UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

"Desarrollo de Algoritmos esteganográficos usando descomposición en mapas de bits de segmentación compleja y transformación wavelet"

TRABAJO RECEPCIONAL
PARA OBTENER EL TÍTULO DE LICENCIADO EN
INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

PRESENTA:

Jaime Ramírez Pineda

Director del trabajo recepcional

Dr. Daniel Tapia Sánchez

Ciudad de México, agosto 2016

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Dedicatoria.

A Dios.
Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi padre Manuel Severiano
Quien en vida me brindo el apoyo incondicional, y ahora desde el cielo me bendice cada día.

A mi madre Margarita
Por apoyarme en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

Mis hermanos, Rafael, Julia, Nancy, Luis y Elizabeth, por estar conmigo y apoyarme siempre, los quiero mucho.

A mis familiares quienes me mostraron su apoyo durante mi formación y han estado al pendiente para impulsarme a seguir superándome.

A mis maestros quienes nunca desistieron al enseñarme y que continuaron depositando su esperanza en mí.

Al director y los sinodales, quienes prestaron su valioso tiempo para estudiar, corregir y aprobar mi tesis.

A la UACM por ser mi casa de estudios, y por brindarme el apoyo para la impresión y empastado del presente trabajo.

Resumen

Las técnicas de ocultación de la información se han desarrollado rápidamente con el fin de eliminar los riesgos y vulnerabilidades del medio de comunicación, y han acaparado la atención de la industria y del mundo académico, la ocultación de la información tiene dos ramas principales: la marca de agua digital y la esteganografía. La primera se utiliza principalmente para derechos de autor, mientras que, la última es una forma de comunicación encubierta. El principal propósito de la esteganografía es transmitir la información en secreto, ocultando la existencia de la misma en otro medio, tal como una imagen, audio o video.

En esta tesis se presentan dos algoritmos para incrustar información en una imagen digital usando esteganografía, por medio de la técnica de Segmentación Compleja de los Planos de Bit (BPCS), con la cual se encubrirá información específica dentro de un canal, de manera que parezca inocuo. Se presentarán por una parte el algoritmo basado en el dominio espacial, el cual utiliza una imagen como contenedora de datos, e inserta la información secreta en los planos de bits de la misma. En ambos métodos se propone obtener una medida de complejidad y con ella determinar áreas óptimas para llevar a cabo el proceso de la inserción de mensajes secretos. Por otra parte, se propone utilizar la esteganografía BPCS en la transformada Wavelet Discreta (BPCS-DWT), la cual tiene dentro de sus principales virtudes permitir modelar mejor procesos que dependen fuertemente del tiempo y cuyo comportamiento no tiene qué ser suave.

Abstract

The techniques of information have developed rapidly in order to eliminate the risks and vulnerabilities of the media, and have captured the attention of industry and academia, concealment of information has two main branches: the brand digital watermarking and steganography. The first is mainly used for copyright, while the latter is a form of covert communication. The main purpose of steganography is to transmit the information secret, hiding the existence of the same in another medium, such as an image, audio or video.

In this thesis two algorithms are presented for embedding information into a digital image using steganography, by the technique Complexity Segmentation bit plane (BPCS), with which specific information will conceal within a channel, so that it appears innocuous. They are submitted by a party based in the spatial domain algorithm, which uses an image as containing data, and inserts secret information on the plans of bits of it. In both methods it proposes to provide a measure of complexity and with it determine optimal areas to carry out the process of inserting secret messages. Moreover, it is proposed that the BPCS Steganography in Discrete Wavelet Transform (BPCS-DWT), which has among its main virtues allow better modeling processes that rely heavily on time and whose behavior does not have to be bland.

Índice

Lista de Tablas

Lista de figuras

Capítulo I - Introducción

1.1 Introducción

En la actualidad la comunicación por internet se ha convertido en un proceso común en casi todo el mundo, miles de millones de personas se comunican de un país a otro por este medio. Se estima que la cantidad de paquetes digitales transmitidos aumente casi tres veces en los próximos años (más de un millón de millones y medio de gigabytes por año para el 2018) (Carrasco, 2014), pero dado que internet resulta ser un medio hostil para la comunicación, surge la necesidad de mantener la privacidad y confidencialidad de la información transmitida. Por ejemplo, la vulnerabilidad de la comunicación entre corporaciones y dependencias gubernamentales y/o bancarias. Estas deben tener un grado de confidencialidad elevado en sus operaciones transmitidas por este medio, un ejemplo son las transacciones bancarias, las cuales deben mantenerse en secreto. Resulta importante el conocimiento de diversas técnicas para establecer mecanismos de seguridad que permitan eliminar los riesgos y vulnerabilidades en el medio (internet). Las técnicas de ocultación de la información se han desarrollado rápidamente con el fin de eliminar los riesgos y vulnerabilidades del medio de comunicación, las necesidades actuales en materia de seguridad de la información requieren métodos “confiables” para ocultar información. La esteganografía es una técnica que permite ocultar información dentro de un medio portador, el cual puede ser imagen, texto, audio o video. En esta tesis se abordarán algunas técnicas para ocultar información.

