UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA INFORMÁTICA

TESIS DE GRADO

OCULTAMIENTO DE DATOS EN IMÁGENES

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INFORMÁTICA

MENCIÓN INGENIERÍA DE SISTEMAS INFORMÁTICOS

Postulante: Univ. Lino Jorge Montecinos Flores

Tutor: Lic. Eufren Llanque Quispe

Revisor: Lic. Javier Hugo Reyes Pacheco

LA PAZ – BOLIVIA

2009

DEDICATORIA

El presente trabajo va en honor a mi familia, con amor a mis queridos padres Lino y Alcira por darme la vida y brindarme todo su cariño, paciencia en cada momento de mi vida, ellos siempre me apoyaron para que estudie y me supere cada día más, siempre me dijeron que con paciencia y esfuerzo todo se puede alcanzar en esta vida. A mis hermanas Lizeth y Jhoseline porque siempre me brindaron su cariño, amor y su compañía apoyándome en cada momento. Para mi hermano Álvaro que esta en el cielo y que me custodias en cada momento.

AGRADECIMIENTOS

Agradecer ante todo a Dios por guiarme día a día y por permitirme continuar en este mundo, disfrutando de la compañía de todos los que quiero.

Agradecer a la Universidad Mayor de San Andrés por constituirse en mi segundo hogar.

También agradecer a la Carrera de Informática y docentes por enseñarme y formarme.

Mi agradecimiento al Lic. Eufren Llanque por guiarme en la realización del presente trabajo. Al mismo tiempo agradecer al Lic. Javier Reyes por los consejos y el tiempo dedicado a la revisión del presente trabajo.

Agradecer a toda mi familia por su apoyo, en especial a mis padres por estar siempre a mi lado, apoyándome en todo y por ocupar un lugar muy importante en mi corazón.

ÍNDICE GENERAL

CAPÍTULO 1 MARCO REFERENCIAL

CAPITULO 2 MARCO TEÓRICO

CAPITULO 3 BIT MENOS SIGNIFICATIVO

CAPITULO 4 CONCLUSIONES Y RECOMENDACIONES

ÍNDICE ESPECÍFICO

CAPÍTULO 1 MARCO REFERENCIAL

CAPITULO 2 MARCO TEÓRICO

CAPITULO 4 CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad existe mucha información que es difundida por todo el mundo mediante la web, por este motivo existe una demanda por el ocultamiento de información en imágenes digitales y se convierte en gasto excesivo de tiempo y dinero que se pierde para ocultar información. La esteganografía es una opción económica y de tiempo ya que permite ocultar información en imágenes digitales. En la presente tesis se plantea una forma para la ocultación de información, recurriendo a herramientas de LSB (Least Significant Bit), que se basa en la utilización del dígito menos significativo, el objetivo es encubrir información en una imagen manteniendo su calidad de visualización.

Se realiza una descripción sobre los tipos de imágenes digitales, la representación binaria de estas, los modelos de color que manejan. Se abarcan temas de números binarios, clases de esteganografía.

Luego se realiza un diseño de los bits menos significativos basándose en la técnica LSB descrito anteriormente y se desarrolla un prototipo para mostrar los resultados. A los resultados obtenidos se usa el formato BMP (Windows BitMap) que es el formato más simple y aunque teóricamente es capaz de realizar compresión en imagen.

Los resultados finales permiten concluir que la técnica utilizada no altera el formato, la resolución, el tamaño del archivo grafico; manteniendo la calidad de la visualización de la imagen.

A partir del presente trabajo, es posible introducirse en otros tipos de formatos como ser en audio combinando otras técnicas de ocultación de información en imágenes.

ABSTRACT

As of the present moment a lot of information that is once the Web was spread out all over the world intervening, by this motive exists a request for the concealment of information in digital images exists and becomes excessive time expense and money that gets lost to hold back information. The esteganografía is a cost-reducing and time option since it allows hiding information in digital images. A way for the hiding of information is presented in present thesis, turning to LSB's tools (Least Significant Bit), that he is based on the utilization of the least significant digit, the objective is abetting information in an image holding its quality of visualization.

A description on the guys of digital images that drive, the binary performance of these, the fashion models of color are accomplished. They comprise themes of binary numbers, esteganografía's classes.

Next basándose in the technique sells off a design of the least significant bits itself just described LSB and a prototype to show results develops. BMP uses to the obtained results the format (Windows BitMap) that it is the simplest format and although theoretically you are able to accomplish compression in image.

Final results allow concluding that the used technique does not alter the format, resolution, the size of the graphic file; Holding the quality of the visualization of the image.

As from the present work, he is possible to get into other types of formats like being in audio combining other techniques of hiding of information in images.

CAPITULO I

MARCO REFERENCIAL

Desde tiempos antiguos los seres humanos hemos deseado enviar mensajes ocultos destinados a una persona en especial pero que el mensaje no pueda ser obtenido por tercera personas.

En Grecia, se ocultó un mensaje enviado hacia Esparta. En esos tiempos se usaban tablones cubiertos con cera para escribir mensajes, por lo que el mensaje oculto fue escrito directamente en el tablón, luego cubierto con cera y finalmente un nuevo mensaje fue escrito sobre la cera. [HOSMER Y HIDE, 2003]

Durante la segunda guerra mundial, se microfilmaron los mensajes hasta reducirlos al tamaño de un punto, con lo que el mensaje podía ser enviado como el punto de "i" dentro de otro mensaje, sin levantar sospecha alguna. [HOSMER Y HIDE, 2003]

Actualmente, con el uso de computadores y el intercambio de información a través de medio de informáticos, se ocultan mensajes en archivos que a simple vista son comunes y corrientes, como fotografías, pero que con un software adecuado podría obtenerse un mensaje que se encuentre oculto dentro de esos archivos.

En él presente tesis de grado definiremos la manera de ocultar mensajes en imágenes, ocultando la mayor cantidad posible de información, además distribuyendo de la mejor manera los pixeles a modificar en la imagen.

A todo se le da una definición llamado Esteganografía, del griego (*steganos*, encubierto "con el sentido de oculto") y (*graphos*, escritura) nace el término esteganografía: el arte de escribir de forma oculta, puede parecer en un principio términos equivalentes con Criptografía (*criptos*, oculto) y (*graphos*, escritura), dado que el último es el arte de escribir de forma enigmática. Queda claro que esteganografía no es un tipo de criptografía: son técnicas distintas e independientes, si bien pueden complementarse entre ellas (algunas ocasiones suelen hacerlo).

Si hablamos rigurosamente de la definición de esteganografía, veremos que, mediante distintas soluciones técnicas, lleva aplicándose siglos en la vida del ser humano (casi siempre ligado al espionaje o al secreto).

No obstante, aunque es bueno conocer su origen, vamos a centrar en sus aplicaciones actuales en el campo de la informática.

Para los que no conozcan absolutamente nada sobre la técnica, y antes de ver definiciones rigurosas, podemos decir que la esteganografía es una forma cómoda de trabajar con información, es decir, información dentro de la información.

En otros tiempos la información que rodeaba a una persona era transportada por unos canales muy definidos (correo, teléfono...) y de forma limitada; pero eso es algo que en las últimas décadas ha cambiado de forma radical. El actual desarrollo de la tecnología computacional y las telecomunicaciones (cuyas culminaciones son el ordenador personal e Internet respectivamente) han rodeado completamente nuestras vidas de torrentes de información.

Si se piensa en la información que extraemos al visitar una web, y la cantidad real de información que contiene, podemos ver que el vivir en un medio ruidoso hace en cierto modo impermeables a la información no deseada.

1.1 ANTECEDENTES

Esteganografía da sus primeros pasos en la antigua Grecia. Se cuenta en "Las Historias de Herodoto" ("Les *Hisróries d'Heródot*") que Demeratus quería comunicar a la ciudad de Esparta que Xerxes tenía planes para invadir Grecia. Para evitar ser capturado por espionaje en los controles, escribió sus mensajes en tablas que luego fueron cubiertas con cera, de forma que parecían no haber sido usadas. Ésta es posiblemente una de las primeras manifestaciones en la historia de mensajes esteganografiados. [HOSMER Y HIDE, 2003]

Otro método usado durante siglos consistía en tatuar al mensajero (generalmente un esclavo) un mensaje en la cabeza afeitada para después dejarle crecer el pelo y enviar así el mensaje oculto.

Aunque el método de escritura con tinta invisible es usado desde la edad media, es en la Segunda Guerra Mundial cuando adquiere una importancia capital. Fue usado muy activamente por la resistencia en los campos de prisioneros nazis.

Generalmente se usa de la siguiente forma: en primer lugar se escribe una carta completamente normal, y después se escribe, entre las líneas de esa carta, otro texto donde está la información importante. Era habitual el uso de vinagre, zumos de frutas u orina, aunque hoy en día existe compuestos químicos específicos que sirven igualmente y no desprenden olores tan fuertes (que serían fácilmente detectados por un perro entrenado). Al calentar el papel, la escritura se hace visible.

Actualmente la esteganografía está irremediablemente sujeta a las computadoras, que le han proporcionado el medio necesario para ser efectiva, y del que durante siglos no pudo disponer.

Son realmente pocas las publicaciones que existen sobre esteganografía, en comparación por ejemplo con la criptografía. Si buscamos publicaciones en castellano, el número desciende muchísimo más, hasta casi el cero.

Al contrario que la criptografía, que existe de una manera importante desde antes del desarrollo de la computadora y fue desarrollada especialmente en la Segunda Guerra Mundial, la esteganografía, pese a haber sufrido un desarrollo similar durante ese mismo periodo de tiempo, nunca dispuso de medios que la permitieran tomarse en cuenta hasta la aparición de la moderna ciencia de la computación. Es por eso que las publicaciones referentes al tema son tan escasas, y generalmente se encuentran englobadas como una parte de un texto criptográfico.

Algunas de las principales publicaciones relacionadas con el tema por orden cronológico:

- *Hypnerotomachia poliphili (1499)* – Anónimo, es un libro publicado en 1499 por Aldus Manutius. El libro versa sobre conocimiento general, tratando temas como arquitectura, ingeniería, paisajes, creación de jardines, pintura, escultura de todo menos esteganografía, criptografía o códigos de forma alguna. [HOSMER Y HIDE, 2003]

¿Qué es lo que hace tan significativo el libro? Contiene muchísimos datos escondidos en su interior. El más famoso, y el considerado como primer texto esteganografiado de forma escrita se obtiene tomando la primera letra de cada uno de sus capítulos, formando:

Poliam frater Franciscus Columna peramavit

Que significa "El padre Francesco Colonna ama apasionadamente a Polia". Por cierto, Francesco Colonna aún vivía cuando el libro fue publicado.

- *Steganographia (1499) - Tritheim Johannes Heidenberg*, se trata de la publicación más notoria de Tritheim, se incluye un sistema de esteganografía bastante avanzado, pero la temática general del libro (magia y métodos de aprendizaje acelerados) hizo que nunca se tomara demasiado en serio el texto.

[HOSMER Y HIDE, 2003]

1.2 PLANTEAMIENTO DEL PROBLEMA

Desde que una persona entra en contacto con una computadora ya se considera una persona vulnerable a toda clase de peligros informáticos, en principal cuando tiene una información privada, datos privados empezaremos a describir:

- Usar un programa para editar texto (Block de notas).
- Texto escrito confidencial para un receptor.
- Guardar el archivo de texto en cualquier formato: .doc , .txt mencionando algunos de ellos.
- Envío de mensaje a su receptor vía: email.
- El archivo no contiene contraseña (caso documentos tipo .doc).

FIGURA 1.3.1 LA MATRIZ CAUSA – EFECTO

N	PROBLEMAS	CAUSA	EFECTO	SOLUCIÓN
1	Usar un programa para editar texto	Vulnerable en cualquier ordenador	Mensaje descifrado	Ocultar el texto en imágenes mediante esteganografía
2	Guardar en formatos conocidos: . doc, .txt, etc.	Vulnerable en cualquier ordenador	Cambio de formato y mensaje descifrado	Guardar en formatos desconocidos y ocultar el texto en imágenes mediante esteganografía
3	Envió de mensajes por correo electrónico, descargas de documentos en formatos conocidos	Hackeo de los correos electrónicos y de las descargas de los documentos	Perdida de documentos en línea	Esteganografiar el documento para ser enviado por email.
4	Guardar el documento sin seguridad de contraseña	Vulnerable y modificable en cualquier ordenador	Mensaje descifrado	Guardar con contraseña y esteganografiar el documento
5	Guardar el documento con contraseña	Vulnerable con diccionarios de hackeo y	Mensaje descifrado	Esteganografiar el documento

		su respectivo software para encontrar el contraseña		

De acuerdo a los problemas planteados analizados en la tabla se propone el siguiente problema:

¿Se puede ocultar datos dentro de una imagen en formato bmp?

1.3 OBJETO DE ESTUDIO

La ocultación de datos privados en imágenes aplicando la Esteganografía que es el arte y ciencia de escribir mensajes secretos de tal forma que nadie fuera de quien lo envía y quien lo recibe sabe de su existencia, en contraste con la criptografía, en donde la existencia del mensaje es clara pero es obscurecido.

Los mensajes en la esteganografía muchas veces son cifrados primero por medios tradicionales, para posteriormente ser escondidos por ejemplo en un texto que puede contener dicho mensaje cifrado, resultando el mensaje esteganográfico. Un texto puede ser manipulado en el tamaño de la letra, espaciado, tipo y otras características para ocultar un mensaje, sólo el que lo recibe, quien sabe la técnica usada, puede extraer el mensaje y luego descifrarlo.

1.4 JUSTIFICACIÓN

En el área científica para él siguiente tesis de grado se proporcionara un método del bit menos significativo para el proceso de ocultamiento de datos.

En el área tecnológica se aplicaran en máquinas antiguas hasta las modernas desde el Pentium I incluso las Pentium actuales (Centrino, Core, etc)

En el área social, la constante y creciente demanda por servicios de seguridad de archivos de datos a ser enviados de un emisor a un receptor sea segura.

En el área de conocimiento se enfocara en el uso de bits colores RGB (Red, Green, Blue), Matrices de los bits.

En el área económica el uso del software no es muy costoso, solo es la implementación es portable.

1.5. HIPÓTESIS

La técnica de ocultación de datos se puede utilizar en archivos de imágenes, manipulando su representación binaria.

1.6. OBJETIVOS

1.6.1 OBJETIVO GENERAL

Desarrollar una técnica de ocultación de datos que permita obtener a partir de una imagen digital una versión esteganografiada de la misma, aplicando el método del bit menos significativo.

1.6.2 OBJETIVOS ESPECÍFICOS

- Implementar el método del bit menos significativo en imágenes digitales.
- Desarrollar un software en el cual se puedan mostrar los resultados obtenidos al implementar la técnica de ocultación desarrollada,
- Realizar la comparación de los resultados obtenidos con la técnica desarrollada.
- Ver la calidad de las imágenes esteganografiadas, con los datos ocultos.
- Demostrar el grado de confianza del bit menos significativo en el campo de la

esteganografía

1.7 LÍMITES Y ALCANCES

En el desarrollo del presente trabajo se considera los siguientes procesos:

- Manejo de pixeles de las imágenes en donde se procederá a guardar la información para la ocultación de datos.
- Manejo de archivos de imagen BMP para la manipulación binaria.
- El sistema no contempla criptografía.

1.8 APORTES

1.8.1 APORTE TEÓRICO

Como uno de los inicios de la esteganografía aplicada a imágenes el método a emplear que consta en poner los datos tales como son en la imagen de salida, lo cual en la mayoría de los casos genera ruido.

A causa del problema nace el método del bit menos significativo, propuesto por Derek Upham's, el cual consiste en tomar los bits menos significativos de los pixeles de la imagen, por supuesto la técnica permitirá ocultar cantidad de información pero lo hará casi imperceptible al ojo humano.

Como primer paso para esteganografiar, se necesita una imagen en RGB, el formato es de mucha importancia ya que la que más se adapta es el formato bmp.

Para ello es necesario obtener un archivo de texto plano y una imagen con las características mencionadas anteriormente. Y como último parámetro, es una matriz (M) de n filas, por dos columnas. Donde n representa la cantidad total de caracteres que se incrustaran en la imagen y las dos columnas que identifican la posición a ocultar de cada letra en la imagen.

