

Análisis Comparativo Entre las Diversas Técnicas
Esteganográficas en Imágenes de Mapa de Bits

Elkin José Garrido Mendoza
Jaime Alfonso Garrido Mendoza

Fundación Universitaria San Martín
Facultad de Ingeniería
Programa de Ingeniería de Sistemas
Barranquilla
2005

**ANALISIS COMPARATIVO ENTRE LAS DIVERSAS TECNICAS
ESTEGANOGRAFICAS EN IMÁGENES DE MAPA DE BITS**

ELKIN JOSE GARRIDO MENDOZA.

Presidente del Jurado

JAIME ALFONSO GARRIDO MENDOZA.

Firma del Jurado

PROYECTO DE GRADO

Firma del Jurado

Director.

**Douglas Hurtado Carmona.
Ingeniero de Sistemas.**

**FUNDACIÓN UNIVERSITARIA SAN MARTIN
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BARRANQUILLA**

2005

Barranquilla, 15 Julio del 2005

RESUMEN

Este trabajo presenta un análisis comparativo entre las más importantes técnicas que ocultan información en imágenes de mapa de BITS, este proceso se llama Esteganografía.

CONTENIDO

1. INTRODUCCIÓN	14
2. ANTECEDENTES DEL PROYECTO	17
2.1. DESCRIPCIÓN DEL PROBLEMA	17
2.2. FORMULACIÓN	19
3. JUSTIFICACIÓN	19
4. OBJETIVOS	20
4.1. Objetivo general	20
4.2. Objetivos específicos	21
5. MARCO REFERENCIAL	21
5.1. Marco teórico	21
5.2. Marco conceptual	22
6. METODOLOGÍA	25
6.1. Tipo de investigación	25
6.2. Método de investigación	26
6.3. Técnicas para la recolección de la información	26
7. ASPECTOS ADMINISTRATIVOS Y DE CONTROL	27
7.1. Plan de actividades	27
7.2. Cronograma de actividades	28
7.3. Recursos físicos, humanos y costos	28
7.3.1. Recursos físicos y disgregación de precios	28

0.7.4. Recursos humanos	28
CONTENIDO	
1. ACTORES, APLICACIONES Y DEFINICIONES DE TÉCNICAS ESTEGANOGRÁFICAS	30
1.1. ACTORES INVOLUCRADOS	30
1.2. OTRAS APLICACIONES DE LA ESTEGANOGRAFÍA	pág.
INTRODUCCIÓN	14
0. ANTECEDENTES DEL PROYECTO	17
0.1. IDENTIFICACION DEL PROBLEMA	17
0.1.1. Área de conocimiento	17
0.1.2. Área temática	17
0.1.3. Tema	17
0.1.4. Título	17
0.2. PLANTEAMIENTO DEL PROBLEMA	17
0.2.1. Descripción	17
0.2.2. Formulación	19
0.3. JUSTIFICACIÓN	19
0.4. OBJETIVOS	20
0.4.1. Objetivo general	20
0.4.2. Objetivos específicos	21
0.5. MARCO REFERENCIAL	21
0.5.1. Marco teórico	21
0.5.2. Marco conceptual	22
0.6. METODOLOGÍA	25
0.6.1. Tipo de investigación	25
0.6.2. Método de investigación	26
0.6.3. Técnicas para la recolección de la información	26
0.7. ASPECTOS ADMINISTRATIVOS Y DE CONTROL	27
0.7.1. Plan de actividades	27
0.7.2. Cronograma de actividades	28
0.7.3. Recursos físicos, humanos y costos	28
0.7.3.1. Recursos físicos y disgregación de precios	28