1.2 Objetivos

1.2.1 Objetivo general:

La presente tesis tiene como objetivo implementar el algoritmo de segmentación compleja de mapas de bits aplicado en el dominio espacial y en el dominio de la transformada wavelet, considerando medidas para evaluar la imagen con mensaje insertado.

1.2 .2 Objetivos específicos:

- Implementar el algoritmo esteganográfico BPCS en el dominio espacial en imágenes a color y en escala de grises.

- Implementar el algoritmo esteganográfico BPCS en el dominio de la transformada wavelet en imágenes a color y en escala de grises.

- Definir las medidas necesarias para evaluar el desempeño de los algoritmos variando el mensaje insertado.

- Realizar la extracción del mensaje en ambas implementaciones (dominio espacial y dominio frecuencial) y comparar el mensaje insertado con el extraído.

- Comparar el desempeño de los métodos desarrollados evaluando su capacidad de inserción y parámetros de calidad (BPP y MSE, PSNR).

1.3 Planteamiento del problema

Día con día el internet se convierte en parte integral de la vida cotidiana, la comunicación por este medio facilita y acelera el flujo de la información, pero existe la problemática de no mantener la seguridad y privacidad de lo que enviamos. En los últimos años se dieron a conocer documentos filtrados en los medios de comunicación (prensa), los llamados WikiLeaks pusieron al descubierto el gran problema que representa la intercepción de comunicaciones y el robo de información a nivel personal, corporativo, empresarial y gubernamental, podríamos ser víctimas sin saberlo.

En la actualidad existen técnicas que hacen frente a la exposición de la información en un medio hostil, la Estenografía es una técnica que tiene la capacidad de crear un canal de información oculto, lo cual dificulta a un atacante espiar nuestras comunicaciones y robar nuestros datos. La técnica más sencilla y utilizada es la del bit menos significativo o LSB por sus siglas en inglés, pero esta técnica se enfrenta al problema de tener baja capacidad de inserción, facilidad de detección del mensaje oculto, extracción del mismo, así como a la perdida y alteración de la información ante factores como la compresión y adhesión de ruido. El algoritmo propuesto se enfoca a abordar las problemáticas antes mencionadas.

1.4 Justificación

Existen métodos esteganográficos que ocultan información y soportan modificaciones como la compresión y adhesión de ruido, estos métodos hacen uso del dominio de la transformada la cual puede ser la DFT (Discrete Fourier Transform), la transformada DCT (Discrete Cosine Transform) o la transformada DWT (Discrete Wavelet Transform), estos métodos transforman una imagen en el dominio espacial al dominio espectral y de esta forma se oculta el mensaje secreto en áreas significativas de la imagen. Los métodos en el dominio espacial tienden a proporcionar mayor capacidad de inserción a diferencia de los métodos en el dominio de la frecuencia, sin embargo, los métodos en el dominio de la frecuencia son más robustos. El interés del estudio, análisis e implementación del algoritmo BPCS, es que al ser de dominio espacial ofrece alto porcentaje de capacidad de inserción, con baja modificación visual, además si se aplica en el dominio de la transformada lo convierte en un método robusto de gran capacidad de inserción.

1.5 Metodología

La presente tesis se realizó de acuerdo a la siguiente metodología:

- Se realizó un estudio y revisión del estado del arte de la esteganografía y sus diferentes algoritmos y metodologías.

- Se analizaron los algoritmos esteganográficos basados en las técnicas de segmentación compleja de planos de bits y la transformación wavelet.
- Se realizó la implementación del algoritmo esteganográfico BPCS en el dominio espacial y el dominio de la frecuencia.
- Se definieron las medidas de desempeño necesarias para evaluar el rendimiento de los algoritmos en escenarios específicos.

1.6 Organización de la tesis

El trabajo de Tesis se organiza de la siguiente manera:

- En el capítulo 1 se presenta la introducción, objetivos generales y específicos, planteamiento del problema y justificación.
- En el capítulo 2 se presenta el estado de arte de la esteganografía, donde se hace una reseña histórica de la esteganografía y las diferentes técnicas y metodologías en los dominios espacial y frecuencial.
- El capítulo 3 presenta una descripción de los algoritmos propuestos, los cuales están basados en la técnica de descomposición en mapas de bits de segmentación compleja BPCS (Bit-Plane Complexity Segmentation Steganography), el primer algoritmo aplicado en el dominio espacial y el segundo aplicado en el dominio frecuencial.

- El capítulo 4 presenta una descripción de los parámetros de evaluación, con los cuales se definió la calidad de la imagen con mensaje oculto.
- En el capítulo 5 se presentan los resultados para el dominio espacial y para el dominio de la transformada.
- En el capítulo 6 se presentan los comentarios, el análisis, las conclusiones y el trabajo a futuro.