1.8.2 APORTE PRÁCTICO

Si deseáramos almacenar la letra a (código ASCII) tenemos:

Figura 1.8.2.1 Aporte Práctico

		R	G	B
PIXEL	1	0	1	1
PIXEL	2	0	0	0
PIXEL	3	0	1	-

Fuente: [Elaboración propia]

El método del bit menos significativo tomando en cuenta escoge los pixeles a modificar de una manera secuencial, aglomerando los cambios realizados en la imagen en su parte inicial.

1.9 METODOLOGÍA

1.9.1 METODOLOGÍA CIENTÍFICA

En cuanto a los métodos involucrados para el desarrollo, se menciona:

- **Método Analógico - Sintáctico**

  Se contempla la necesidad de realizar un análisis y síntesis en varias etapas del proyecto.

- **Método Inductivo - Deductivo**

  La inducción viene siendo la única forma de conseguir la deducción o deducciones propuestas en los objetivos.

- **Método Abstracción - Concreción**

Se necesita tener una visión exacta del trabajo de investigación.

CAPITULO II

MARCO TEÓRICO

2,1 EL ARTE DE LA ESTEGANOGRAFÍA

La esteganografía está definida como el arte de ocultar información en archivos de imágenes, sonidos o en canales encubiertos a través de método o técnicas computacionales. Se encuentra enmarcada en el ámbito de transportar información a través de las redes informáticas.

Existen diferentes técnicas que permiten implementar la esteganografía, sin embargo, las más utilizadas son las que se aplican el método LSB (Least Significant Bit), que se basa en la utilización del digito menos significativo para ocultar el mensaje. Otros métodos se fundamentan sobre la estadística, que busca los valores más redundantes del archivo y ubican allí los bits que hacen referencia al mensaje que se desee ocultar. Este es uno de los métodos más potentes y seguros.

Las técnicas de esteganografía se deben apoyar en dos principios básicos: el primero, en seleccionar muy bien el medio en el que se desea aplicar dicha técnica, refiriéndose a que el archivo encubierto, a pesar de que pierde calidad, no sea perceptible a dicha pérdida; el segundo principio, trata de aprovechar las limitaciones del hombre referidas

a la percepción de algunas señales visuales (gama de colores) y auditivas (algunas frecuencias que el oído humano no alcanza a percibir).

Los colores que utilizan una imagen también se ven representados por la cantidad de bits que dispongan, lo que significa que si posee 3 bytes existen en la imagen un color rojo, uno azul y otro verde, formando una paleta de colores. Por tal razón, cuando se cambia un bit, como lo es el menos significativo en la imagen cubierta, el color de la imagen puede variar dentro de su paleta de un estado al siguiente o al anterior, ocasionando que el cambio no sea perceptible.

El bit menos significativo consiste en codificar cada bit de la información a lo largo de la imagen quitando un bit de la misma y colocando el bit del mensaje, normalmente se hace en las áreas más ruidosas de la imagen que no atraen la atención, como por ejemplo, un prado o el cielo.

La esteganografía es una ciencia que abarca mucho más allá del simple ocultamiento de mensajes en imágenes, a pesar de que es una de las técnicas más desarrolladas en el momento, también estudia con profundidad el sonido y como a través de este medio puede transportar y camuflar grandes volúmenes de información. Las imágenes a pesar de que poseen técnicas muy avanzadas, siempre se encuentran con el obstáculo de la cantidad de espacio disponible para ocultar un mensaje.

El propósito de esteganografía es comunicación encubierta para esconder un mensaje de un tercero. Lo que difiere de criptografía, el arte secreto de escribir, lo cual está dirigido a hacer un mensaje ilegible por tercera persona pero no esconde la existencia de la comunicación secreta.

Aunque la esteganografía está separada y es discreta de la criptografía, existen muchas analogías entre los dos, y algunos autores clasifican en categorías esteganográficas como una forma de criptografía desde la comunicación oculta sea una forma secreta escribiendo [Bauer, 2002].

En la antigüedad, los mensajes estaban escondidos en la parte trasera de mesas, de la escritura de cera, escritos en los estómagos de los conejos o tatuado en el cuero

cabelludo de esclavos. La tinta invisible ha estado funcionando por siglos para la diversión de los niños y estudiantes y para el espionaje serio por espías y terroristas.

- *Polygraphiæ (1516) -Tritheim Johannes Heidenberg*, segunda publicación relacionada con el tema de Tritheim, vuelve a tratar el tema de la escritura y su significado, aunque no es un libro muy importante en el campo de la esteganografía. [HOSMER Y HIDE, 2003]

  No obstante, junto a Steganographia (del mismo autor), sentará las bases de lo que será Schola Steganographica, el considerado como primer libro de esteganografía y criptografía de la historia, y uno de los más importantes.

- *Schola Steganographica (1665) - Gasparis Schott*, el libro es uno de los más importantes en la historia de la criptografía y la esteganografía. [HOSMER Y HIDE, 2003]

  En él se discuten los conocimientos de la época respecto a la escritura oculta o cifrada, algunos de ellos tratados anteriormente, pero que en el libro toman un profundo giro en el enfoque de estudio: Schott se aleja de lo esotérico y lo mágico para enfocar la esteganografía y la criptografía desde el punto de vista de la técnica y la ciencia.

- En el *Whipple Science Museum* de Cambridge se conserva una copia completa e intacta (la de la fotografía) que fue publicada junto a otra obra del mismo autor (Technica curiosa). [HOSMER Y HIDE, 2003]

- *The Pigeon Post into Paris 1870-1871 (1871) - J. D. Hayhurst O.B.E.*, el texto trata el uso de micrografía y escritura oculta en los mensajes enviados por palomas durante la guerra franco-prusiana (1870-1871). [HOSMER Y HIDE, 2003]

  Según el texto, las técnicas de ocultación de información fueron decisivas en el desenlace de la contienda.

- *La cryptographie militaire (1883) - Auguste Kerckhoffs*, es el uso de técnicas criptográficas, esteganográficas y en general de ocultación de información en el ejército francés del siglo XIX. [HOSMER Y HIDE, 2003]

- Cualquier estudioso de la criptografía ha oído al menos hablar de los Principios de Kerckhoffs. Pues los principios fueron enunciados en Enero de 1883 durante la redacción del libro. [HOSMER Y HIDE, 2003]

- *Le filigrane (1907) - Charles-Moïse Briquet*, la publicación es un diccionario histórico de las marcas de agua, usadas a lo largo de la historia para autentificar todo tipo de documentos. Hoy en día las marcas de agua siguen usándose en la expedición de papel moneda. [HOSMER Y HIDE, 2003]

- *The Codebreakers: The story of secret writing (1967) - David Kahn - [KAHN67]* - Actualizado 1996, es un libro de obligada lectura para los aficionados a la criptografía, esteganografía y ocultación de información en general. [HOSMER Y HIDE, 2003]

Se trata de "La Biblia" de los códigos, formando un texto de referencia histórica incomparable. El autor barre un periodo de tiempo descomunal, desde los primeros jeroglíficos del 3000 A.C. hasta la época de publicación de la primera edición del libro (1967). [HOSMER Y HIDE, 2003]

El hecho de que el libro fuera publicado antes de la existencia de la moderna criptografía computacional no hace sino aumentar el valor intrínseco del texto, pues muestra las entrañas de la teoría de códigos. El libro también muestra episodios históricos importantes relacionados con la ocultación de información, como el Telegrama Zimmermann de la I Guerra Mundial o el funcionamiento y ruptura de las máquinas Enigma de la II Guerra Mundial. [HOSMER Y HIDE, 2003]

El libro fue revisado en 1996 por el propio autor para contemplar la moderna criptografía de clave pública y la influencia de la informática en la ocultación de información. Aún así, no son muchos los cambios entre ediciones, y podríamos decir que el libro sigue siendo algo que pertenece a 1967. El proceso de la esteganografía generalmente implica

colocar un mensaje escondido en algún medio de transporte. El mensaje secreto está incrustado en el transportador para formar el medio de esteganografía. El uso de una llave del esteganografía puede ser utilizado para códigos del mensaje escondido y/o para la aleatorización en el plan del esteganografía. [HOSMER Y HIDE, 2003]

La esteganografía usa métodos científicos para esconder un mensaje, como el uso de tinta invisible y otros clasifican según el tamaño de los métodos de reducción.

2.2 TIPOS DE ESTEGANOGRAFÍA

La esteganografía lingüística esconde el mensaje en el transportador en algunas formas poco obvias y está más allá clasificado en categorías como los códigos abiertos.

Los códigos abiertos esconden información con el uso de símbolos o las señales, un código abierto visual usa objetos de aspecto inocente para transportar un mensaje, como garabatos o el posicionamiento de artículos en un escritorio o un sitio Web. Un código abierto del texto esconde un mensaje modificando la apariencia del texto del transportador como los usados en imprentas que dimensionan o mecanografían, sumando espacios adicionales.

Los códigos abiertos esconden un mensaje en un mensaje legítimo del transportador en las formas que no son observables por el ojo humano ni por un observador ingenuo. El mensaje del transportador es algunas veces llamado comunicación abierta, mientras que el mensaje escondido es la comunicación encubierta. La categoría se subdivide en el lenguaje de codificación y las cifras cubiertas.

Las cifras cubiertas o de ocultamiento esconden un mensaje abiertamente en el medio del transportador a fin de que puedan ser recobrados por alguien que sabe el secreto para ser leído. Una cifra del enrejado utiliza una plantilla que se usa para cubrir el mensaje del transportador. Las palabras que aparecen en las aberturas de la plantilla son el mensaje escondido. Una cifra nula esconde el mensaje según lo planeado de antemano que pasa a ser un conjunto de reglas, como “la lectura a cada quinta palabra” o “mirada en el tercer carácter en cada palabra”. [HOSMER Y HIDE, 2003]

Con un costo creciente de datos se guarda en computadoras y transmitido sobre

redes, no es de extrañar que la esteganografía se haya introducido en la edad digital. En computadoras y redes, las aplicaciones esteganográficas tiene previstas alguien para esconder cualquier tipo de archivos binarios en algún otro archivo binario, aunque la imagen y los archivos de audio son la mayoría de transportadores comunes de hoy.

Esteganografía provee algunas funciones muy útiles comercialmente importantes en el mundo digital, entre ellas se encuentra *watermarking* en la aplicación el autor puede insertar un mensaje escondido en un archivo a fin de que la propiedad intelectual no sea alterada.

La esteganografía tiene un número de aplicaciones ilegales, la mayoría notablemente es de actividad ilegal, fraude financiero, espionaje industrial y comunicación entre miembros de organizaciones criminales o terroristas [HOSMER Y HIDE, 2003]

2.3 CIFRAS NULAS

Históricamente las cifras nulas son una forma para esconder un mensaje en otro sin el uso de un algoritmo complicado. Una de las cifras nulas más simples se muestra en el siguiente ejemplo:

- *"El presidente el regir embargos debería tener aviso inmediato, calafatee situación afectando derecho internacional, la declaración presagia ruina de muchos neutrales. Las publicaciones amarillas unificando escitacion nacional inmensamente. Aparentemente neutral el sistema intermedio de protesta completamente descontó operador booleano and ignorado. Isman duramente golpe. El asunto de bloqueo afecta pretexto para el embargo en subproductos, eyectadno sebos y aceites vegetales".*

El German Embassy en Washington, envió los mensajes en telegramas a su centro de operaciones en Berlín durante la Primera Guerra Mundial. Leer el primer carácter de cada palabra en el primer mensaje o el segundo carácter de cada palabra, leído en el segundo mensaje producirá el siguiente texto escondido:

- *"Pershing navega de nueva york el 1 de junio"* [KAHN, 1996]

En el internet, el correo electrónico masivo no solicitado es un medio potencial del

transportador para los mensajes escondidos. Consideremos lo siguiente:

- *"¡Estimado Amigo, La Presente estaba especialmente seleccionada para serle enviada! ¡Cumpliremos con todo lo que la remoción pide! Este correo está siendo enviado en conformidad con cuenta del Senado 1621; Título 5; ¡Sección 303! No nos confunda con artistas de estafa de la Internet. ¡Por qué trabajar para alguien más cuando ustedes pueden hacerse ricos en un plazo de 38 días! ¡Se han fijado ustedes alguna vez que los resonadores bebés son más exigentes que sus padres y más personas antes que alguna vez deslizarse sobre Internet! ¡Sano, ahora es su probabilidad para sacar provecho de esto! Le ayudaremos a vender más y VENDER MÁS. ¡Ustedes le pueden empezar en absolutamente gratis para ustedes! ¡Pero no nos crea! El Señora Anderson que reside en Missouri nos probó y dice "que Mi único problema ahora está donde para estacionar todos mis autos". Esta oferta es 100 % legal. ¡Ustedes se culparán por siempre si ustedes no hacen el pedido ahora! Contrate a un amigo y su amigo estará rico también. ¡Salud! Estimado Salaryman, Especialmente para ustedes - esto asombrando noticia. ¡Si ustedes no están interesados en nuestras publicaciones y tienen el deseo de ser removidos de nuestras listas, simplemente no responda e ignore este correo! Este correo está siendo enviado en conformidad con cuenta del Senado 2116, Título 3; ¡Sección 306! ¡Ésta es una propuesta de negocio del legitímate! ¡Por qué trabajar para alguien más cuando ustedes pueden hacerse ricos en un plazo de 68 meses! ¡Han notado ustedes alguna vez a más personas antes que alguna vez navegar por la Internet y nadie llega un poco más joven! Sano, ahora es su probabilidad para sacar provecho de esto. Le ayudaremos a disminuir percibido tiempo de espera por 180 % y vender más. ¡Lo mejor acerca de nuestro sistema es que es absolutamente libre de riesgos para ustedes! ¡Pero no nos crea! El Señora Ames de Alabama puso a prueba a nosotros y puntos de vista "que Mi único problema ahora está dónde para estacionar todos mis autos". ¡Estamos autorizados para operar en todos los estados! ¡Ustedes se culparán por siempre si ustedes no hacen el pedido ahora! ¡Contrate a un amigo y ustedes gozarán de una rebaja de 20 %! ¡Gracias! ¡Estimado Salaryman, Su dirección de correo electrónico ha sido enviada a nosotros indicando su interés en nuestra sesión informativa! Si ustedes ya no tienen el deseo de recibir nuestras publicaciones simplemente replican un Tema: De "remove" y ustedes inmediatamente será removido de nuestra lista de correo. Este correo está siendo enviado en conformidad con cuenta del Senado 1618, Título 6, la Sección 307. Esto no*

es uno tiene plan enriquecedor. ¡Por qué trabajar para alguien más cuando ustedes pueden hacerse ricos en un plazo de 17 días! ¡Han notado ustedes alguna vez a más personas antes que alguna vez deslizarse sobre Internet y más personas antes que alguna vez navegar por la Internet! ¡Sano, ahora es su probabilidad para sacar provecho de esto! ¡Le ayudaremos a convertir su negocio en un Comercio Electrónico y entregar mercancías bien para el umbral del cliente! ¡Se garantiza que ustedes tienen éxito porque tomamos todo el riesgo! Pero no nos crea. ¡La Señora Simpson de Wyoming puso a prueba a nosotros y puntos de vista "que Ahora yo estoy rico, Rich, rico"! Le reconfortamos que operamos dentro de todas las leyes aplicables. ¡Le hacemos plegarias - actúe ahora! Contrate a un amigo y ustedes gozarán de una rebaja de 50 %. Gracias para su consideración seria de nuestra oferta."

El mensaje se parece al correo electrónico masivo no solicitado típico, lo cual está generalmente ignorado y descartado, el mensaje fue creado en la mímica del coreo electrónico masivo no solicitado usando una primera parte de idea de mímica basada en la gramática dijo Peter Wayner. [WAYNER, 2002]

Para cualquier persona no entendería absolutamente nada sobre el mensaje descrito anteriormente, considerando las palabras espaciadas o por la falta de ortografía en el mensaje. Los ceros y los unos están codificados por la elección de las palabras. El mensaje escondido en el transportador del correo electrónico masivo no solicitado es:

- *"encuéntrese en cañería maestra y willard a las 8:30"*

El número extraordinario de habilidades a esconder mensajes en archivos digitales usando discordias de una cifra nula no son necesidad. Una imagen o bloque del texto puede estar escondida debajo de otra imagen en un archivo Power Point, en comentario de las páginas web. [ARTZ, 2001].