0.7.4. Recursos humanos	28
1. ACTORES, APLICACIONES Y DEFINICIONES DE TÉCNICAS	49
1.1. ESTEGANOGRÁFICAS	30
1.1.1. ACTORES INVOLUCRADOS	30
1.2. OTRAS APLICACIONES DE LA ESTEGANOGRAFIA	32
1.3. CLASIFICACION Y PROPIEDADES BÁSICAS DE LAS MARCAS DE	36
1.3.1. AGUA	33
1.3.1.1. Visibles vs. Invisibles	34
1.3.1.2. Marcas invisibles	34
1.3.1.3. Marcas visibles	34
1.3.1.4. Frágiles vs. Robustas	35
1.3.1.4.1. Marcas frágiles	35
1.3.1.4.2. Marcas robustas	36
1.4. DOMINIO ESPACIA VS. DOMINIO ESPECTRAL	37
1.4.1. Técnicas del dominio espacial	37
1.4.2. Técnicas del dominio espectral	38
1.4.3. Otras clasificaciones	39
1.5. ESQUEMA GENERAL DEL PROCESO DE MARCADO PARA IMÁGENES	39
1.5.1. Generación de la marca de agua	40
1.5.2. Inserción de la marca de agua	41
1.5.3. Detección de la marca de agua	42
1.6. ALGORITMOS DE MARCADO	44
1.6.1. Técnicas de marcado en el dominio espacial	44
1.6.1.1. Técnica del BIT Menos Significativo (LSB)	45
1.6.1.2. Técnica CW2D	46
1.6.1.3. Patchwork Method	48
1.6.1.4. Texture Block Coding	48

1.6.1.5	Checksum	49
1.6.2.	Técnicas de marcado en el dominio espectral	49
1.6.2.1.	SysCoP	50
1.6.2.2.	Spread Spectrum Watermarking	53
2.	DESCRIBIR EL PROCESO DE LA ESTEGANOGRAFIA EN ARCHIVOS DE MAPA DE BIST BMP	56
2.1.	POR QUE EN BMP'S	56
2.2.	ESTRUCTURA DE UN BMP Ó ARCHIVO DE MAPA DE BITS	56
2.3.	Manipulación de archivos BMP	59
3.	COMPARAR LAS TÉCNICAS ESTEGANOGRÁFICAS PARA ASÍ DAR A CONOCER CADA UNA LAS VENTAJAS Y DESVENTAJAS SEGÚN SUS TIPOS	61
3.1.	COMPLEJIDAD ALGORITMICA TEMPORAL	65
3.2.	COMPLEJIDAD DE DESARROLLO ALGORITMICO	67
3.3.	CONSERVACION DELA CALIDAD	68
3.4.	SEGURIDAD DE ROMPIMIENTO	70
3.5.	VENTAJAS Y DESVENTAJAS	71
4.	SOCIALIZAR EL ORIGEN CONCEPTUAL Y TECNOLÓGICO, ASÍ COMO LA IMPORTANCIA DE LA ESTEGANOGRAFÍA EN LA ERA POST-INDUSTRIAL	73
4.1.	QUE USOS TIENE LA ESTEGANOGRAFÍA EN LA ACTUALIDAD?	74
4.1.2.	Algunos usos del Procesamiento de Imágenes	74
4.2.	LA ESTEGANOGRAFÍA EN LA MEDICINA	76
	CONCLUSIONES	79
	RECOMENDACIONES	80
	BIBLIOGRAFIA	81
	ANEXOS	84

LISTA DE TABLAS

	pág.
Tabla1 de ventajas y desventajas de espaciales vs. Espectrales	71
Figura 1. Esquema de Aplicación de una Marca de Agua Espacial	74
Figura 2. Esquema del proceso de generación e inserción de una marca de agua	75
Figura 3. Esquema del proceso de extracción de una marca de agua	76
Figura 4. Esquema del proceso de detección de una marca de agua	77
Figura 5. Procedimiento total del watermarking	78
Figura 6. Procedimiento de la autenticación para las imágenes marcadas por el agua.	48
Figura 7. Coeficientes de un bloque de 8x8	50
Figura 8. Exploración en Zig Zag	52
Figura 9. Marca de agua X de 1000 elementos generada con distribución $N(0,1)$	54
Figura 10. Proceso de inserción de la marca	55
Figura 11. Imagen original	68
Figura 12. Imagen con una marca de agua	69
Figura 13. Imagen original	70
Figura 14. Imagen reconstruida	70
Figura 15. Imagen de error	70

LISTA DE FIGURAS

	pág.
Figura 1. Esquema de Aplicación de una Marca de Agua Frágil	36
Figura 2. Esquema del proceso de generación e inserción de una marca de agua	41
Figura 3. Esquema del proceso de extracción de una marca de agua	43
Figura 4. Esquema del proceso de detección de una marca de agua	43
Figura 5. Procedimiento total del watermarking	46
Figura 6. Procedimiento de la autenticación para las imágenes marcadas por el agua.	48
Figura 7. Coeficientes de un bloque de 8x8	50
Figura 8. Exploración en Zic Zac	52
Figura 9. Marca de agua X de 1000 elementos generada con distribución $N(0,1)$	54
Figura 10. Proceso de inserción de la marca	55
Figura 11. Imagen original	68
Figura 12. Imagen con una marca de agua	69
Figura 13. Imagen original	70
Figura 14. Imagen reconstruida	70
Figura 15. Imagen de error	70