Capítulo II - Marco Teórico

2.1 Introducción

Comunicarse de un punto otro hoy en día resulta ser un proceso que se ejecuta de manera rápida, pues en la actualidad se puede realizar una video llamada en tiempo real de un extremo a otro de nuestro planeta, todo esto debido a los avances tecnológicos que se van dando día a día , pero aun cuando la transmisión puede realizarse en tiempo real y existen "conexiones seguras", en el medio hay ojos y oídos que vulneran la seguridad, logrando observar y escuchar lo que se envía por medio de internet, estos resultan ser usuarios inadecuados que se interponen entre la comunicación origen y destino, hecho por el cual las agencias de estado y empresas que manejan información confidencial tratan de blindar la información mediante varios métodos con el objetivo tener una comunicación secreta, los motivos pueden ser diversos, desde el caso de la realización de una fiesta sorpresa, los mensajes de una pareja que desea mantener el anonimato su relación, o podría ser una comunicación entre organizaciones políticas o entre dependencias gubernamentales, o en el peor de los casos comunicación entre organizaciones criminales y/o terroristas. Desde hace años se ha buscado tener métodos de comunicación segura, pero dependiendo el método utilizado este es útil durante el tiempo que tarda el intruso en descubrirlo y descifrarlo, técnicas como la criptología y la esteganografía son utilizadas de manera efectiva, y de manera conjunta debido a la efectividad.

En este capítulo se presenta el marco teórico, el cual consta de una reseña histórica, orígenes, así como algunas definiciones conceptuales y la definición detallada de esteganografía. Se consideran también las diversas técnicas esteganográficas existentes, como lo son la aplicación en el dominio espacial y el dominio de la frecuencia, haciendo referencia del principio básico y los protocolos de la esteganografía.

2.2 Origen e Historia de la esteganografía

Existen antecedentes a cerca de la esteganografía que resultan fascinantes, los cuales son mencionados por Heródoto de Halicarnaso, en su obra “Los Nueve Libros de la Historia”, en el texto se narra como un famoso tirano griego llamado Histieo rapo a su más fiel esclavo y tatuó en la cabeza un mensaje en el que alentaba a un aliado a rebelarse contra los persas, el hecho de escribir el mensaje en la cabeza radica en el hecho de esperar a que creciera el pelo del esclavo para poder mandar el mensaje y el destinatario tuvo que afeitar la cabeza del emisario para poder leerlo (Gelinek, 2008).

A lo largo de la historia se han utilizado diferentes métodos para ocultar la información, dentro de los cuales los más conocidos son la tinta invisible, la cual fue muy usada durante la segunda guerra mundial, las marcas hechas por medio de pequeños orificios hechos con pinchazos de alfiler. Otro hecho histórico de la esteganografía fue la manera en que los griegos del siglo V a. C. se enteraron del plan de invasión de Persia,

pues según se narra en la obra del historiador Herodoto “Los nueve libros de la Historia” cuenta como Demarato, un exiliado griego de Persia, grabó los planes persas en un par de tablillas de madera y después las cubrió con cera, ocultando así el mensaje, dichas tablillas partieron desde la ciudad persa de Susa hasta Esparta sin ser interceptadas en el camino (Heródoto, 2009). Una vez en su destino, Gorgo, la esposa del rey Leónidas, adivinó que debajo de la cera debería encontrase algo escrito. Una vez leído el mensaje, Esparta comunicó las intenciones persas al resto de las ciudades griegas y, gracias a ello, los griegos pudieron armarse a tiempo y derrotar a los persas en las batallas de las Termópilas, de Salamina y Platea. Otro antecedente es la escritura con tinta invisible, la cual seguramente es la técnica más empleada en todos los tiempos, existen antecedentes de que en el siglo I, “Plinio el viejo mostró cómo hacer tinta invisible con el jugo de ciertas plantas, dichas tintas eran llamadas simpáticas, se hacen visibles al entrar en contacto con otra sustancia o calor” (Ortega, 2005). En el siglo XV El científico italiano Giovanni Batista della Prota descubrió cómo esconder un mensaje dentro de un huevo cocido, el método consistía en preparar una tinta mezclando una onza de alumbre y una pinta de vinagre, y luego se escribía en la cáscara. “La solución penetra en la cáscara porosa y deja en la superficie de la albúmina del huevo duro, que se puede leer pelando el huevo” (López, 2012). Eneas el estratega propuso diferentes técnicas de esteganografía que para su época resultaban novedosas y efectivas, algunos de estos métodos es el ocultamiento de mensajes en los aretes de las mujeres y los mensajes enviados por medio de palomas mensajeras. La lingüística esteganográfica también llamado acróstico, fue uno de los métodos más populares de la antigua esteganografía.

Una versión más avanzada de la lingüística esteganográfica fue concebida originalmente en China y reinventada por Girolamo Cardano, la cual es conocida también como rejilla móvil, de celosía o de Cardano, en honor a su autor (siglo XVI), consiste en un cuadro de lados iguales que se puede utilizar siempre, dividido en tantas cuadriculas como se quiera, y de las cuales se vacían la cuarta parte. De ahí, que al girarlo y colocarlo en cada una de las cuatro posiciones posibles vayan dejando al descubierto espacios distintos. “Los mensajes secretos eran escondidos en las letras iniciales de cada párrafo o en los tercetos consecutivos de un poema” (Muñoz & Ramio, 2013) .