El texto puede estar escondido en la línea de un documento poniendo el texto en el mismo color como el historial y colocando otro dibujo en primer plano. El receptor podría recuperar el texto escondido cambiando el color. [SEWARD, 2004]

2.4 ESTEGOANÁLISIS

El estegoanálisis se define como el arte y la ciencia de romper la seguridad de un sistema esteganográfico. Existen dos tipos de estegoanálisis según la intención con que se hagan: ataque pasivo, donde sólo se busca detectar el archivo con el mensaje oculto; y el ataque activo, donde se manipula la información secreta.

2.4.1 ESTRATEGIAS PARA IDENTIFICAR Y ANALIZAR DATOS OCULTOS

Los ataques a la esteganografía se refiere a las estrategias implementadas para identificar, analizar y detallar archivos que contengan elementos ocultos, y estos se clasifican en:

- Ataques al esteganograma: el atacante intercepta el esteganograma y por lo tanto puede analizarlo.

- Ataque por repetición de cubierta: Quien creó los esteganogramas ha utilizado el mismo método para ocultar diferentes mensajes. Por lo tanto, el atacante posee diferentes esteganogramas que fueron generados del mismo archivo encubierto.

- Ataque por cubierta conocida: el atacante intercepta el esteganograma y conoce la cubierta que usó para crearlo. Lo que facilita demasiado el trabajo porque detecta inmediatamente cualquier variación por más mínima que sea.

- Ataque por manipulación: el atacante tiene la habilidad de manipular los datos del esteganograma. Lo cual se da gran ventaja de poder eliminar el mensaje oculto en el esteganograma

El estegoanálisis en imágenes: es la detección de esteganogramas utilizados para ocultar información en estas, como uno de los medios más comunes para transportar mensajes ocultos.

Se distinguen dos formas para el tipo de ataques: ataques visuales, que se basan en las capacidades de la vista humana, y los ataques estadísticos, que se basan en la realización de test ala archivo esteganográfico.

- Ataque visual: es un ataque al esteganograma, que se basa en la observación de los bits menos significativos ocultando mensajes de forma aleatoria en los mismos. El tipo de ataque se basa en el juicio humano, que es el que determina si en un archivo de imagen después de pasar un filtro determina que existe un mensaje oculto o no. El algoritmo de filtrado elimina las partes de la imagen que cubren el mensaje. Después del filtrado que da una imagen conformada únicamente de los bits que potencialmente podrían haber sido utilizados para incrustar los bits del mensaje oculto. El filtrado que se vaya a aplicar a la imagen esteganográfica depende totalmente de la función de incrustación que se analice.

  Una de las formas más sencillas de deshabilitar la probabilidad de la existencia de mensaje oculto en las imágenes es comprimiendo el archivo, pasándolo a formato JPG; así no se reconozca en él la existencia de algún mensaje, se realiza este proceso y esto garantiza que si existe el mensaje oculto éste desaparecerá. Aunque es una medida un poco fuerte ya que se ataca de forma deliberada cualquier imagen, garantiza que a la red no va a entrar ningún mensaje oculto en una imagen.

2.5 ESTEGANOGRAFÍA MÁS CRIPTOGRAFÍA

Hay que dejar claro la diferencia entre la criptografía y la esteganografía. Cuando únicamente utilizamos la criptografía, el dato puede ser ilegible, pero es obvio que allí existe un secreto.

Si el dato es sólo oculto y no encriptado, uno puede buscar todos los archivos sospechosos de contener información oculta y percatarse de quien existe esa información que queremos ocultar.

La forma en que actúan juntos criptografía y esteganografía es que la criptografía

hace el dato ilegible a quien no conozca la clave y la esteganografía, oculta además la existencia de esos datos. Así los archivos siendo ocultados, hacen que lo oculto no sea ni leído ni detectado fácilmente.

Hoy en día, con la ayuda de las computadoras ambas técnicas son perfectamente combinables, complementándose la una a la otra y consiguiéndose una seguridad aún mayor.

2.6 IMÁGENES DIGITALES

Las imágenes digitales son fotos electrónicas tomadas de una escena o escaneadas de documentos ya sean fotográficos. Se realiza una muestra de la imagen digital y se confeccionan un mapa de ella en forma de cuadricula de puntos o elementos de la figura (que son llamados pixeles). A cada pixel se le asigna un valor tonal (ya sean negro, blanco matices de gris o color), el cual está representado en un código binario (ceros y unos). Los dígitos binarios ("bits") para cada pixel son almacenados por una computadora en una secuencia, luego la computadora interpreta y lee los bits para producir una versión analógica para su visualización o impresión [KENNEY, RIEGER, 2003].

2.6.1 FICHEROS DE IMAGEN

A pesar de que se pueden utilizar distintos medios para llevar a cabo la función de la esteganografía, como pueden ser sonido, video, texto, programas ejecutables, el medio más utilizado es el fichero gráfico, por ello a continuación se van a ver algunos formatos de este tipo de fichero.

A pesar de que cada tipo de formato se pueda utilizar para una cosa concreta todos ellos tienen características comunes. Estas son las siguientes:

- Contienen una cabecera que identifican el tipo de fichero del que se trata, como puede ser el tamaño de la imagen o el número de colores, que contiene información para interpretar dicho fichero.

- Una vez descomprimidos los datos de un fichero mediante el algoritmo

concreto de cada formato, los datos del fichero indican el color específico de cada pixel de la imagen.

- En función de los colores de la imagen se utilizaran más o menos bits que se indicaran las cantidades de rojo, verde y azul que se utilizara para representar cada color en cada píxel. Debido a que la paleta de colores puede ser modificada según la imagen, es necesario almacenarla en un fichero. Un caso particular es utilizar los 16 millones de colores, en el caso no se utiliza la paleta de colores ya que la relación entre número de color y cantidad del mismo es implícita. De los 24 bits de cada pixel, se utilizan 8 bits por color, es decir, 8 bits para el rojo, 8 bits para el azul y 8 bits para el verde [ROQUE, 2002]

Así cada fichero contendrá una cabecera, los datos de los pixeles, que pueden estar comprimidos o no, y una paleta de colores, a excepción de que se usen los 16 millones de colores es decir, 24 bits por pixel.

Los ficheros de imagen son todos aquellos en los cuales se guarda información la cual será interpretada para mostrar pixeles en distintos tonos de color. Por su simplicidad de estructura (en condigo binario), las imágenes son el formato más utilizado en el campo de la esteganografía. Se dividen en distintos formatos los cuales son:

- *Windows Bitmap* (.bmp): Es el formato gráfico más simple, pues el mismo no es siquiera formato de compresión, por su sencillez es el mejor formato para practicar la esteganografía, pero por no recibir ningún tipo de compresión son demasiados pesados. El formato está compuesto simplemente por una cabecera y el código que representa cada pixel, por ello pueden ser 4, 8 ,16 ó 32 dependiendo del tamaño de la paleta de color.

- *Graphics image format* (.gif): el formato ofrece una de las mejores compresiones, sobre todo si las imágenes de alta calidad ocupan grandes áreas del mismo color. [ROQUE, 2002]

También es el más indicado para guardar la información creada en flash o bien animaciones creadas por algún programa grafico como *image ready*, el formato también acepta transparencia lo cual es una función muy usada en creación de logos y diseños gráficos que no tienen un contorno uniforme.

Una de sus principales desventajas es que el formato solo acepta una paleta de 256 colores lo cual es equivalente a 8 bits, y lo hace como un mal formato para fotos digitales o imágenes que intentan dar una apariencia realista.

- *Join Photographic Esperts Group* (.jpeg): el fichero es por muchos él más conocido en la actualidad, no solo por la compresión que ofrece, sino que varias cámaras y celulares guardan fotos en el formato. [ROQUE, 2002]

Dado que las imágenes comunes que son observables por el ojo humano solo se encuentran en la paleta de 24 bits, los demás colores y matices variables, no son completamente observables por el ojo humano. El formato *.jpeg* se encarga de eliminarlas, es así como obtiene una enorme ventaja de compresión.

El principal problema de su compresión es que una vez que entra en acción, la imagen perderá mucha información lo cual no podrá ser recuperable, y en caso de querer transformar un *.jpeg* a otro formato no se podrá tener la calidad original con la que se creó dicha imagen.

- PC *Paintbrush (.psx)*: El Pc *paintbrush* es la mejora del .bmp el cual ofrece una compresión en información igualitaria, también llamado como algoritmo RLE, lo que hace el RLE es guardar información correspondiente a cada bit de la imagen:
  Explicando una imagen guarda 3 bits de imagen así; bit1 color amarillo, bit2 color café y bit3 color amarillo. El RLE lo guardaría como: bit1 y 3 como color amarillo y bit2 color café. A pesar de la ocultación aún deja el inconveniente de imágenes un poco pesadas, por lo cual sigue siendo recomendable usar otros formatos en la esteganografía.

- *Portable Network Graphics (.png)*: El formato .png se creó con la intención de

igualar las funciones que otorgaba un archivo .gif. Lo que lo hace especial es el tamaño menor a un .gif y aún asi aplicando transparencias y efectos de colores pesados. El formato .png acepta una paleta superior a 256 colores sobrepasando por ello a .gif.

Figura 2.6.1 Ficheros de imagen

Fuente: Modificado de [xionexsystems.com]

Como se puede ver en la imagen existen muchos tipos de formatos de imágenes pero lo que se mencionó anteriormente son los más recomendables para la esteganografía.

Todos los formatos aumentan su calidad y eficiencia en la esteganografía dependiendo de cuantos colores permitan usar, es debido a que todos los colores existente, visibles o no visibles para el ojo humano, se representan en información binaria y entre mas colores manejemos más fácil será ocultar un mensaje en una imagen digital. [ROQUE, 2002]

Explicando mejor se tiene una tabla de bits (paleta) y a cuantos colores es equivalente cada una de ellas. Como se puede ver en la figura 2.6.2 es una cantidad inmensa de colores, si se modificara algunos de los bits en una imagen de 16 colores se correría el riesgo de la misma fuese descubierta y no sería apto para realizar una esteganografía eficaz. Pero si se modificara en imágenes de 294, 976 colores, el cambo en una cantidad tan colosal de colores, sería casi imposible de identificar por medio del ojo humano. [ROQUE, 2002]

Es por eso que la cantidad de colores es siempre importante en la esteganografía, así como también las dimensiones de la imagen con la que se trabaje.

Figura 2.6.2 Ficheros de imagen

Bits	Colores
4	16
8	256
16	65.535
24	16.777.216
32	4.294.967.296

Fuente: Modificado de [xionexsystems.com]

2.7 SISTEMAS BÁSICOS

En el mundo de la esteganografía se usan distintos sistemas (especie de lenguaje), los cuales ayudarán en cierta manera a facilitar la ciencia. Los principales son: Binario, Hexadecimal y ASCII.

- Sistema binario: En la informática el sistema binario se representa solo usando 2 símbolos el 1 y el 0, eso por ello que se le otorga el nombre. Por su simplicidad y por poseer únicamente dos dígitos diferentes, el sistema de numeración binario se usa en la electrónica digital y en la informática para el manejo de datos e información.

  A cada digito binario se le llama BIT y al conjunto de 8 bits se le llama byte, por ejemplo: 110 contiene 3 bits, 1001 contiene 4 bits. Como el sistema binario usa la notación posicional entonces el valor de cada digito depende de la posición que tiene el número.

- Sistema Hexadecimal: El sistema es de base 16, quiere decir que utiliza como símbolos de diez dígitos decimales y las primeras seis letras del alfabeto y son entonces: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F). Para contar en Hexadecimal se inicia de 0. 1. 2… hasta llegar a su último digito que es F.

- Código ASCII: No se trata de un lenguaje o sistema, se trata de un código, el nombre ASCII se debe a un acrónimo ingles que significa: *American Standard Code for Information Interchange.* Que en español significa: Código Estadounidense Estándar para el Intercambio de Información.

Cada símbolo en la computadora tiene una especie de equivalencia numérica. Es decir que tanto el alfabeto y números se representan por un número.

2.8 MÉTODO (LSB).

El método LSB (*Least Significant BIT Insertion*) – (Inserción en el BIT menos significativo), como bien lo dice su nombre, es un método que consiste en insertar información en el bit con menos valor, significa que se hace la modificación para que la imagen no sea demasiado notoria.

La técnica puede ser usada para video y audio, pero es más recomendable en imágenes, por su alta definición en dimensiones y calidad, será casi imposible que algún cambio se pueda detectar.

2.9 FORMAS DE ESTEGANOGRAFÍA EN IMÁGENES

La información puede ser escondida de diferentes formas en imágenes.

Para esconder la información el programa puede codificar cada bit de la información a lo largo de la imagen, robando un bit de cada pixel de la imagen o selectivamente colocar el mensaje en áreas "ruidosas" de la imagen que no atraen la atención, por ejemplo el cielo.

El método de Inserción del último bit menos significativo (LSB) es el más común para lograr almacenar información en una imagen, y los parámetros importantes para tomar en cuenta en la representación de imágenes son:

- Pixel: Es la unidad mínima de visualización para imágenes digitalizadas. Las imágenes digitales están compuestas por píxeles. Las cámaras digitales capturan las imágenes en pixeles, lo propio el monitor se visualiza en pixeles, entonces se puede determinar cuánto más píxeles contenga la imagen, mayor será su definición y también serán aptas para la esteganografía. [ROQUE, 2002]

- Resolución: Es el grado de detalle de una imagen digital, sea escaneada, fotografiada o impresa. La resolución se puede expresar de diversas formas, por ejemplo: ppp (puntos por pulgada), ppi (pixeles por pulgada). La resolución de un monitor se refiere al número de píxeles por pulgada y en una impresora al número de puntos por pulgada. Cuantos más puntos haya en cada pulgada lineal, mayor calidad se obtendrá a la hora de esteganografiar. [ROQUE, 2002]

- Profundidad de color en bit: Hace referencia al número de bits necesarios para representar cada pixel en una imagen. Cuanto mayor sea la profundidad en bits, más colores habrá en la imagen global. Se utiliza 1 bit para imágenes en blanco y negro (sin grises). Cada vez que se añade otro nivel de profundidad de color en bits se dobla el número de colores disponibles, es decir, 2 bits = 4 colores, 3 bits = 8 colores, etc. Un ajuste de 8 bits genera 256 colores (o tonos de gris), con resultados adecuados para la web. La configuración de 24 bits produce 16,7 millones de colores y es la que se utiliza la mayoría de las aplicaciones de gama alta, ya que ofrece color con realismo fotográfico.[ROQUE, 2002]

2.10 MODELOS DE COLOR

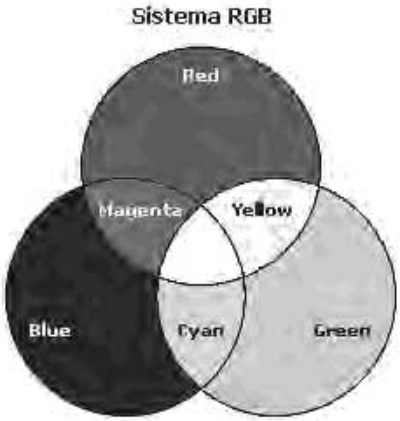
Un modelo de color, es un modelo matemático abstracto que describe la forma en que se representan los colores, por medio de tuplas (conjunto de n elementos) de números. El conjunto de colores posibles que surgen de las tuplas, es conocido como el espacio del color. [MORENO, 2003]

Se necesita un método en específico para definir los colores, los modelos de color proporcionan varios métodos para definir los colores, y cada modelo define los colores mediante componentes de color específicos. Existen diversos modelos de color para elegir cuando se crean gráficos, se tienen:

- Modelo de color RGB: Los colores obtenidos directamente por descomposición de la luz solar o artificialmente mediante focos emisores de luz de una longitud de onda determinada se denominan colores aditivos.