INTRODUCCION

LISTA DE ANEXOS

Hoy en día debido al gran auge y desarrollo que ha tenido la informática, muchas personas e instituciones se han visto obligadas a manejar la información de sus actividades electrónicas.	pág.
ANEXO A - Algoritmo de Esteganografía para ocultar a información en imagen usando la técnica LSB Pascal	83
ANEXO B - Algoritmo de Esteganografía para extraer la información en imagen usando la técnica LSB. Pascal	85
ANEXO C - Código fuente del programa que realiza Esteganografía en BMP	88
ANEXO D - Formato WAVE (RIFF)	94

La información digital reside en dispositivos diseñados especialmente para reconocer los diferentes patrones de almacenamiento en que se guardan los datos, tal es el caso de los computadores que pueden llegar a albergar millones de archivos en sus discos duros o unidades de almacenamiento.

Se dice que el activo más valioso para una compañía es la información, y si ésta se almacena en medios digitales debe someterse a reglas que permitan su uso adecuado. Dada la cantidad de personal que puede manipular dispositivos electrónicos y que tienen acceso a la información en una empresa, es preciso de alguna manera preservar la integridad de los datos.

INTRODUCCION

Hoy en día debido al gran auge y desarrollo que ha tenido la informática, muchas personas e instituciones se han visto obligadas a manejar la información de sus negocios y/o actividades personales bajo medios digitales y electrónicos.

En muchas ocasiones, estos tipos de información digital representan datos de vital importancia para el funcionamiento de una organización, también describen actividades y procesos de interés para pequeños grupos específicos o simplemente contienen estadísticas de carácter estratégico que sirven de apoyo a decisiones gerenciales.

La información digital reside en dispositivos diseñados especialmente para reconocer los diferentes patrones de almacenamiento en que se guardan los datos, tal es el caso de los computadores que pueden llegar a albergar millones de archivos en sus discos duros o unidades de almacenamiento.

Se dice que el activo más valioso para una compañía es la información, y si ésta se almacena en medios digitales debe someterse a reglas que permitan su uso adecuado. Dada la cantidad de personal que puede manipular dispositivos electrónicos y que tienen acceso a la información en una empresa, es preciso de alguna manera preservar la integridad de los datos.

Con la creciente demanda de medios de comunicación digitales de carácter masivo, como el caso de Internet, es conveniente tomar medidas de control que aseguren que nuestra información no será alterada y que siempre se conservará tal y como fue creada.

Los medios digitales son los más utilizados para transmitir información, cualquier persona podría duplicar material digital de solo contar con los medios adecuados en un computador o cualquier otro dispositivo. Las copias son exactamente iguales que las originales, pues los medios electrónicos representan la información en unidades de almacenamiento llamadas bits¹ que al ser duplicados permanecen igual que su representación original.

Las copias sin autorización que se hacen de material digital, ya sean archivos de texto, audio, imágenes, etc., son violaciones a las normas y leyes de derechos de autor. Esta difusión de la información va en contra de la distribución de la propiedad intelectual sin consentimiento del creador de la información y por lo tanto se considera un delito en la mayoría de los países.

Ante este problema de “piratear” la información, la tecnología informática nos ofrece mecanismos de protección que garanticen los derechos de autor para los creadores de los contenidos. Aunque realmente es imposible evitar todos los tipos de fraude que se puedan hacer sobre un medio digital, al menos se puede proteger el material de algunos de los peores ataques que se le puedan hacer.

¹Bit: Binary Digit. Dígito Binario.

Una de las técnicas de protección se basa en insertar marcas digitales o marcas de agua en los medios electrónicos de manera oculta que identifiquen al autor, de tal forma que los actores que manipulen la información no perciban éstas señales y posteriormente se pueda detectar cuál es el origen de la transmisión

0.1.2. Área temática: Criptografía

0.1.3. Tema: Esteganografía

Este proceso de ocultar información de manera que no sea perceptible por los sentidos recibe el nombre de **Esteganografía**, y permite que un emisor y un receptor establezcan un canal de comunicación encubierto sin que terceros perciban la existencia de mensajes.