Un ejemplo esteganográfico curioso en este periodo tuvo lugar en la Inglaterra del siglo XVI donde la esteganografía tuvo una gran importancia en las conspiraciones urgidas entre los nobles católicos ingleses que querían destronar a la reina protestante Isabel I (1533-1603) y entregar el trono a la católica María I de Escocia (1542-1587). La comunicación entre los conspiradores y la reina María debía pasar lo más desapercibida posible ya que cualquier conocimiento de esta implicaría ser acusados de alta traición y condenados a muerte. Por este motivo, emplearon tanto criptografía como esteganografía para ocultar sus mensajes. Un mecanismo recurrido fue la ocultación de mensajes en barriles de cerveza que se transportaban sin levantar la atención (ídem).

En una obra del científico alemán Gaspar Schott (1608-1666) “Schola Steganographica” se describía como ocultar mensajes en partituras de música, haciendo

equivaler una nota musical concreta con una letra. En ningún momento se buscó que las notas musicales tuvieran alguna coherencia y su resultado diera una melodía agradable, en cualquier caso, su representación, por ejemplo, en papel, permitía perfectamente ocultar un mensaje. Basado en estas ideas surgieron otros procedimientos de ocultación, como los basados en el número de ocurrencias de las notas (ibíd).

2.3 Técnicas de protección de la información

El interés concreto de un sistema esteganográfico dependerá de tres características:

- capacidad (cantidad de información que puede ser ocultada)
- seguridad/invisibilidad (probabilidad de detección por un estegoanálista)
- robustez (cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta).

Stefan Katzenbeisser en su obra “Information Hiding Techniques for Steganography and Digital Watermarking” menciona que entre las principales subdiciplinas para ocultar información se encuentran las siguientes:

Canales encubiertos (Covert chanel): Es un canal que puede ser usado para transferir información, pero para que la comunicación sea posible debe haber un preacuerdo entre emisor y receptor que codifique el mensaje de una forma que el receptor sea capaz de interpretar. Para comprender mejor el concepto, se acudirá al ejemplo de los prisioneros el cual se detallará más adelante.

Anonimato (Anonymity): Es el ocultamiento de los metadatos de los mensajes, es decir, el remitente y el destinatario no son revelados. La idea es que se pueda ocultar el rastro de un mensaje mediante el uso de un conjunto de remailers o routers, por ejemplo, se reenviaban mensajes anónimos con el fin de obscurecer el rastro del mensaje, con un número de reenvíos tan largo que los intermediarios no podían atacar el mensaje.

Escritura Cubierta (Steganography): Mientras que la criptografía se encarga de proteger el contenido de los mensajes, la esteganografía es la ciencia que se encarga de ocultar la existencia del mismo. En la actualidad la esteganografía se usa para esconder mensajes dentro de otro mensaje, de tal forma que el más externo se hace público (visible por todos) y solo el receptor de dicho mensaje, aplicando alguna descodificación, podrá recuperar el mensaje oculto. Más adelante se ampliará la definición y se presentarán diferentes ejemplos.

Watermarking (Marcas de Agua): Las marcas de agua tradicionales o físicas son agregadas a algunos tipos de papel (el uso más común es en billetes) para bridar una prueba de autenticidad. Al contrario de la esteganografía, tiene un requerimiento adicional

de robustez contra posibles ataques en donde se trata principalmente de hacer que la marca sea indetectable; sin embargo, las marcas de agua no siempre necesitan ocultarse, ya que algunos sistemas utilizan marcas de agua digital visibles.

2.4 Definición de la esteganografía

La palabra esteganografía procede del griego y consta de dos palabras *steganos*, que significa encubierto y graphos, que significa escritura, por tanto, su traducción completa es "escritura encubierta". Existen diversas definiciones que se manejan en los textos relacionados con la esteganografía, de las cuales a continuación se presentan algunas.

“La esteganografía es el arte de encubrir información específica dentro de un canal que parezca inocuo” (Eason, 2003).

“La esteganografía se refiere a la información que se oculta en archivos digitales que pueden ser audio, video e imágenes” (H. Noda, 2002, págs. 98-107).

“Esteganografía es el conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos” (Gómez Cárdenas, 2016).

En el contexto de las comunicaciones seguras, dos partes pueden intercambiar información oculta sobre un canal inseguro de modo que, aunque una tercera parte

> no autorizada intercepte, y realice un análisis de los datos de información, no podrá detectar o probar la existencia de la información oculta y solo percibirá su portadora, contenedor, cubierta, envoltorio o texto inocuo utilizado como tapadera (Areitio, 2008, pág. 404).