Los colores aditivos son los usados en trabajos de diseño grafico, ya que el monitor produce los puntos de luz partiendo de tres tubos de rayos catódicos, uno rojo, otro verde y otro azul. Por tal motivo, el modelo de definición de colores usados en trabajos digitales es el modelo RGB (Red, Green, Blue). [MORENO, 2003]

Figura 2.10.1 Modelo de color RGB



Fuente: [MORENO, 2003]

Todos los colores que se visualizan en el monitor están en función de las canticades de rojo, verde y azul utilizadas. Por ello, para representar un color en el sistema RGB se le asigna un valor entre 0 y 255 (notación decimal) o entre 00 y FF (notación hexadecimal) para cada uno de los componentes del RGB que lo forman. Los valores más altos de RGB corresponden a una cantidad mayor de luz blanca. Por consecuente, cuantos más altos sean los valores RGB, más claros son los colores.

Un color cualquiera vendrá representado en el sistema RGB mediante la sintaxis decimal (R, G, B) o mediante la sintaxis hexadecimal #RRGGBB. El color rojo puro se especificará como (255, 0, 0) en notación RGB decimal #FF0000 en notación RGB hexadecimal.

- Modelo de color CMYK: La forma aditiva de percibir el color no es única. Cuando la luz solar choca contra la superficie de un objeto, absorbe diferentes longitudes de onda de su espectro total, mientras que refleja otras. Las longitudes de onda reflejadas son precisamente las causantes de los colores en los objetos, colores que por ser producidos por filtrado de longitudes de

onda se denominan colores sustractivos.

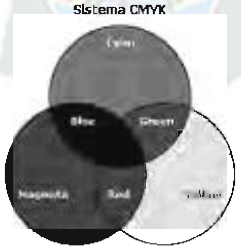
El fenómeno es el que produce en pintura, donde el color final de una zona va a depender de las longitudes de onda de la luz incidente reflejadas por los pigmentos de color de la mima. Un coche es de color azul porque absorbe todas las longitudes de onda que forman la luz solar, excepto la correspondiente al color azul que refleja, mientras que un objeto es blanco porque refleja todo el espectro de ondas que forman la luz, es decir: refleja todos los colores y el resultado de la mezcla de todos ellos da como resultado el blanco. Por su parte, un objeto es negro porque absorbe todas las longitudes de onda del espectro, el negro es la ausencia de luz y de color.

En la concepción sustractiva, los colores primarios son otros, concretamente el cian, el magneta y el amarillo. A partir de los tres colores obtener casi todos los demás colores, salvo el blanco y el negro.

Efectivamente, la mezcla de pigmentos cian, magneta y amarillo no produce el color blanco, sino un color gris sucio. En cuanto, tampoco es posible obtenerlo a partir de los primarios, siendo necesarios incluirlos en el conjunto de colores básicos sustractivos obteniéndose el modelo CMYK (Cyan, Magneta, Black). [MORENO, 2003]

Los colores sustractivos son usados en pintura, imprenta y en general en todas aquellas composiciones en que los colores se obtienen mediante la reflexión de la luz solar, en mezclas de pigmentos (tintas, óleos acuarelas, etc). En las composiciones se obtiene el color blanco mediante el uso de pigmentos de ese color (pintura) o usando un soporte de color blanco y dejando sin pintar las zonas de la composición que deban ser blancas (imprenta).

Figura 2.10.2 Modelo de Color CMYK



Fuente: [MORENO, 2003]

El sistema CMYK define los colores de forma similar a como funciona una impresora de inyección de tinta o una imprenta comercial de cuatricromía. El color resulta de la superposición o de colocar juntas gotas de tinta semitransparente, de los colores cian (un azul brillante), magneta (un color rosa intenso), amarillo y negro, y su notación corresponde a un valor en tanto por ciento de cada uno de los colores.

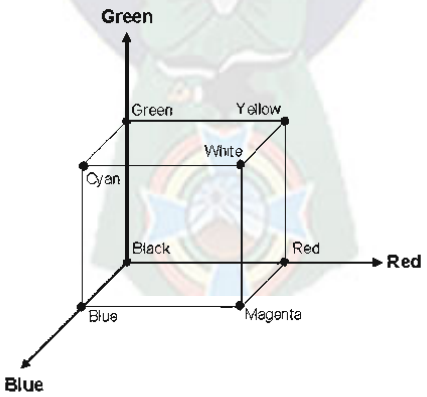
Un color cualquiera vendrá expresado en el sistema CMYK mediante la expresión (C, M, Y, K), en la que figuran los tantos por ciento que el color posee de los componentes básicos del sistema. Por ejemplo (0, 0, 0, 0) es blanco puro (el blanco del papel).

Los sistemas RGB y CMYK se encuentran relacionados, ya que los colores primarios de no son los secundarios del otro (los colores secundarios son los obtenidos a partir de la mezcla directa de los primarios).

2.11 TRANSPORTANDO EN IMAGEN DIGITAL

Muchas técnicas digitales comunes de la esteganografía utilizan imágenes graficas o archivos de audio como el medio del transportador. Entonces para revisar una imagen y su codificación, una manera común para representar un color dado por la intensidad relativa de sus tres componentes de colores (rojo, azul, verde), y tras la ausencia de todos los colores muestran al negro.

Figura 2.11.1 Transportando en imagen digital



Fuente:[Forencis, 2004]

Las aplicaciones de imagen digitales soportan colores de 24 bits donde cada elemento del cuadro (pixeles). Otras aplicaciones codifican los colores usando 8 bits pero no son aptas para la esteganografía.

2.12 MÉTODOS DIGITALES DEL TRANSPORTADOR

Hay muchas formas en las cuales los mensajes pueden estar escondidos en formatos digitales (imágenes). La información también puede estar escondida en una unidad del disco duro en una partición secreta, una partición escondida no se verá bajo ninguna circunstancia normal, aunque la configuración del disco y otras herramientas podrían permitir acceso completo hacia la partición escondida. [JOHNSON, 2001]

La teoría ha sido implementada en un sistema de archivos esteganográficos para Linux. Un escondido sistema de archivos es en particular interesante porque protege al usuario de estar inseparablemente atado a cierta información en una unidad de disco duro, deja al usuario que no obtenga cierta información o afirme que ciertos acontecimientos nunca ocurrieron.

Detrás del sistema los usuarios pueden esconder el número de archivos, para garantizar el secreto del contenido de los archivos y que no pueden desestabilizar archivos pocos escondidos. [ANDERSON, 1998]

Otro transportador digital puede ser la red, que forma canales encubiertos de comunicaciones usando el campo de la identificación en paquetes de Protocolo del internet o el campo de números de secuencia en segmentos de protocolo de control de transmisión. [ROWLAND, 1996]

Hay varias características de sonido que pueden estar alterados en forma que son indiscernibles para los sentidos humanos, y las alteraciones leves, como los cambios diminutos en la frecuencia pueden transportar información escondida. [CURRAN Y BAILEY, 2003]

Para esconder información en una imagen es alterar la orden de los colores en la paleta o codificación del bit menos significativo del uso de los colores en vez de los datos de

la imagen. Los métodos son potencialmente débiles, sin embargo. Muchas herramientas de desarrollo de software de gráficos han sobrepasado los límites de estimación del análisis estadístico. [FRIDRICH Y DU, 2000]

Los métodos de esteganografía son análogos para las radiotransmisiones del espectro (Segunda Guerra Mundial) y comúnmente usado en sistemas de comunicaciones de datos, hoy donde la señal circula (energía), la frecuencia ancha en vez de ser enfocada sobre una sola frecuencia, en un esfuerzo para hacer detección y el atascamiento de la señal más duro. Los métodos se aprovechan del hecho que genera pocas distorsiones para la imagen y los archivos en buen estado son menos detectables en las porciones de alta energía del transportador. [WAYNER, 2002]

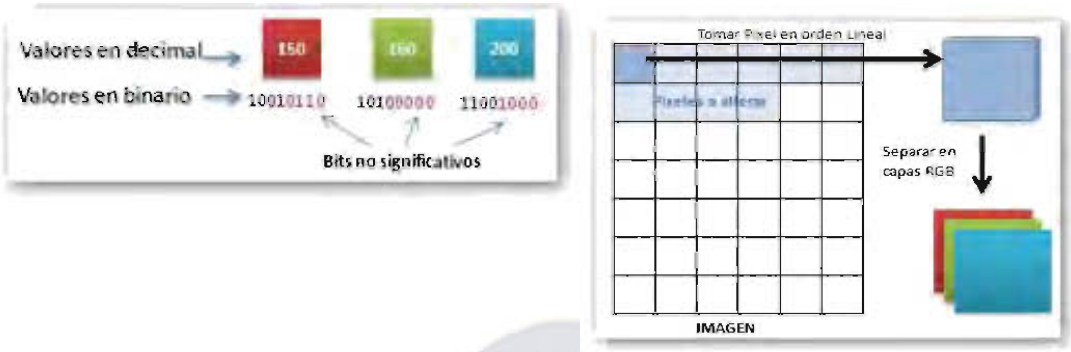
2.13 DISTINTAS TÉCNICAS DE ESTEGANOGRAFÍA

2.13.1 TÉCNICA LINEAL

Denominada asi por el orden secuencial de toma de los pixeles para su manipulación, supongamos que tenemos la letra L y su código ASCII 76 y su código binario 1001100. Deseamos ocultarlo en una imagen, lo primero que hacemos es tomar los pixeles necesarios, separar cada pixel en sus tres capas en RGB obteniendo 3 valores, los cuales convertimos a binario, teniendo los valores originales en bits y la información a ocultar (Letra "L") también en bits, procedemos a aplicar diversas técnicas aritméticas o lógicas entre ambos valores, produciendo un valor nuevo que es el que se enviara al receptor.

Como se puede ver en las figuras 2.13.1 debemos asegurar que los bits a alterar estén entre los 4 menos significativos, para producir una imagen muy parecida al original. Lo adecuado sería tomar solo el primer bit no significativo para producir la mínima alteración visual en caso de que las imágenes sean de mucha importancia.

Figura 2.13.1 Técnica Lineal



Fuente: [UNT 2005]

2.13.2 TÉCNICA BASADO EN KERNELS

La mayoría de técnicas esteganográficas en imágenes toman a los pixeles en orden lineal, pero que pasa si en lugar de tomar los pixeles en orden lineal la hacemos dentro de una matriz de NxM.

2.13.2.1 FUENTE DE INSPIRACIÓN

La forma de tomar pixeles consiste en partir la imagen en pequeñas matrices en dimensiones impar, de igual dimensión que una matriz base escogida denominada kernel espacial; generalmente se utiliza para evaluar al pixel central del kernel, por ello es que las matrices se ocultan. Dependiendo la transformación que quisiéramos hacer a la imagen existen diversas formas de evaluar a los pixeles dentro del kernel. Los pixeles continuos al central se denominan "Vecinos", si están en dirección vertical y horizontal se denominan: "4 Vecinos" y si están en dirección diagonal: "Vecinos Diagonales" y en conjunto toman el nombre de "8 Vecinos" [UNT, 2005]

CAPITULO III

BIT MENOS SIGNIFICATIVO

3.1 MÉTODO DEL BIT MENOS SIGNIFICATIVO

El bit menos significativo consiste en codificar cada bit de la información a lo largo de la imagen quitando un bit de la misma y colocando el bit del mensaje, normalmente se hace en las áreas más ruidosas de la imagen que no atraen la atención, como por ejemplo, un prado o el cielo.

El Método más utilizado del bit menos significativo es:

1. Para una computadora un archivo de imagen es simplemente un archivo que muestra diferentes colores e intensidades de luz en diferentes áreas de una imagen. El mejor tipo de archivo de imagen para ocultar la información es dentro de una imagen de 24 bit BMP (Bitmap).

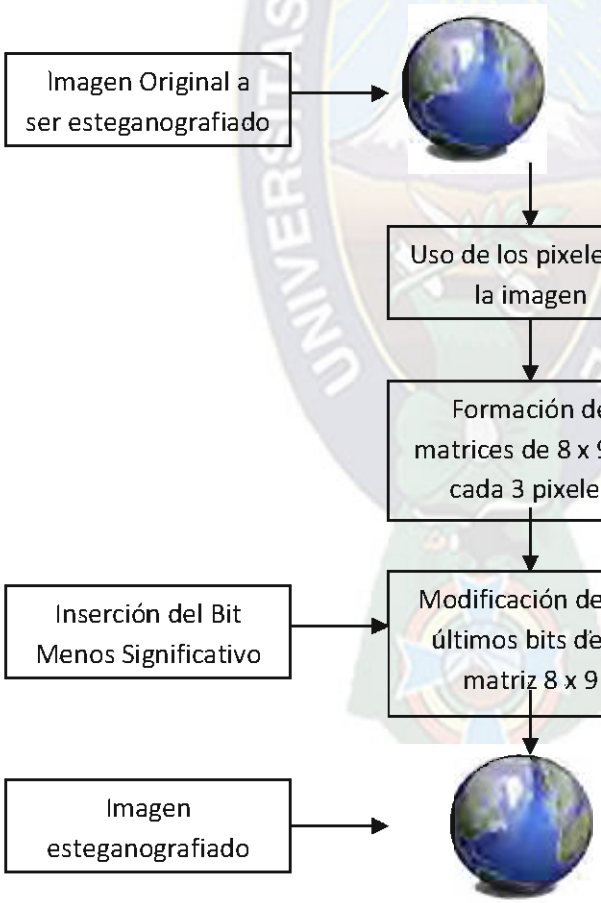
2. Luego consiste en hacer uso del bit menos significativo de los pixeles de una imagen y alterarlos. Radica en el uso de los colores RGB, se obtiene 3 pixeles de la imagen las cuales tienen un valor numérico y estas se transforman en valores binarios formando a su vez una matriz de n x m en este caso (8 x 9).

3. De la matriz se toma los últimos bits del lado derecho los que son denominados bit menos significativos (columna 8 y todas las filas) y estas sufren el cambio por otra columna de datos binarios.

4. La distorsión de la imagen en general se mantiene al mínimo (la percepción es prácticamente nula), mientras el mensaje es esparcido a lo largo de sus pixeles.

El Algoritmo propuesto es la siguiente:

Figura 3.1.1 Método bit menos significativo

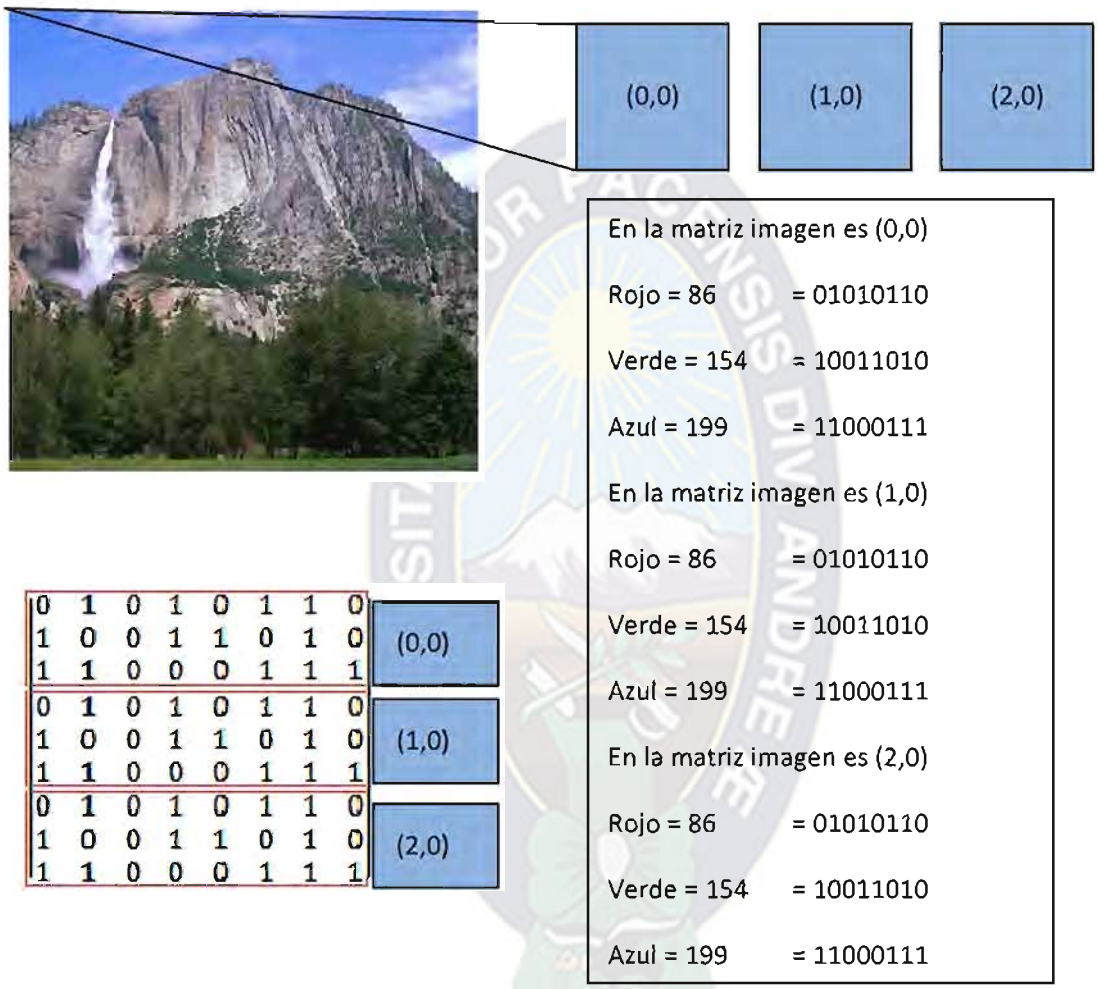


Fuente: [elaboración propia]

El método es de la siguiente forma:

Se extrae los pixeles de una imagen y estas van de acuerdo a las coordenadas (x, y) donde x son las filas, y son las columnas:

Figura 3.1.2 Método bit menos significativo



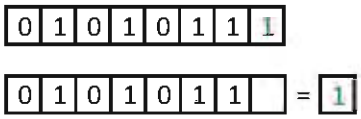
Fuente: [elaboración propia]

2) Se utiliza las instrucciones de corrimiento SHR, que son parte de la capacidad lógica de la computadora, pueden realizar las siguientes acciones: Hacer referencia a un registro o direccion de memoria, recorre bits a la izquierda o a la derecha, recorre hasta 8 bits en un byte.