Por tanto en el desarrollo de este proyecto se pone a prueba las diversas técnicas existentes con relación a la Esteganografía lo que nos permite ampliar nuestro conocimiento y dar a conocerlo importante que es proteger nuestra información y lograr comprender lo benéfico que resulta aprovechar lo que la tecnología informática nos proporciona.

El análisis de esta técnicas nos muestra las ventajas de poder poner en seguridad nuestra información de una manera novedosa, esta técnica comprobada con herramientas y aplicaciones informáticas que nos posibilitan la demostración de cómo y cual es la funcionalidad de dicha técnica por lo cual también este nos indica como se compone y cual es la estructura de una imagen de mapa de BIT's (BMP) igualmente su manipulación y la variedad de técnicas esteganográficas que existen para poder codificar y decodificar información dentro de un archivo de esta extensión (BMP).

¹ Bit: Binary Digit. Dígito Binario.

0. ANTECEDENTES DEL PROYECTO

0.1. IDENTIFICACION DEL PROBLEMA

0.1.1. Área de conocimiento: Criptología

0.1.2. Área temática: Criptografía

0.1.3. Tema: Esteganografía

0.1.4. Título del proyecto: **ANALISIS COMPARATIVO ENTRE LAS DIVERSAS TECNICAS ESTEGANOGRAFICAS EN IMÁGENES DE MAPA DE BITS.**

0.2. PLANTEAMIENTO DEL PROBLEMA

0.2.1. Descripción

La Esteganografía es el arte o ciencia de comunicar de manera oculta un mensaje, camuflando la información entre otro conjunto de datos para que pase desapercibida. Hoy día suele utilizarse para esconder información en todo tipo de archivos tales como fotos, videos o audio.

El término Esteganografía proviene del griego "steganos" (secreto) y "grafía" (escrito), y los primeros documentos que describen el uso de estas técnicas datan de los tiempos de Herodoto en la Grecia antigua.

Durante la segunda guerra mundial el sistema más utilizado consistió en microfilmar un mensaje y reducirlo hasta el extremo de un pequeño punto, de forma que podía pasar como un signo de puntuación de un carácter dentro de otro texto. Por ejemplo, el punto de la vocal "i" podía ser en realidad un microfilm con un mensaje.

Con la llegada de los ordenadores se han ampliado y diversificado las técnicas esteganográficas. Una de las más comunes consiste en ocultar un mensaje dentro

de contenidos multimedia, mezclando los bits del mensaje original entre los bits del archivo gráfico o de sonido. El archivo resultante será una imagen o archivo de audio totalmente funcional que, a primera vista, no levanta ninguna sospecha, pero con el software² adecuado es posible extraer la información oculta.

El siguiente mensaje es un mensaje real mandado por un espía alemán de la segunda guerra mundial:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Si tomamos la segunda letra el siguiente mensaje emerge:

Pershing sails from NY June 1.

Así se pueden ver que existe vital información. Edgar G Hoover³ se refirió a "la pieza maestra de espionaje del enemigo" a los micro puntos. Esto era en si una foto de microfilm que pasaba por un punto dentro de la carta.

0.3. JUSTIFICACION

En la actualidad, la falta de seguridad en los sistemas de red y en los recursos computacionales en las organizaciones y en los hogares es un problema, consecuencia posterior a esto y debido al continuo crecimiento masificado de sistemas de redes, ya sea en el hogar, PYMES⁴ ó macro empresas, dan como resultado un mayor número de atacantes que quieren sacar provecho de manera ilegal de la información que reside en los equipos de cómputo, violando las normas y leyes de derechos de autor, estos atacantes con el transcurrir del tiempo

² Software: conjunto de actividades que tienen por objeto la concepción y el empleo de ordenadores electrónicos.

³ Edgar G Hoover: Personaje importante en los años 30 en los estados unidos por su lucha contra el hampa junto con el FBI.

⁴ PYME: Pequeñas y medianas empresas.



Nota

Este trabajo se encuentra disponible únicamente en **formato físico**, ya que no cuenta con versión digital. Por tal motivo, en este repositorio solo serán visibles las páginas preliminares con fines informativos. Para su consulta completa, el usuario deberá verificar la ubicación o sede donde se encuentra el ejemplar físico, o bien solicitar información adicional escribiendo al correo institucional:

repositoriofusm@sanmartin.edu.co