La esteganografía moderna utiliza un medio digital como archivos de texto, audio, imagen y video que son utilizados como archivos portadores, el mensaje secreto se oculta en estos, a este tipo de archivos portadores se les denomina contenedores, cubiertas o portadoras, de igual forma el mensaje secreto o la información a ocultar, puede ser cualquier medio digital, cuando el mensaje secreto es ocultado en el contenedor a través de una técnica esteganográfica se obtiene un estego-objeto que contendrá el mensaje oculto en el archivo portador. El proceso descrito se muestra en la figura 2.1, puede observarse al contenedor y el mensaje secreto que puede o no hacer uso de técnicas de cifrado para darle una mayor protección a la información. En el canal, aunque ninguna persona sospechara la existencia del mensaje, éste se encuentra expuesto a cualquier ataque. Finalmente, para recuperar el mensaje secreto se aplica el proceso inverso.

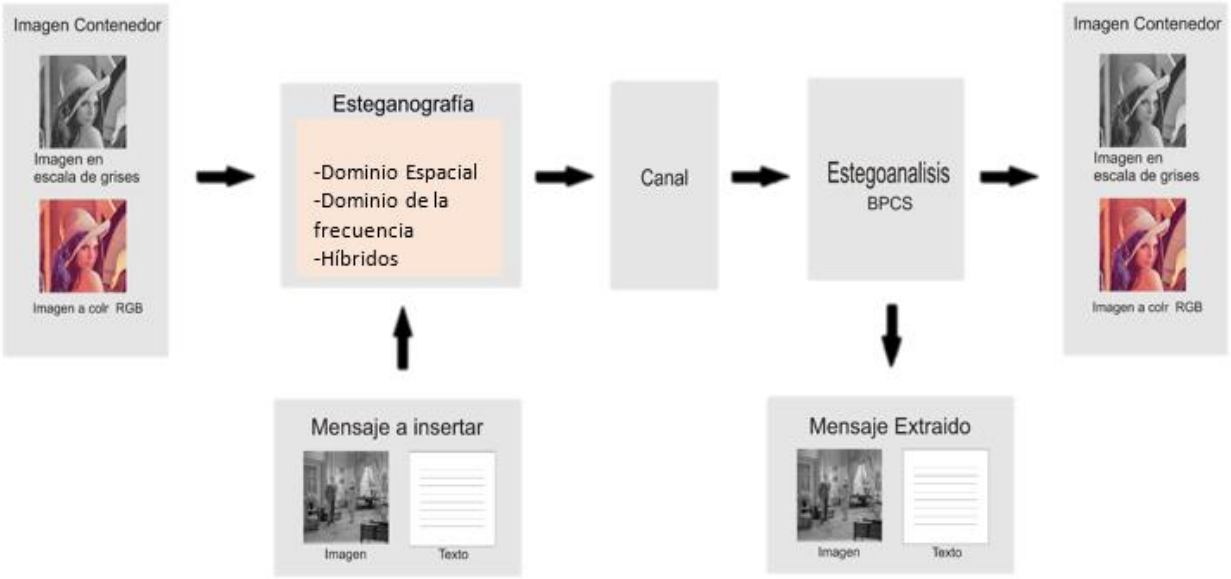


Figura 2.1. Proceso esteganográfico.

Los actores implicados en el campo de la esteganografía pueden definirse de la siguiente manera:

Contenedor: se trata de la entidad que se emplea para portar el mensaje oculto, este puede ser elegido entre una gran variedad de archivos digitales, por ejemplo, audio, video e imágenes.

Mensaje: Es la información que se desea transmitir.

Esteganograma: se trata del objeto contenedor más el mensaje encubierto. Se refiere al objeto que ya tiene el mensaje adherido a él y se utilizará para transmitir este mismo mensaje a través del canal.

Canal: Medio por el cual es transmitida la información.

Estegoanálisis: Ciencia que estudia la detección de información dentro de un esteganograma. La detección de la información puede realizarse por medio de ataques pasivos o activos.

Adversario: son todos aquellos entes a los que se trata de ocultar la información encubierta. Este adversario puede ser pasivo o activo.

Adversario pasivo: Es aquel que sospecha que se puede estar produciendo una comunicación encubierta y trata de descubrir el algoritmo que se extrae del estego-objeto, pero no trata de modificar dicho objeto.

Adversario activo: Aquel que además de tratar de hallar el algoritmo de comunicación encubierta, modifica el estego-objeto con el fin de corromper cualquier intento de mensajería subliminal.

2.5 Principio básico de la esteganografía

La esteganografía con un adversario pasivo está muy bien ilustrado en el problema de los prisioneros (Simmons, 1998).

“Alice y Bob son detenidos por algún delito y son encarcelados en celdas diferentes. Ambos quieren desarrollar un plan de escape, para su desgracia cualquier tipo de comunicación entre ellos será vigilada por la guardia Wendy, misma que no les

permite la comunicación por medio de mensajes cifrados y si ella nota cualquier comunicación sospechosa los confinará a una celda de aislamiento total, por lo que ambas partes desean comunicarse de manera secreta sin que Wendy se dé cuenta de los mensajes, por lo que tienen que establecer un canal subliminal de comunicación. Una forma práctica de hacerlo es ocultar el significado de la información en un mensaje que no despierte sospecha alguna. Por ejemplo, Bob podría esconder su mensaje usando la primera letra de cada palabra dentro de un párrafo aparentemente inocente el cual no llamara la atención de Wendy.