Los corrimientos hacia la derecha (SHR) mueven los bits hacia la derecha en el registro designado. El bit recorrido fuera del registro es el bit menos significativo cuando

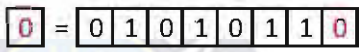
llegue al ultimo bit (0,1,2,3,4,5,6,7) al numero 7 se cambia por el bit que se quiere esteganografiar.

SHR: desplazamiento lógico a la derecha



3) También se utiliza la instrucción INC, que es una instrucción para aumentar en 1 los contenidos de registros y localidades de memoria, dependiendo del resultado la operación apaga o prende (0,1) el ultimo bit.

INC: aumenta en 1 el contenido



En el ejemplo se muestra la inserción de un dato: cuando SHR es igual a 7 desplaza a la derecha el ultimo bit que provoca un acarreo, luego interviene INC que aumenta en un dato el contenido vacio del último bit, para toda la imagen se realiza el mismo procedimiento.

3.2 BASES DE LA ESTEGANOGRAFÍA

Toda información (texto ASCII, hexadecimal, código morse) que se quiere introducir, debe ser primero convertida a binario. Si cualquier base numérica es válida, la comodidad trabajando con binario es mucho mayor.

No se debe permitir que terceras personas obtenga el fichero original (antes de la modificación) el cual permitiría mediante comparación establecer pautas de cambio en la información. Podría llevar en última instancia a descubrir el mensaje oculto.

Las cabeceras de los ficheros no deben ser modificadas.

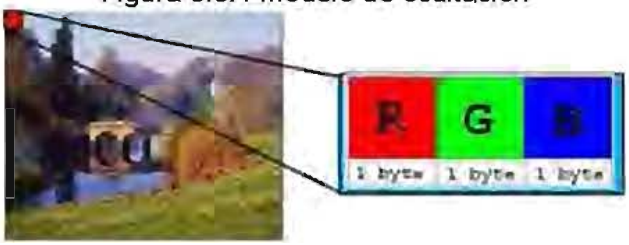
No se debe transmitir la clave o algoritmo esteganográfico por un medio inseguro.

3.3 MODELO DE OCULTACIÓN

Para la computadora, una imagen es una matriz de números que representan intensidades de colores en varios puntos (pixel). Una imagen típica es de 640 x 480 pixeles y

256 colores o (8 bits por pixel).

Figura 3.3.1 modelo de ocultación



Fuente: [elaboración propia]

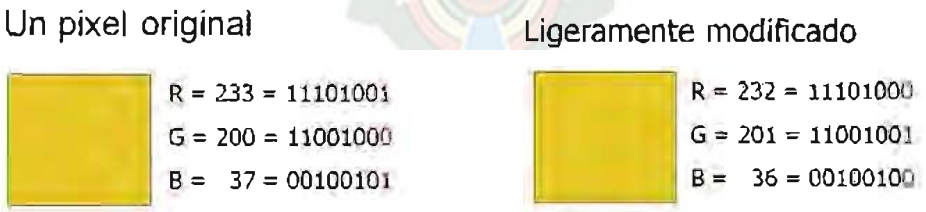
Cada pixel, en un archivo BMP (de 24 bits), está representado por 3 bytes conteniendo la intensidad de color para ROJO, VERDE y AZUL (RGB: red, green, blue). Entonces combinando valores en esas posiciones podemos obtener los: 2^{24} = 16777216 colores

Los colores que puede mostrar un pixel es el dato obtenido anteriormente, habitualmente se dice 16 millones de colores, pero son un poquito más.

Cada byte contiene un valor entre 0 y 255 (en binario 00000000 y 11111111), los bytes igual que en el sistema decimal conforme sus cifras se encuentren mas a la izquierda tendrán más valor.

Explicando: Si tenemos el número **5768**, si cambiamos la primera cifra (la más significativa) a 3 queda **3**768, la diferencia es notable. Pero si cambiamos la última cifra (la menos significativa) por ejemplo a un 2 queda 576**2**, la diferencia es relativamente mínima. Se puede modificar los LSB (*Lest significant bits,* o cifras menos significativas) sin producir mayor alteración.

Figura 3.3.2 modelo de ocultación



Fuente: [elaboración propia]

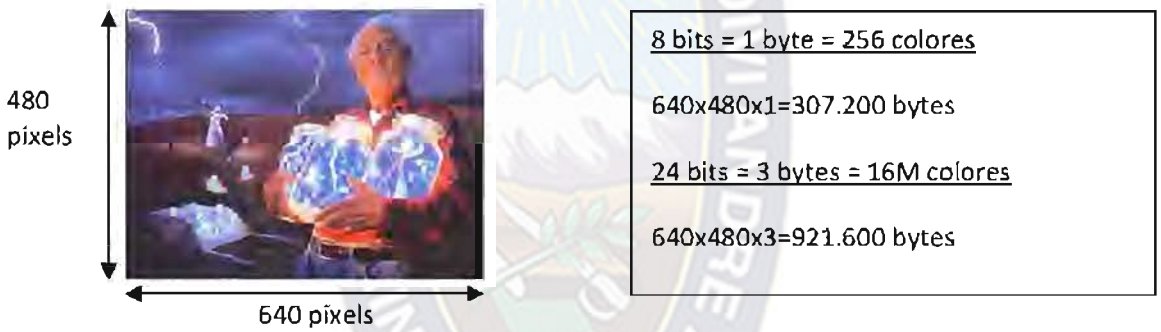
En los dos pixeles anteriores tan solo se le ha modificado una unidad a cada componente R, G, B y la variación de color ha sido mínima. Al ojo humano son prácticamente el mismo color.

Se logra dispersar 3 bits que originalmente eran 101 ahora es de 010, eso significa que por cada pixel podemos almacenar 3 bits sin producri un cambio aparente en el pixel.

Si el paso se repite, recorriendo los pixeles de la imagen, se puede ir ocultando los bits que se quiere dentro de una imagen. En cada pixel se puede poner 3 bits es decir se necesita 8 pixeles para poner 3 bytes (un byte tiene 8 bits)

Las imágenes de 24 bits utilizan 3 bytes por cada pixel para representar un valor de color. Los bytes podrian ser representados en decimal, los valores que podriamos tomar cada uno de los bytes va desde 0 a 255.

Figura 3.3.2 modelo de ocultación



Fuente: [elaboración propia]

3.1 IMPLEMENTACIÓN DEL BIT MENOS SIGNIFICATIVO

El bit menos significativo en base a esteganografía tiene por objetivo ocultar información en los bits menos significativos de un byte, es el método que ahora se utiliza en el caso de imagen.

Para entender mejor tomamos una fracción de tres pixeles que sus valores son convertidos al código binario que es la siguiente:

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Para insertar la letra x, primero consultaremos la tabla ASCII para ver su valor:

Carácter : X
ASCII : 88
Binario : 01011000
Hexadecimal : 58

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

En ejemplo se puede observar que solo sufre una modificación el último bit de cada fila de la matriz y solo la última columna.

3.4 DESTRIPANDO UN BMP

Existe una gran variedad de formatos de imágenes tal como BMP, TIFF, GIF, PNG, JPEG, etc.

El más sencillo de todos es el formato BMP de 24 bits.

Entre sus características se encuentra:

- ❖ No es comprimido (una desventaja con respecto a espacio pero ventaja por su simplicidad)
- ❖ Por no ser comprimido es de alta calidad.
- ❖ Se pude ver en cualquier visor de imágenes por ser el más básico.

Los primeros 54 Bytes contienen los metadatos de la imagen y su estructura es la

siguiente:

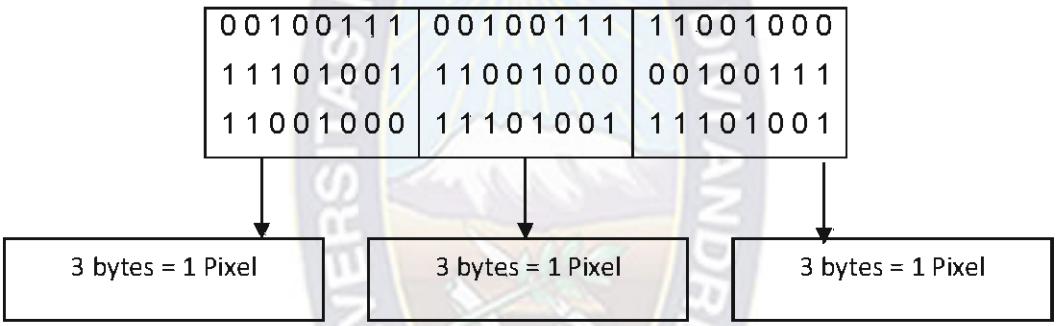
- 2 bytes: Contienen siempre “BM, sirve para poder identificar que realmente es un bmp.
- 4 bytes: Tamaño del archivo (en bytes).
- 4 bytes: Reservados, contienen ceros (son reservados para usos futuros)
- 4 bytes: *Offset*, distancia en bytes entre la cabecera y los pixeles.
- 4 bytes: Tamaño de metadatos (tamaño de su estructura = 40)
- 4 bytes: Ancho (número de pixeles horizontales)
- 4 bytes; Alto (número de pixeles verticales)
- 2 bytes: Número de planos de color
- 2 bytes: Profundidad de color (24 para la imagen)
- 4 bytes: Tipo de compresión (0, ya que el bmp es descomprimida)
- 4 bytes: Tamaño de la estructura imagen.
- 4 bytes: Pixeles por metro horizontal.
- 4 bytes: Pixeles por metro vertical.
- 4 bytes: Cantidad de colores usados.
- 4 bytes: Cantidad de colores importantes.

Suman 54 bytes, y son los primeros 54 bytes que se debe leer del archivo.

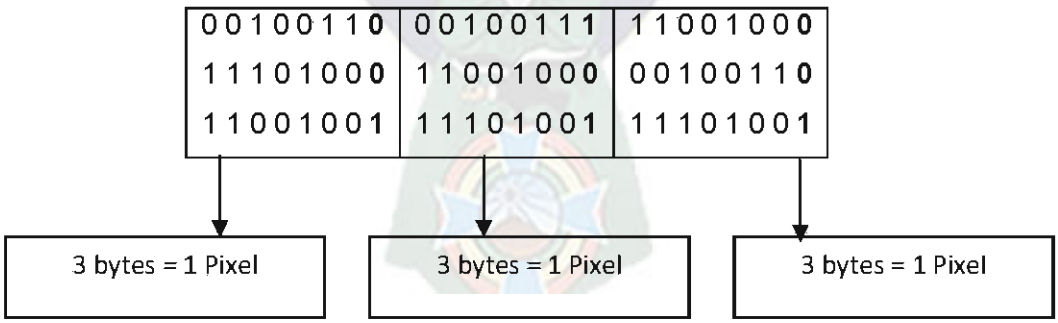
3.4 ALMACENANDO INFORMACIÓN

Almacenar la información que va a ser escondida en una imagen requiere de dos archivos. El primero es la imagen "inocente" que será nuestra cubierta y alojará la información que queremos esconder, el archivo se denomina: Imagen de cubierta. El segundo archivo es el mensaje (la información a esconder). Un mensaje puede ser texto plano, un texto encriptado, otra imagen o cualquier cosa que pueda ser llevado a bits.

Seleccionando 3 pixeles se obtiene:



Se desea almacenar como mensaje oculto un letra como por ejemplo la "C", que código ASCII es 67, en binario seria: 0 1 0 0 0 0 1 1. Se obtiene:



Por tanto cualquier información ya sea texto, número, carácter o símbolo que desea ocultar en una imagen primero se tiene que llevar a lo que es el Código ASCII, luego a Código Binario y finalmente reemplazarlo en la imagen para obtener la imagen

esteganografía.

Figura 3.4.1 Almacenando información

Fuente: [Elaboración Propia]

Lo estándar para esteganografiar es utilizar el formato BMP, cuando se tiene que esconder información dentro de una imagen en formato BMP, el primer paso es seleccionar la imagen en donde esconder la información. Se debe elegir una imagen que no posea grandes aéreas de colores sólidos.

Una vez que la imagen se selecciona hay que pasar al paso de seleccionar la técnica que se va a utilizar para esconder la información (Bit menos significativo).

3.5 FORMAS DE ESTEGANOGRAFIAR EN IMÁGENES

La información puede ser escondida de diferentes formas en imágenes.

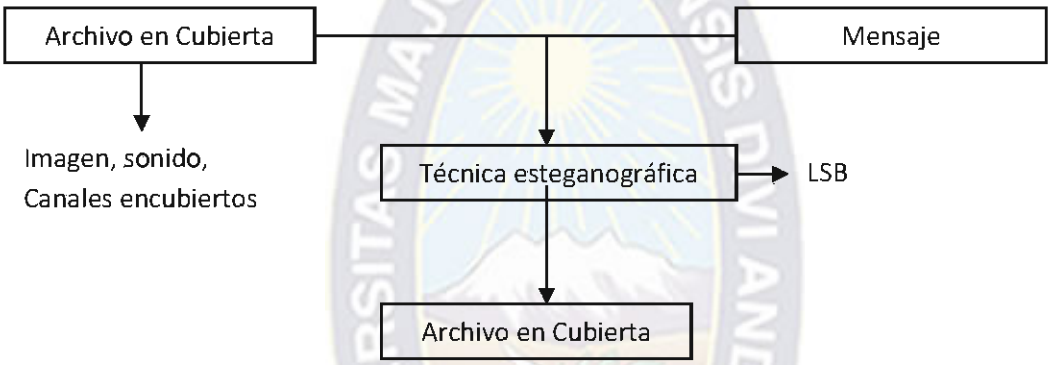
Para esconder la información el software puede codificar cada bit de la información a lo largo de la imagen, robando un bit de cada pixel de la imagen o selectivamente colocar el mensaje en áreas "ruidosas" de la imagen que no atraen la atención (por ejemplo el cielo).

El método del bit menos significativo almacena información en una imagen, también es vulnerable a la manipulación de la imagen. Como por ejemplo si tenemos un archivo BMP, con nuestra información escondida y lo convertimos a .JPEG, el archivo grafico seguirá igual, pero toda nuestra información escondida se perderá para siempre.

Para esconder información en una imagen de 24 bits utilizando el método de inserción del último bit significante, se puede almacenar 3 bits en cada pixel.

