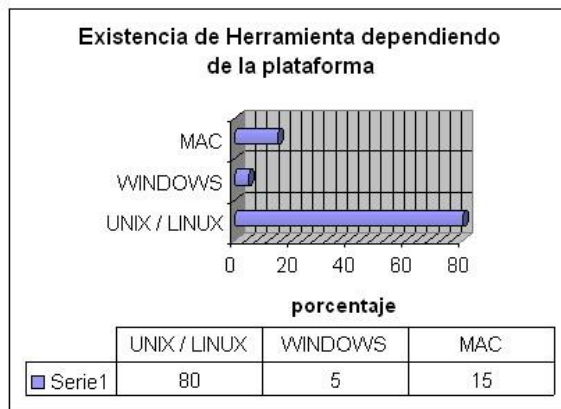
Esta imagen ya está portando un mensaje oculto, observando ambas imágenes, observamos que no existe diferencia a simple vista del proceso al que estuvo sujeta esta imagen.

Aunque la versión final sea desarrollada tentativamente en Visual C++, el desarrollar este prototipo en ANSI C nos permitirá generar código lo suficientemente manipulable, para los fines que hemos planteado.

Justificación de usar *visual C++*

Ya que es una versión mejorada de C y C++ pero esto no justifica su uso... mas bien la justificación de desarrollar una herramienta a partir de un lenguaje específico se elabora a partir de entender las características que debe cumplir el nuevo sistema y a otros criterios técnicos como la factibilidad y la gestión del proyecto.

Una de las etapas del análisis del sistema fue emprender una investigación a cerca de las herramientas esteganográficas existentes en el mercado, con este estudio encontramos que al menos el 80% de las herramientas y sistemas existentes en esta área de la seguridad, son sistemas basados para plataformas Unix / Linux (ver figura abajo)



Y el resto como observamos en la Figura se encuentra dividido entre las herramientas para MAC y Windows, este último representa la plataforma en la que existe el menor desarrollo de herramientas esteganográficas; razón por la cual la plataforma de desarrollo elegida es Windows, implica generar una herramienta mas dentro de las pocas existentes (solo dos) para esta plataforma.

Una vez determinada la Plataforma se entiende la respuesta de porque se utiliza Visual C++ como el Lenguaje de Desarrollo de la herramienta propuesta.

5. CONCLUSION

La herramienta esteganográfica a desarrollar, nos permitirá, contar con un transporte de información más seguro, ya que la información podrá pasar desapercibida, por los ojos de cualquier persona ajena al destinatario, en forma de imagen, sin despertar la sospecha de que ocultamos información, aunque el ocultar información dentro de otra, ó en especifico una información dentro de una imagen, aún es considerado un arte, el desarrollo de un algoritmo capaz de implementar este proceso resulta benéfico por las cuestiones de seguridad que se verán implicadas, proporcionando confidencialidad e integridad a la información a tratar.