Para la desgracia de los prisioneros existen otros problemas que dificultarán el escape de Alice y Bob, por ejemplo, Wendy puede alterar el mensaje que Bob le ha mandado a Alice. Wendy podría cambiar las palabras que Bob ha usado y así destruir la información, o aun peor, si actuara de forma maliciosa podría falsificar en mensaje y enviarlo a uno de los dos criminales pretendiendo ser uno de ellos".

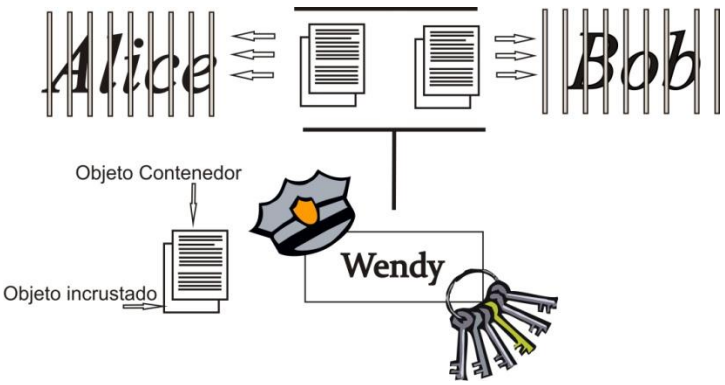


Figura 2.2. Modelo esteganográfico del problema de los prisioneros. (Stefan Katzenbeisser, Fabien A. P. Petitcolas, 2000).

El modelo presentado en la figura 2.2 es generalmente aplicable en situaciones de comunicaciones esteganográficas, donde Alice y Bob representan dos partes de la comunicación (emisor y receptor) deseando intercambiar información secreta, así mismo la guardia Wendy representa un tercer sujeto con posibilidad de leer y posiblemente alterar los mensajes enviados entre emisor y receptor.

Teniendo en cuenta que pueden existir adversarios activos, una buena técnica esteganográfica debe ser robusta ante distorsiones, ya sean accidentales o fruto de la interacción de un intruso activo.

2.6 Protocolos esteganográficos

La mayoría de las aplicaciones esteganograficas surgen a partir del principio general, que se ilustra en la Figura 2.3. Alice, tiene la intención de compartir un mensaje secreto m con Bob, elige al azar (usando la fuente aleatoria privada r) un mensaje inofensivo c, llamado objeto de presentación, el cual puede transmitirse a Bob sin levantar sospechas, e incrusta el mensaje secreto en c, probablemente usando una clave k, llamado clave estego. Por lo tanto, Alice cambia la cubierta c para un estego-objeto s. Esto debe ser hecho de una manera muy cuidadosa, de manera que un tercer partido, sabiendo sólo el mensaje s aparentemente inofensivo, no pueda detectar la existencia del secreto. En un sistema “perfecto”, una cubierta normal no debe ser distinguible de un estego-objeto, ni por un ser humano ni por un dispositivo electrónico que busque un

patrón estadístico. En teoría, las cubiertas pueden ser cualquier dato entendible por una computadora, este puede ser: imagen, sonido digital o texto escrito.

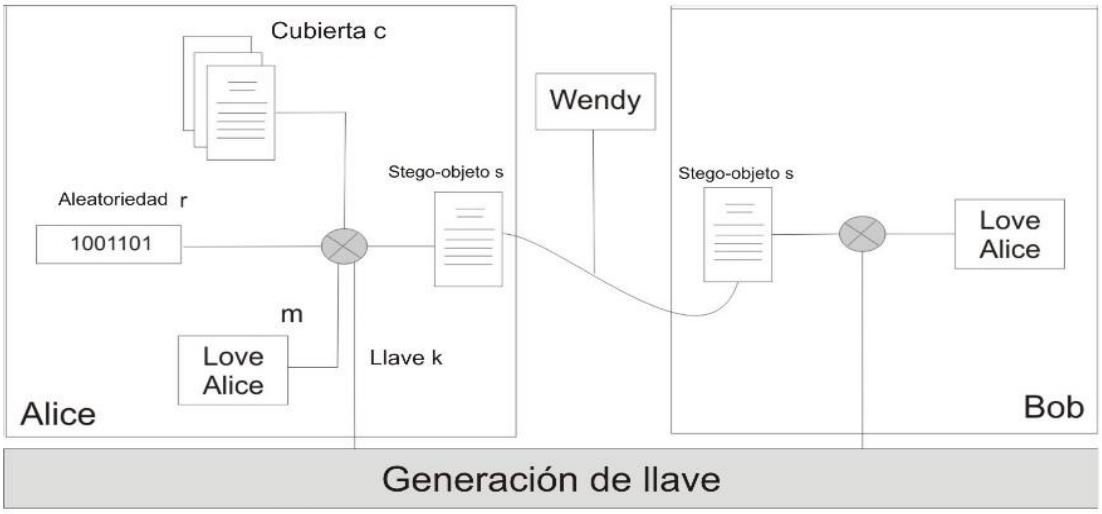


Figura 2.3. Descripción esquemática del problema de los prisioneros: Alice elige al azar una cubierta c utilizando una fuente aleatoria privada r, y un mensaje m oculto en c utilizando una llave k, la creación del estego-objeto s se pasa a Bob. Bob reconstruye m con la clave k que comparte con Alice. Katzenbeisser S. et al. (2000)