Una imagen de alta resolución de 1024 x 768 en 24 bits en tamaño real ocupa: 2.359.296 Kb, si se utiliza el ultimo bit de cada byte de la imagen de cubierta para almacenar nuestra información, quedan unos 294.912 Kb para almacenar información. Si a su vez la información es compactada, por ejemplo se podría esconder un documento de Word de unas 300 hojas sin que exista ninguna variación en la imagen para el ojo humano.

Para comprender mejor el diagrama de esbozo que se lleva a cabo en el momento en que se oculta un mensaje en cualquier medio disponible que se haya escogido.



El esteganograma es el resultado de infiltrar el mensaje secreto en la cubierta. Para develar el esteganograma no se requiere de la cubierta original.

3.6 AVANCE DEL SOFTWARE

Para el desarrollo del software, es conveniente utilizar el modelo de la ingeniería de software para el desarrollo de software.

Para crear una aplicación software, se debe describir el problema, las necesidades o requerimientos que la necesita, en qué consiste el problema y que debe hacerse, luego se realiza un diseño rápido que pone de relieve una solución lógica, como el sistema cumple con los requerimientos, después la construcción del software se encarga de codificarlo en un lenguaje de programación, para luego utilizar el software con el fin de identificar los cambios y mejoras que sean necesarios, por último el software se revisa para realizar cambios y mejoras repitiendo el proceso varias veces.

3.6.1 TECNOLOGÍA EMPLEADA

El lenguaje de programación en el que se ha implementa el software, es Delphi 7.0, proporciona muchas características deseables para el desarrollo de prototipos, es un lenguaje orientado a objetos y desarrollado para un entorno Windows, es una herramienta visual ideal en la construcción de interfaz gráfica para los usuarios, la aplicación terminada es un archivo ejecutable.

La facilidad del lenguaje permite crear aplicaciones en muy poco tiempo. En otras palabras, permite un desarrollo eficaz y menor inversión en tiempo que con otros lenguajes.

3.6.2 DESCRIPCIÓN DE LOS REQUERIMIENTOS

El desarrollo del software para el sistema de ocultación de datos utilizando el método del bit menos significativo, tiene por objetivo crear un software con fines de estudio en base a la técnica planteada anteriormente.

Los usuarios del sistema serán las personas que deseen utilizar el software y realizar pruebas con la técnica de ocultación propuesta, a continuación se detalla los procesos que sistema debe realizar:

Figura 3.6.2 Descripción de requerimientos

REFERENCIA	PROCESO
1	Abrir un archivo de imagen en pantalla para ocultar el o los datos
2	Realizar el ocultamiento de datos en una imagen cargada en pantalla.
3	Permitir guardar la imagen con datos ocultos en el formato establecido .BMP
4	Permitir recuperar en pantalla una imagen esteganografiada por el sistema
5	Mostrar en pantalla la imagen original y la imagen esteganografiada, para poder comparar visualmente ambas imágenes
6	Mostrar en pantalla el texto oculto
7	Mostrar el proceso que se uso para la ocultación de los datos en la imagen

Fuente: [Elaboración propia]

Además el sistema funcionará bajo la plataforma Windows xp o superior, y será de fácil utilización para los usuarios.

3.7 DISEÑO DE DATOS

El diseño de datos es una de las fases más importantes en el desarrollo de software, traduce los objetos de datos en estructuras globales a nivel de componentes de software.

A continuación se presenta el diseño de algoritmos para la ocultación de datos y el proceso inverso de desocultar el texto:

Figura 3.7.1 Diseño de datos

```
INICIO
bytesKernel←floor((tamKernel^2)/9);
kernels[3]←  crearTresMatrices de (tamKernel x
tamKernel);
bits[9* bytesKernel]
Final=false;
FOR i←0; i<=N – tamKernel AND NOT Final;
i=i+tamKernel DO
FOR j←0; j<=M –tamKernel AND NOT Final;
j=j+tamKernel DO
copiarAKernels(imagen, kernels, i, j, tamKernel);
FOR c←0; c<3 AND NOT Final ; c++ DO
sacarBistDeKernel(kernel[c], bits, tamKernel);
FOR b←0; b<bytesKernel; b++ DO
car←convertirACaracter(bits, b*9);
IF car != terminal THEN
texto ←  texto +car;
ELSE
Final=true;
END IF
END FOR
END FOR
END FOR
END FOR
retornar texto;
      FIN
```

```
INICIO
bytesKernel←floor((tamKernel^2)/9);
maxBytes←calcularMaxCaracteres(bytesKenel, tamKernel);
lenText←  tamañoTexto(texto);
IF lenText > maxBytes THEN
retonar Error(" Texto muy grande");
END IF
kernels[3]←  crear tres Matrices de (tamKernel x tamKernel);
bits[9* bytesKernel]
Final=false;
posT=1;
FOR i←0; i<=N – tamKernel AND NOT Final; i=i+tamKernel
DO
FOR j←0; j<=M –tamKernel AND NOT Final; j=j+tamKernel
DO
copiarAKernels(imagen, kernels, i, j, tamKernel);
FOR c←0; c<3 AND NOT Final ; c++ DO
limpiarBits(bits, 9 x bytesKernel);
FOR b←0; b<bytesKernel; b++ DO
IF post <= lenText THEN
car←texto[posT];
ELSE
FINAL ←  true;
Car ←  terminal;
END IF
convertirABits(car, bits, b*9);
posT←  posT + 1;
END FOR
colocarBistEnKernel(kernel[c], bits, tamKernel);
END FOR
```

Fuente: [elaboración propia]

3.8 DISEÑO DE LA INTERFAZ DE USUARIO

El diseño de interfaz de usuario crea un medio de comunicación efectivo entre un ser humano y una computadora, creando un formato en pantalla que permite al usuario interactuar con el sistema [PRESSMAN, 2007]

3.9 PRESENTACIÓN DE LA HERRAMIENTA

3.9.1 INICIO DEL SOFTWARE

SITUACIÓN. La presentación de la figura 3.9.1 del software da las diferentes opciones que podemos realizar para el proceso de la ocultación de los datos que el usuario quiera realizar, muestra las opciones de abrir una imagen, borrar texto, ocultar texto, mostrar texto, guardar la imagen esteganografiada, el proceso que se da de guardar el texto oculto, borrar el proceso de corrido de la ocultación de los datos.

3.9.1 Presentación de la herramienta

Fuente: [Elaboración Propia]

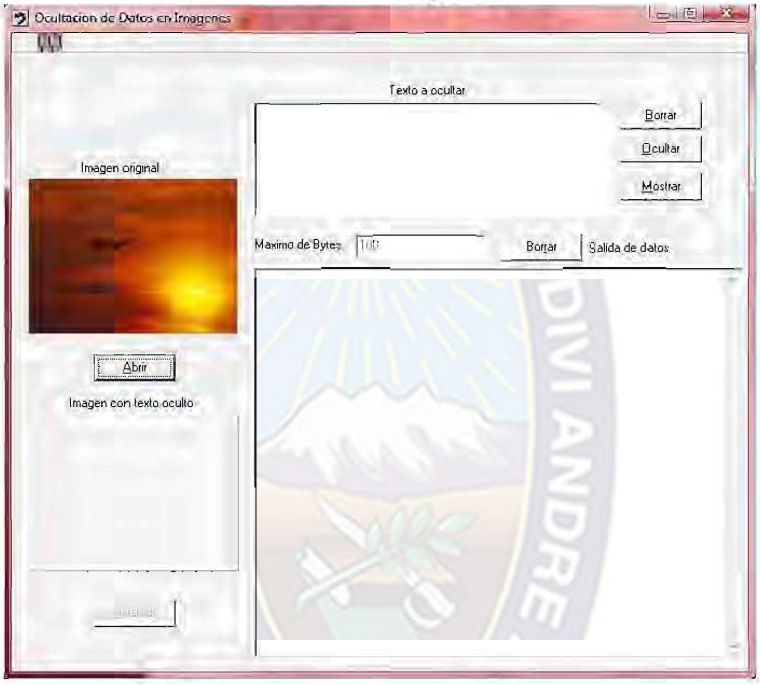
RESULTADO. La figura 3.9.1 del software donde se muestra la primera opción de llenar texto para la ocultación de textos en imágenes, con la segunda opción de muestra de la corrida de los datos ocultos.

CONCLUSIÓN. Se puede mostrar que el software es muy sencillo de usar para cualquier usuario que desee ocultar información y que sea enviada a un receptor.

3.9.2 ABRIR IMÁGENES

SITUACIÓN. La figura 3.9.2 muestra la opción de abrir una imagen con formato BMP que consiste en una cabecera y a continuación los valores de cada pixel siguiendo un orden de abajo hacia arriba, es decir, desde la última línea hasta la primera, y de izquierda a derecha. Permite comprensión y una ventaja es la sencillez en contraposición al gran tamaño de los ficheros.

3.9.2 Abrir imágenes



Fuente: [Elaboración Propia]

RESULTADO. La figura 3.9.2 del software donde se muestra en la imagen en izquierda es el original, y donde con el botón Abrir se puede abrir imágenes del tipo BMP, la versión de la primera opción de escribir el texto para la ocultación de datos en dicha imagen.

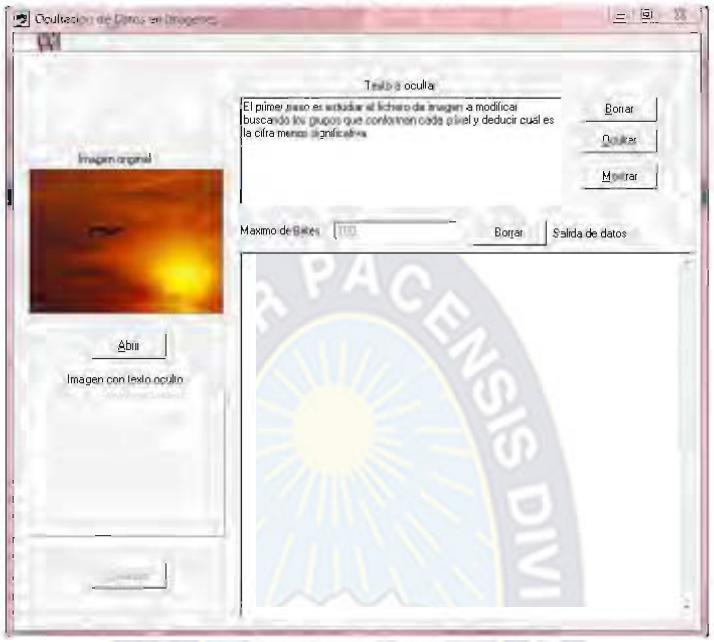
CONCLUSIÓN. Se puede mostrar que el software ejemplifica la imagen original para luego ser llenado con datos en su interior.

3.9.3 LLENAR DATOS

SITUACIÓN. La figura 3.9.3 muestra la opción de llenar los datos en los bits menos

significativos, se puede llenar los datos que está en un rango de 100 – 500 caracteres de letras, entre los llenados depende de la imagen que uno abre puede ser de acuerdo al tamaño de la imagen, el número de bits que puede tener dicha imagen.

3.9.3 Llenar datos



Fuente: [Elaboración Propia]

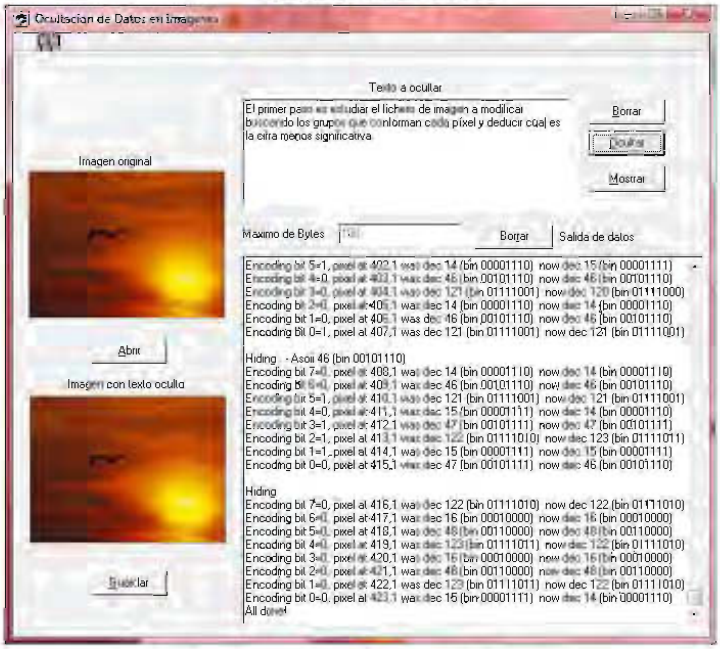
RESULTADO. La figura 3.9.3 del software donde se muestra en la imagen, en la versión de la primera opción de escribir el texto para la ocultación de datos en dicha imagen se puede escribir la cantidad de texto de 100 – 500 palabras.

CONCLUSIÓN. Se puede mostrar que el software ejemplifica la imagen original y el texto escrito para luego ocultar dicho texto en la imagen.

3.9.4 OCULTAR DATOS

SITUACIÓN. La figura 3.9.4 muestra la opción de ocultar el texto que es introducido por el usuario el texto escrito como se ve en la figura no es tan largo entonces lo que hace el software es simplemente reemplazarlos en los bits menos significativos y se muestra en la segunda opción el resultado de la ocultación letra por letra.

3.9.4 Ocultar datos



Fuente: [Elaboración Propia]

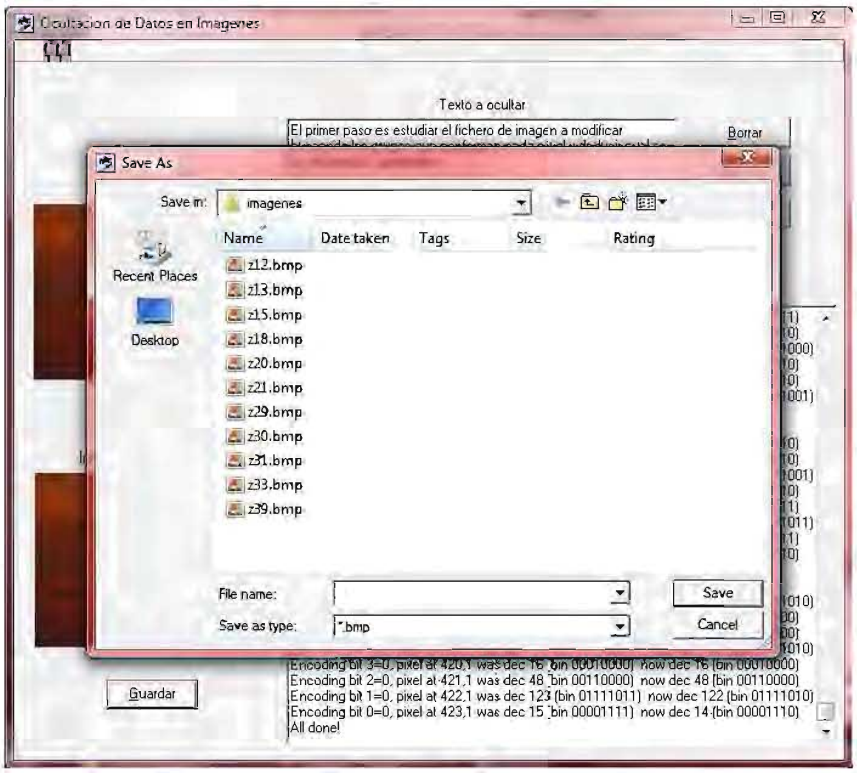
RESULTADO. La figura 3.9.4 del software donde se muestra en la imagen, en la versión de la primera opción de escribir el texto para la ocultación de datos en dicha imagen se puede escribir la cantidad de texto de 100 – 500 palabras. Donde luego se ve en la figura en la opción de impresión de los resultados de la ocultación del texto en los pixeles de la imagen.

CONCLUSIÓN. Se puede mostrar que el software ejemplifica la imagen original y la imagen esteganografiada el texto escrito que luego es oculto en los pixeles de la imagen.