Alice transmite a Bob sobre un canal inseguro, y espera que Wendy no notará el mensaje incrustado. Bob puede reconstruir m ya que él sabe el método de incorporación utilizado por Alice, y tiene acceso a la llave K, la cual es utilizada en el proceso de incrustación. Este proceso de extracción debe ser posible sin la cubierta original c. Una tercera persona que observa la comunicación no debe ser capaz de decidir si el emisor está activo en el sentido que envía cubiertas que contiene mensajes secretos en lugar de

las tapas sin información adicional. De manera más formal, si un observador tiene acceso al conjunto $\{C_1, C_2 ... C_n\}$ de objetos de cubertura de transmisión entre ambas partes, la comunicación debe ser capaz de decidir cuáles objetos cubierta C_i contienen información secreta. Por lo tanto, la seguridad de la comunicación invisible se presenta principalmente en la incapacidad de distinguir objetos cubierta de los estego-objetos. En la práctica, sin embargo, no todos los datos pueden ser utilizados como cubiertas para la comunicación secreta, ya que que las comunicaciones empleadas en el proceso de inserción no deben ser visibles para alguien no involucrado en el proceso de comunicación.

Este hecho requiere que la cubierta contenga suficientes datos, los cuales pueden ser reemplazados por información secreta. Como ejemplo, debido a errores de medición cualquier resultado de algún proceso de escaneo físico, contendrá un componente estocástico llamado ruido, tales artefactos[1] aleatorios pueden utilizarse para él envió de información secreta. De hecho, se tiene que los datos ruidosos tienen propiedades más ventajosas en la mayoría de aplicaciones esteganográficas. Una cubierta no debe ser utilizada dos veces debido a que el atacante, tiene acceso a las dos versiones de la cubierta y puede fácilmente detectar y posiblemente recuperar el mensaje. Para evitar el rehúso accidental, tanto el emisor como el receptor deben destruir todas las cubiertas que han utilizado para la transferencia de información.

[1] Los artefactos se refieren a una serie de cambios indeseables de una imagen digital causado por el sensor, la óptica y algoritmos de procesamiento de imagen interna de la cámara. Vincent Bockaert. (2015). Artifacts. 20 Diciembre 2015, de DP PREVIEW Sitio web: http://www.dpreview.com/glossary/digital-imaging/artifacts

2.6.1 Técnicas Esteganográficas

Gran cantidad de métodos esteganográficos se han propuesto recientemente, en la mayoría de ellos se pueden ver sistemas de sustitución. Estos métodos tratan de sustituir las partes redundantes de una señal con el mensaje secreto. La principal desventaja que estos métodos presentan es la relativa debilidad de la cubierta para ser modificada. Gracias a que existe un gran interés por la protección de la información, y con el fin de resolver los problemas de los métodos de sustitución se han desarrollado nuevas técnicas robustas, con las cuales se han construido sistemas esteganográficos seguros.

Los métodos de esteganografía se clasifican de acuerdo a las características que emplea, por ejemplo: uno de ellos se clasifica de acuerdo al tipo de cubierta que utiliza para la comunicación secreta, mientras que otro los clasifica de acuerdo a las modificaciones que se aplicaron en el proceso de ocultamiento.

(Katzenbeisser & Petitcolas, 2000) clasifican a los sistemas esteganográficos en las siguientes categorías:

- Sistemas de sustitución: En este sistema se sustituyen las partes redundantes de una cubierta, por un mensaje secreto.
- Técnicas en el dominio de la transformada: Inserta la información secreta en un espacio transformado de la señal, por ejemplo, DCT y DFT.

- Técnicas de espectro disperso. En estas se adoptan ideas utilizadas en las comunicaciones de espectro disperso.
- Método estadístico. Esta técnica codifica información cambiando varias propiedades estadísticas de la cubierta, y utiliza pruebas de hipótesis en el proceso de extracción.
- Técnicas de distorsión. Almacenan información por distorsión de señales y miden la desviación de la cubierta original en el paso de la codificación.
- Métodos de generación de cubierta. Codifican información de tal forma que se crea una cubierta para comunicación secreta.

2.7 Métodos en el dominio espacial

Se dice que una imagen se encuentra en el dominio espacial cuando los procedimientos operan directamente sobre los pixeles. Las transformaciones de procesamiento de imágenes en el dominio espacial se pueden expresar como:

$$g(x,y) - T\{f(x,y)\} \tag{2.1}$$

Donde f (x, y) es la imagen de entrada, g (x; y) es la imagen procesada, y T es el operador de definido sobre alguna vecindad del punto (x, y) (González, 1996).