3.9.5 GUARDAR IMAGEN

SITUACIÓN. La figura 3.9.5 muestra la opción de guardar una imagen con formato BMP que consiste en una cabecera y a continuación los valores de cada pixel siguiendo un orden de abajo hacia arriba, es decir, desde la última línea hasta la primera, y de izquierda a derecha. Además va con el texto oculto dentro de sus pixeles sin una ampliación en el tamaño o cambio de colores en la imagen.

3.9.5 Guardar imagen



Fuente: [Elaboración Propia]

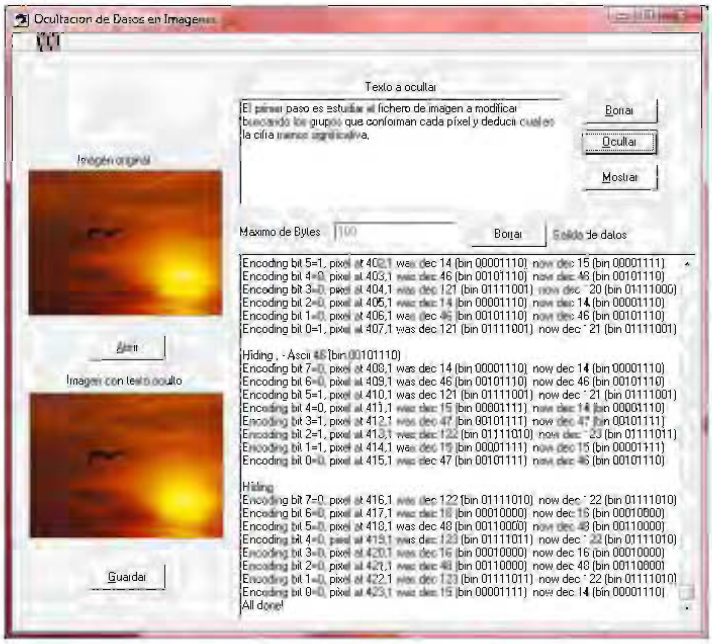
RESULTADO. La figura 3.9.5 del software donde se visualiza la ventana de guardar la imagen en un directorio donde el usuario desearía guardar con el formato original BMP con un nombre distinto o con el mismo nombre.

CONCLUSIÓN. Se puede mostrar que el software ejemplifica el momento en que el usuario guarda la imagen esteganografiada en un directorio con el mismo formato BMP.

3.9.6 MOSTRAR DATOS

SITUACIÓN. La figura 3.9.6 muestra la opción de mostrar los datos ya esteganografiados en la imagen esteganografiada donde primero se visualiza los pixeles donde se guardó el texto que el usuario escribió para un receptor.

3.9.6 Mostrar datos



Fuente: [Elaboración Propia]

RESULTADO. La figura 3.9.6 del software donde se visualiza la imagen esteganografiada con el texto oculto y los pixeles donde se guarda el texto a ocultar.

CONCLUSIÓN. Se puede mostrar que el software ejemplifica la imagen esteganografiada con el texto oculto y los pixeles donde se oculto dicho texto.

3.11 CASOS DE PRUEBA

Las pruebas para la técnica de ocultación de datos en imágenes digitales utilizando el método del bit menos significativo, se realizan utilizando el software desarrollado.

3.11.1 PRUEBA 1

Nombre del archivo:	a1.bmp
Máximo de datos a escribir:	479.888 bits
Tipo de imagen:	24 bits

3.11.1.1 Prueba 1

Fuente: [Archivo de imagen de la Web]

3.11.1.2 Prueba 1

Como se puede observar al restaurar la imagen no muestra un mensaje solo contiene información que es basura y se procede a esconder información.

Aplicando el software se tiene, para el proceso de ocultación de datos en la imagen, y que no contenga mensajes que no son entendibles se procede a esconder una información que sea entendible:

3.11.1.3 Prueba 1

Fuente: [Elaboración propia]

3.11.2 Prueba 2

Nombre del archivo:	a2.bmp
Máximo de datos a escribir:	479.888 bits
Tipo de imagen:	24 bits

3.11.2.1 Prueba 2

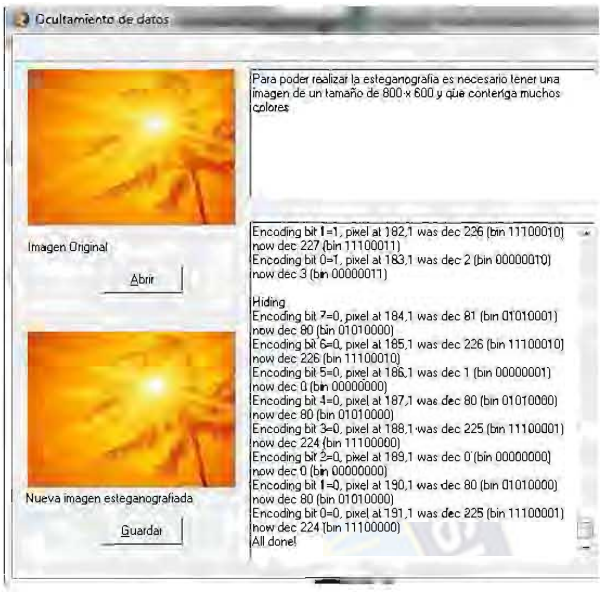
3.11.2.2 Prueba 2

Fuente: [Elaboración propia]

Como también se puede observar en la nueva imagen al restaurar no muestra un mensaje solo contiene información que no sirve.

Aplicando el software se tiene, para el proceso de ocultación de datos en dicha imagen, y que no contenga mensajes que no son entendibles se procede a esconder una información que sea entendible:

3.11.2.3 Prueba 2



Fuente: [Elaboración propia]

3.12 INTERPRETACIÓN DE LAS PRUEBAS

Los resultados obtenidos en los ejemplos realizados en formatos BMP muestran que:

- El grado de ocultación es aceptable con la técnica del bit menos significativo, pues la visualización de las imágenes no son alteradas ni el tamaño de las mismas.

- La velocidad de ocultación con la técnica es menor o igual a un segundo, para todas las imágenes y para cualquier grado de ocultación de datos.

- Aplicando la técnica del bit menos significativo se logran obtener resultados aceptables en comparación con el tamaño de la imagen original, llegando a ocultar texto más extenso.

- Los bit no son alterados en su mayoría como se ve en los ejemplos no existe ningún cambio en los colores de las imágenes puestas a prueba tampoco son alterados las resoluciones.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES GENERALES

Realizar el ocultamiento de datos en imágenes digitales utilizando el método del bit menos significativo, proporciona una técnica para llevar a cabo el proceso de ocultamiento de datos, logrando ocultar datos en imágenes sin alterar su tamaño, los colores de las imágenes y claro manteniendo la visualización.

Al realizar la comparación con los ejemplos realizados en distintos gráficos, se ha podido evaluar y analizar el comportamiento de la técnica desarrollada, llegando a evidenciar que se puede alcanzar a dicha técnica en sus grados de mayor cantidad de datos a ocultar.

El análisis de los resultados obtenidos, con las pruebas realizadas en el software muestra que la ocultación de datos en las imágenes utilizando el método del bit menos significativo, es eficiente en cuanto al tamaño de la nueva imagen esteganografiada y la

calidad de visualización de la imagen reconstruida.

Realizar la compresión de imágenes utilizando el software desarrollado, trae las ventajas de que se puede llegar a niveles de ocultar datos de casi 50 hojas o mas de Word pero lleva un tiempo estimado de 1 a 2 minutos de acuerdo al texto que se quiere ocultar.

4.2 CUMPLIMIENTO DE LOS OBJETIVOS

El objetivo general "desarrollar una técnica de ocultación de datos que permita obtener a partir de una imagen digital un versión esteganografiada de la misma, aplicando el método del bit menos significativo ", planteado en el capitulo uno, se cumplió con la técnica de ocultación de los datos en imágenes y con la implementación de la técnica en un software, descritos en el capitulo tres.

En cuanto a los objetivos específicos planteados a continuación se describe el grado de cumplimiento de cada uno.

- Implementar el método del bit menos significativo en imágenes digitales.
- Desarrollar un software en el cual se puedan mostrar los resultados obtenidos al implementar la técnica esteganográfica desarrollada.
- Realizar la comparación de los resultados obtenidos con la técnica desarrollada.
- Medir la calidad de las imágenes esteganografiadas y las originales.
- Demostrar el grado de confianza del bit menos significativo en el campo de la esteganografía.
- Se cumple el diseño del bit menos significativo en el capitulo tres con los algoritmos de entrenamiento para el bit.
- Se cumple en el desarrollo del software en base a la técnica de ocultación planteada, que se describe en el capitulo tres, el cual se utilizo para obtener los resultados de los

casos de pruebas presentados.

- Se cumple con la comparación de los resultados obtenidos por la técnica de ocultación de datos utilizando el bit menos significativo, llegando a evidenciar que se puede alcanzar a ocultar datos de una magnitud comprensiva.

- Se puede medir la calidad de las imágenes esteganografiadas a simple vista como para cualquier usuario que la imagen no ha sufrido ninguna transformación alguna, sin pérdida de colores, tamaño.

- Se cumple, con los resultados de ocultación para las imágenes puestas a pruebas, logrando esconder datos de uno a varios párrafos.

4.3 ESTADO DE LA HIPÓTESIS

La hipótesis del trabajo de investigación solicita lo siguiente:

La técnica de ocultación de datos se puede utilizar en archivos de imágenes, manipulando su representación binaria.

Para demostrar la hipótesis, recurrimos a los resultados obtenidos mediante el software de ocultación de datos, donde se observo que las imágenes esteganografiadas son iguales a las imágenes originales utilizando el método del bit menos significativo, manteniendo la calidad de visualización.

Con ello se demuestra que se puede ocultar datos en imágenes digitales, mediante el uso del bit menos significativo, manteniendo la calidad de visualización en la imagen reconstruida.

4.4 RECOMENDACIONES

Con el desarrollo de la esteganografía se genera también el crecimiento del estegoanálisis como la ciencia que se encarga de detectar, identificar y analizar archivos que contiene información oculta con el fin de develar y tener acceso a los mensajes camuflados.

El éxito de la esteganografía se basa en la selección deliberada del medio en el que se desea camuflar la información, existiendo tantos mecanismos para llevar a cabo el camuflaje de información como la imaginación lo permita.

La esteganografía se ha posicionado en los últimos años en el campo de la seguridad, pero de ninguna forma reemplaza a la criptografía, ambas pueden complementarse para lograr buenos resultados en el ocultamiento de información.

La esteganografía ha tomado más fuerza en el campo militar, sin embargo, en poco tiempo podremos aplicar las técnicas en nuestros computadores personales ocultando información en creaciones artísticas de audio y/ o video.

Es interesante aventurarse con ingenio y creatividad a la producción de prototipos experimentales, tanto para camuflar información como para develarla.

4.5 TRABAJOS FUTUROS

Implementar otras técnicas de entrenamiento para la ocultación de datos con otros métodos del tipo estadístico, para observar el rendimiento frente a las técnicas de ocultación propuestas.

Crear un software que permita la distribución del formato .JPEG.

Generalizar la técnica de ocultación para imágenes con colores blanco y negro.

BIBLIOGRAFÍA

[ANDERSON, 1998] Autor: Gabriel Anderson, 1998
"PRINCIPIOS DE PROCESAMIENTO DIGITAL DE IMÁGENES"
http://www.profc.udec.cl/~gabriel/tutoriales/curso/cap06-%20imagenes%20digitales.PDF
Año: 1998

[ARTZ, 2001] ARTZ Donovan. Digital Steganography: Hiding Data within Data [online]. (Sin editorial y demás datos). Páginas 77 en adelante. Junio 2001. Los Alamos National Laboratory. Spotlight. Disponible en:
http://www.cc.gatech.edu/classes/AY2003/cs6262_fall/digital_steganography.pdf

[CRAIG, 1996] [ROWLAND, 1996]CRAIG H., M. Rowland. Covert Channels in the TCP/IP Protocol Suite [online]. 1996. (Sin editorial y demás datos).Disponible En:
http://translate.google.com/translate?hl=es&sl=en&u=http://www.firstmonday.org/issues/issue2_5/rowland/&pre v=/search%3Fq%3Dcovert%2Bchannel%2B%26hl%3De s%26lr%3D

[FRIDRICH Y DU, 2000] FRIDRICH Julio, CARATTI Mariana, DU CABO Roberto, GIUSTO Mariel, ISAR Guido, PAGOUAPÉ Matías, SCHELLHASE Livio, STAVRINAKIS Florencia. Esteganografía [online]. (Sin editorial y demás datos). Universidad Jhon F. Kennedy, año 1998, Buenos Aires, Argentina Disponible en:
http://www.cybsec.com/Stegano.pdf

[HOSMER Y HIDE, 2003] Hosmer A, Hide L. Exploring Steganography: Seeing the Unseen [online]. Páginas 26 a 30. Año 2003. (Sin editorial y demás datos). Universidad de George Mason 2026.pdf. Disponible en:
http://www.jjtc.com/pub/ r2026.pdf

[JOHNSON, 2001] Johnson Juan F., OSPINA Carlos, RANGEL Mauricio, ROJAS Jaime A., VERGARA Camilo. Covert Channels Sobre http. Páginas 1 a 3 [online]. Febrero de 2001. (Sin editorial y demás datos). Universidad de los Andes. Disponible en:
http://www.criptored.upm.es/ guiateoria/gt_m142m.htm

[KAHN, 1996] Autor: Kahn M. Modern Steganography [online]. Página 3. Abril 1996 (Sin

editorial y demás datos). Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague. Disponible en: http://www.scycore.com/papers/ow04_paper.pdf

[KENNEY, RIEGER, 2003] Autor: KENNEY P., RIEGER F. 2003
Practical Privacy Guide: Steganography [online]. (Sin editorial y demás datos). All Net Tools - Library - Privacy Guide. Html. Disponible en: http://www.all- nettools.com/library,privacy3

[KENNEY, 2003] Autor: Anne R. Kenney
"TUTORIAL DE DIGITALIZACIÓN DE IMÁGENES"
http://www.rlg.org /preserv/mtip2000.htm
Año: 2003

[MARARON, 2001] ÁLVAREZ MARAÑÓN Gonzalo. Canales subliminales [online]. (Sin editorial y demás datos). Abril de 2001. Disponible en;
http://www. cibernauta.com/cibertecno/cibertecno_analisis_articulos, php?articulo=1329.php

[MORENO, 2003] Autor: Luciano Moreno
"TEORIA DEL COLOR" http://www.htmlweb.net/ Aflo: 2003

[ROQUE, 2002] Autor: Germán Roque Arias
"IMAGENES DE PIXELES (BITMAPS) E IMAGENES DE VECTORES "
http://www.canalaudiovisual.com/ezine/books/jirimag/1IMAG.htm
Año: 2002

[SEWARD, 2004] Seward J., Copyright © 1997-2005, S.L. All rights reserved [online]. Esta página fue Revisada/modificada: 22 de enero de 2004. (Sin editorial y demás datos). Disponible en: http://www.opticdata.es/ docs.htm

[WAYNER, 2002] T. Wayner, Esteganografía… No es lo que parece [online]. Febrero de 2003. Página 9 en adelante.(Sin editorial y demás datos).Disponible en:
http://webs.ono.com/usr011/r-tolosa/archivos/steg.pdf

ANEXO A

GLOSARIO

Endian

Big endian es un formato para el almacenamiento y la transmisión de datos binarios en el que el bit (o el byte) más significativo obtiene la dirección más baja. La norma contraria, denominada little endian, coloca en la dirección más baja el bit menos significativo.

Encryption [cifrado]

Encriptacion. Es el tratamiento de los datos contenidos en un paquete a fin de impedir que nadie excepto el destinatario de los mismos, pueda leerlo. (por supuesto, este debe conocer la clave de desencriptado). Existen muchísimos tipos de cifrado.

Embedded

Encajado, integrado, embutido dentro de algo.

Pixel

Combinación de "picture" y "element". Elemento gráfico mínimo con el que se componen las imágenes en la pantalla de una computadora.

Órdenes

Las instrucciones empotraron en una base de datos o un programa de computadora que da como resultado una operación siendo realizado. Por ejemplo, las opciones para "interlineación", "la búsqueda" y "la impresión" son comandos de computadora.

Las publicaciones electrónicas (diarios electrónicos)

Las publicaciones publicadas en formato electrónico, a menudo disponible en la Internet.

Publicación

Una publicación resultó en partes sucesivas, intentó ser continuada indefinidamente. Típicamente, una publicación contiene una colección de artículos por autores diferentes, a menudo en un área sujeto particular. Las publicaciones están también conocidas como Publicaciones y Novelas por Entregas.

Ocultar texto

Un elemento de datos tiene 8 bits (1 byte) en un archivo de 8 bits y 16 bits (2 bytes) en un archivo de 16 bits. Steganos, por ejemplo, utiliza los bits menos significativos de un archivo de ondas de 8 bits para ocultar los datos y no oculta los datos en las cabeceras de los archivos. El oído humano no puede distinguir estas ligeras modificaciones debido al ruido de fondo. Por tanto, los datos se ocultan realmente. En archivos de gráficos, los colores de los píxeles se modifican ligeramente, pero no lo suficiente como para afectar al que los está viendo. [Carranza, 2005]

Datos privados

Se filtran en la red datos privados de personas, con datos que van desde los números de teléfonos, direcciones, nombres y apellidos, etc. Estos datos rápidamente fueron notados por las administraciones de sitios y removidos lo antes posible, no sin que antes alcanzaran a verlos fácilmente cientos de usuarios.

Donde estos datos son difundidos a varios servidores e inclusive a crear torrents para que quien quisiera bajar la información pudiese hacerlo.

Peor aún, si sus datos son publicados por una empresa o particular que tiene sus servidores en el extranjero, la denuncia deberá hacerla en el país en que éstos están instalados, ya que rige la territorialidad del delito.

Estos datos privados se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada. Por ejemplo: raza, opiniones políticas, las creencias religiosas.[Villagrán, 2002]

Archivos

Los archivos también denominados ficheros (file); es una colección de información (datos relacionados entre sí), localizada o almacenada como una unidad en alguna parte de la computadora. Los archivos son el conjunto organizado de informaciones del mismo tipo, que pueden utilizarse en un mismo tratamiento; como soporte material de estas informaciones.

Los archivos como colección de datos sirven para la entrada y salida a la computadora y son manejados con programas.

Los archivos pueden ser contrastados con Arrays y registros; Lo que resulta dinámico y por esto en un registro se deben especificar los campos, él número de elementos de un

arrays (o arreglo), el número de caracteres en una cadena; por esto se denotan como "Estructuras Estáticas".

En los archivos no se requiere de un tamaño predeterminado; esto significa que se pueden hacer archivos de datos más grandes o pequeños, según se necesiten.

Cada archivo es referenciado por su identificador (su nombre.).]

Imagen

Una imagen (del latín imago) es una representación visual de un objeto mediante técnicas diferentes de diseño, pintura, fotografía, video, etc.

En informática puede tener dos significados:

Una imagen puede ser un archivo codificado que, al abrirlo, muestra una representación visual de algo (ya sea fotografía, gráfica, dibujo, etc.) [Plata, 2007]

Esteganografía

La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido.

Si bien la Esteganografía suele confundirse con la criptografía, por ser ambas parte de los procesos de protección de la información, son disciplinas bastante distintas, tanto en su forma de implementar como en su objetivo mismo.

Mientras que la criptografía es utilizada para cifrar o codificar información de manera que ella sea inintelegible para un probable intruso, a pesar del conocimiento de su existencia, la Esteganografía oculta la información en un portador de manera que no sea advertido el hecho mismo de su existencia y envío. De esta última manera un probable intruso ni siquiera sabrá que se está transmitiendo información sensible.

Sin embargo, la criptografía y la esteganografía pueden complementarse, dando un nivel de seguridad extra a la información, es decir, es muy común (aunque no imprescindible) que el mensaje a esteganografiar sea previamente cifrado; de tal modo que a un eventual intruso no sólo le costará advertir la presencia misma de la mensajería oculta, sino que si la llegara a obtener, la encontraría cifrada.

EL origen de esta palabra deriva de la composición de los vocablos griegos *steganos*, que significa cubierto u oculto, y *graphos*, que significa escritura.[1] La palabra

esteganografía, como muchas otras que ya están aceptadas y en utilización, aún no figura en el diccionario de la Real Academia.

La Esteganografía en el moderno sentido de la palabra, y en términos informáticos, se refiere a la información o a un archivo cualesquiera que se encuentra oculto dentro de otro, normalmente multimedial, es decir el portador es una imagen digital, un vídeo o archivo de audio.[Agreda, 2006]

Método

Podemos establecer dos grandes clases de métodos de investigación: los métodos lógicos y los empíricos. Los primeros son todos aquellos que se basan en la utilización del pensamiento en sus funciones de deducción, análisis y síntesis, mientras que los métodos empíricos, se aproximan al conocimiento del objeto mediante sus conocimiento directo y el uso de la experiencia, entre ellos encontramos la observación y la experimentación.

"Es una especie de brújula en la que no se produce automáticamente el saber, pero que evita perdernos en el caos aparente de los fenómenos, aunque solo sea porque nos indica como no plantear los problemas y como no sucumbir en el embrujo de nuestros prejuicios predilectos."

El método independiente del objeto al que se aplique, tiene como objetivo solucionar problemas.[Wikipedia, 2008]

Imagen de salida

Imagen original que fue modificado para obtener una imagen de salida parecida a la imagen original.[wikipedia, 2008]

Combinando las técnicas

Fusionando las distintas técnicas de esteganografía para tener una imagen esteganografiada ocultando información privada. [Brassard, 1997]

Método del bit

A causa de este problema nace el método del bit menos significativo, propuesto por Derek Upham's(Provos and Honeyman, 2003), el cual consiste en tomar los bits menos significativos de los píxeles de la imagen, y en estos bits ocultar los datos necesarios, por supuesto esta técnica nos permitirá ocultar menos cantidad de información pero la hará casi imperceptible al ojo humano.

Por ejemplo si deseáramos almacenar la letra a (código ASCII 97) tenemos: 97 en binario=01100001. Para el caso de una imagen si deseamos almacenar un byte (8 bits) necesitamos tres píxeles (debido a que cada píxel almacena 3 bytes de datos, y nosotros almacenamos un bit por cada byte de la imagen).

El método del bit menos significativo tomado en cuenta escoge los pixeles a modificar de una manera secuencial, aglomerando los cambios realizados en la imagen en su parte inicial.[Murrugarra, 2007]

Procesar imágenes

El procesamiento digital de imágenes es el conjunto de técnicas que se aplican a las imágenes digitales con el objetivo de mejorar la calidad o facilitar la búsqueda de información.

Las operaciones que se pueden realizar con imágenes se dividen en :

- Operaciones de punto
- Operaciones de entorno
- Operaciones con dos o más imágenes [Agreda, 2006]

Contenidos de texto

Conjunto de letras que forman una palabra o frase par ser oculta en una imagen. [Wikipedia, 2008]

Reducir el tiempo

Uno de los detalles que el usuario al usar un software determinado lo hace para reducir el tiempo, aquellos programadores que no les gusta un interfaz gráfico suelen usar comandos DOS para esteganografiar textos en imágenes, y un usuario sin conocimiento en comandos DOS tardaría muchísimo para esteganografiar.[Román, 1999].

ANEXO B

FUTURAS INVESTIGACIONES

Métodos de encriptación

Para realizar un mejoramiento al so del bit menos significativo se puede implementar parte de criptografía para que el software sea más eficiente.

El método de encriptación y desencriptación se denomina código. Hay algunos algoritmos modernos que utilizan claves para controlar la encriptación y la desencriptación.

Algoritmos que utilizan claves para la encriptación.

Algoritmos simétricos.

Estos algoritmos son también llamados **Algoritmos de clave secreta** y se caracterizan por la utilización de la misma clave para la encriptación y para la desencriptación, o bien la clave para la desencriptación es derivada fácilmente de la clave de encriptación.

Generalmente son de ejecución más rápida que los asimétricos. En la práctica se utilizan conjuntamente ambos; los algoritmos de clave pública se utilizan para encriptar una clave de encriptación generada aleatoriamente y la clave aleatoria es utilizada para encriptar el mensaje utilizando para ello un algoritmo simétrico.

Tipos de algoritmos simétricos.

DES. Es un estándar utilizado por el gobierno de los Estados Unidos y otros

Gobiernos del mundo entero. Se utiliza especialmente en la industria financiera.

Es un bloque de código con un tamaño de 64 bits, que utiliza claves de 56 bits.

Esta construcción puede ser comunicada mediante computadoras modernas o hardware especial.

DES es lo suficientemente poderoso como para preservarse de hackers, pero puede ser interrumpido con hardware especial del gobierno, organizaciones criminales o corporaciones mayores.

Una variante de DES es Triple-DES ó 3DES, se basa en la utilización de DES tres veces: normalmente en una secuencia de encriptación-desencriptación encriptación, con tres claves sin conexión.

Algunas implementaciones de DES pueden ser halladas en libdes, alodes, SSLeay, etc.

Blowfish. Es un algoritmo desarrollado por Bruce Schenier. Consta de un bloque de código con un tamaño de 64 bits y claves de longitud variable, superiores a los 448 bits. Es utilizado en una gran cantidad de paquetes de software incluyendo zautilus y PGPfone.

IDEA (International Data Encryptacion Algorithm). Es un algoritmo desarrollado en ETH Zurich, en Suiza. Utiliza una clave de 128 bits, es considerado un algoritmo seguro y es uno de los mejores de conocimiento público. Está patentado en Estados Unidos y varios países de Europa.

En la actualidad hay varias implementaciones de IDEA disponibles: SSLeay, PGP código fuente y Ssh código fuente, idea86, etc.

RC4. Es un código diseñado por RSA Data Security Lt. Era utilizado para el comercio secreto, hasta que alguien diseñó un código para un algoritmo en Usenet News, declarando que sería equivalente a RC4.

El algoritmo es muy veloz, y es utilizado en determinadas aplicaciones, debe tenerse en cuenta que no puede utilizarse la misma clave para encriptar dos datos distintos.

SAFER. Es un algoritmo desarrollado por J. L. Massey, quién fue también uno de los desarrolladores de IDEA. Este algoritmo permite una encriptación segura con una implementación rápida de software hasta en procesadores de 8 bits.

Hay dos implementaciones disponibles, una de ellas, de claves de 64 bits, y la otra de claves de 128 bits.

Enigma. Fue el código utilizado por los alemanes en la segunda guerra mundial.

Vigenere Es comúnmente mencionado en varios libros, los programas para este código están disponibles gratuitamente.

Algoritmos asimétricos.

Son también llamados **códigos asimétricos,** utilizan claves diferentes para la encriptación y desencriptación, no permitiendo además, derivar la clave para la desencriptación de la clave utilizada para la encriptación,

Son también llamados **Algoritmos de clave pública**, ya que permiten encriptar claves públicas.

La clave de encriptación se denomina **clave pública** y la clave de desencriptación; **clave privada** o **secreta**.

Los algoritmos de encriptación modernos son ejecutados por computadoras o hardware especial.

Hay disponible gran cantidad de paquetes de software.

Tipos de algoritmos asimétricos.

RSA (Rivest-Shamir-Adelman). Es el algoritmo de clase pública que se utiliza con mayor frecuencia, y es considerado el más importante dentro de los algoritmos de clave pública.

Puede ser utilizado para la encriptación y desencriptación. Se considera un algoritmo seguro ya que utiliza claves largas, la seguridad se basa en la dificultad para factorear enteros largos.

Entre las implementaciones disponibles se encuentran: RSAREF, RSAEURO, SSLeay, PGP código fuente, Ssh código fuente, etc.

Diffie-Hellman. El un algoritmos de clave pública utilizado generalmente para realizar intercambios de claves. Es considerado seguro ya que utiliza claves largas y generadores propios.

Dentro de las implementaciones disponibles se pueden hallar: RSAREF, RSAURO, SSLeay, alodes, etc.

Criptosistemas de clave pública de curva elíptica. Es una especialidad que está surgiendo en la actualidad. Son de ejecución lenta, pero pueden ser ejecutados por computadoras modernas. Son considerados suficientemente seguros, pero no fueron examinados de las mismas maneras que por ejemplo el algoritmo RSA.

Una de las implementaciones disponible es el paquete elíptico.

DSS (Digital Signature Standar). Es un mecanismo que utiliza una sola firma aprobado por el gobierno de los Estados Unidos. Esta aprobación no fue hecha

pública y mucha gente puede encontrar problemas potenciales con este algoritmo, como por ejemplo: datos escondidos en la firma pueden ser perdidos y revelar la clave secreta si se pasa a un signo dos mensajes diferentes utilizando el mismo número aleatorio.

LUC. Es un sistema de encriptación de clave pública. Utiliza funciones Lucas en vez de exponenciación, Su inventor fue Peter Smith, quién implementó además, junto con la función Lucas, otros cuatro algoritmos: LUCDIF, es un método de negociación de claves como el Diffie-Hellman; LUCELG PK; LUCELG DS Y LUCDSA, que equivale al US Digital Signature Standar.

Modo de bloque de código.

Muchos de los códigos comúnmente utilizados (IDEA, DES, Blowfish), son bloques de código. Esto significa que toman un bloque de datos de tamaño fijo, generalmente 64 bits, y lo transforman en otro bloque de 64 bits utilizando una función seleccionada por la clave. El código básicamente define un uno-a-uno proyectando desde enteros de 64 bits hacia otra permutación de enteros de 64 bits.

Si el mismo bloque es encriptado dos veces con la misma clave, los bloques de texto codificados resultante son los mismos. Este método de encriptación es llamado Electronic Code Book o ECB.

En aplicaciones prácticas, permite construir bloques idénticos de texto puro encriptado para diferentes bloques de texto codificado.

Hay dos métodos utilizados para esto:

Modo CFB. Un bloque de texto codificado es obtenido encriptado el bloque de texto codificado previo y haciendo un XOR con el valor resultante con el texto puro.

Modo CBC. Un bloque de texto codificado es obtenido primero haciendo un

XOR con el bloque de texto puro y encriptado el valor resultante.

El bloque de texto codificado previo es generalmente almacenado en un Vector de Inicialización (IV). El vector inicializado en 0 es utilizado comúnmente por el primer bloque, aunque otros vectores estén también en uso.

Funciones criptográficas hash.

Las funciones hash criptográficas son utilizadas para computar el mensaje cuando se está construyendo una firma digital. Una función hash comprime los bits del mensaje a un valor hash de tamaño fijado, de manera que distribuye los posibles mensajes uniformemente entre los posibles valores hash.

Las funciones criptográficas hash generalmente producen valores hash de 128 o más bits.

Tipos de funciones criptográficas hash.

MD5. Message Digest Algorithm 5, es un algoritmo hash considerado bastante seguro, fue desarrollado en RSA Data Security, Inc. Pueden ser utilizadas cadenas de bytes de longitudes arbitrarias dentro de valores de 128 bits.

MD2, MD4. También fueron creados por RSA Data Security, poseen imperfecciones y no son recomendados.

SHA. Secure Hash Algorithm y también SHS: Secure Hash Standard, son algoritmos criptográficos hash publicados por el gobierno de los Estados Unidos.

Producen un valor hash de 160 bits a partir de una cadena de longitud arbitraria.

Es un algoritmo nuevo, considerado eficiente.

Tiger. Es un algoritmo nuevo desarrollado por Anderson y Biham.

RIPEMD-160. Es un algoritmo hash designado para reemplazar al MD4 y al MD5.

Firmas digitales.

Algunos algoritmos de clave pública pueden ser utilizados para generar firmas digitales.

Una firma digital es un bloque de datos que fue creado utilizando alguna clave secreta y además se utiliza una clave pública para verificar que la firma haya sido generada usando la clave privada correspondiente. El algoritmo utilizado para generar la firma hace que sin conocer la clave secreta sea imposible crear una firma que sea válida.

Las firmas digitales son utilizadas para verificar que un mensaje realmente venga desde el sendero declarado. También pueden utilizarse para certificar que una clave pública pertenece a una determinada persona.

Para verificar una firma, el receptor primero determina si la clave pertenece a la persona que debe pertenecer y luego desencripta la firma utilizando la clave pública de la persona. Si la desencriptación de la firma es correcta y la información es igual al mensaje, la firma es aceptada como válida.

El algoritmo más utilizado es el RSA.