2.7.1 Sistemas de sustitución

Estas técnicas utilizan los niveles de pixeles grises y sus valores de color directamente para que codifique los bits del mensaje. Estas técnicas son algunos de los esquemas más simples en términos de la incorporación y la complejidad de extracción. El principal inconveniente de estos métodos es la cantidad de ruido aditivo que se adhiere a la imagen, que afecta directamente a la pico señal a ruido y las propiedades estadísticas de la imagen. Además, estos algoritmos de incrustación son aplicables a la compresión de imágenes sin perdida, como las imágenes TIFF. Para los esquemas de compresión con pérdida como JPEG, algunos de los bits de mensaje consiguen perdida durante la etapa de compresión. El algoritmo más común que pertenece a esta clase de técnicas es el bit menos significativo o LSB por sus siglas en inglés (***Least Significant Bit***), esta técnica se basa en el reemplazo del bit menos significativo, utiliza la representación binaria de los niveles de gris de pixel para representar el bit de mensaje.

La inserción del mensaje secreto en los diferentes planos de bits, hasta los algoritmos de compresión que modifican propiedades de la imagen como la luminancia. Un sistema básico de sustitución trata de ocultar la información secreta sustituyendo las partes insignificantes de la cubierta por los bits del mensaje secreto, el mensaje puede ser extraído si se conocen los puntos donde la información fue incrustada.

2.7.2 Bit Menos Significativo ó LSB (LeastSignificant Bit)

El algoritmo del Bit Menos Significativo es un método escalar para marcar, comúnmente imágenes, donde cada pixel es representado por cadenas de 8 – bits. En su forma básica, para cada pixel de la imagen se modifica un solo bit de información, el menos significativo (Eason, 2003, págs. 18-31).

El método de Inserción en el Bit Menos Significativo, llamado también método de sustitución, consiste en reemplazar el Bit menos significativo de los pixeles de una imagen por otros Bits que representan el mensaje que se quiere ocultar.

El principio de funcionamiento del método de sustitución consiste en guardar información en los bits menos significativos de manera que los cambios no sean percibidos por el ojo humano. Por ejemplo, si se quisiera esconder dentro de una imagen la letra A, la cual es representada en el código ASCII por el siguiente valor binario: 01000001, el cual está formado por una cadena de 8 bits, para una imagen a color RGB necesitaríamos utilizar 3 pixeles de la imagen, cada pixel tiene 3 bytes para cada color, en las figuras 2.4 y 2.5 puede apreciarse el reemplazo de los bits.

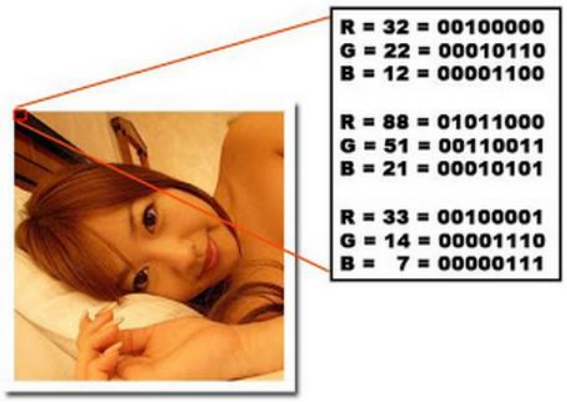


Figura 2.4 Valores de pixel en RGB. (jc mouse, 2015)

Al aplicar la sustitución LSB de cada número binario por cada bit del carácter "A" se obtendría el mensaje encubierto (estego-objeto).

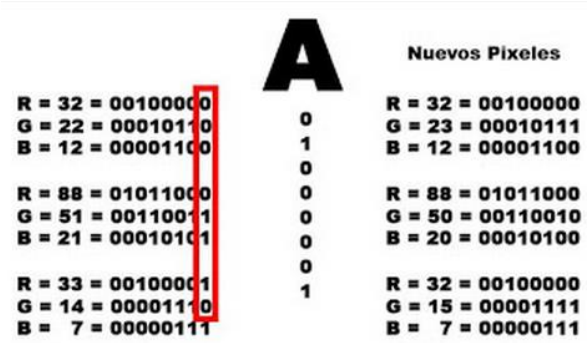


Figura 2.5 Sustitución de los bits menos significativos por una cadena de valores. (jc mouse, 2015)

En la figura 2.5 se puede observar que se ha sustituido cada Bit LSB (mostrado en el recuadro) por cada Bit de carácter "A" formando nuevos valores para los colores RGB, estos nuevos colores no cambian mucho con respecto a la intensidad del color y así no pueden ser distinguidos por el ojo humano, logrando de esta forma pasar inadvertidos.

Este método quizá sea una de las técnicas más comunes y también una de las más sencillas de la esteganografía en imágenes, este método permite el ocultamiento de una gran cantidad de información con un mínimo deterioro perceptual de la imagen-encubridora.

La ventaja de este tipo de métodos es la facilidad de codificación y decodificación, sin embargo, presenta desventajas notables como graves limitaciones al momento de la compresión, por ejemplo, en el caso de utilizar una imagen digital como portadora, los valores de los bits menos significativos cambian al realizar un proceso de compresión con pérdidas por lo tanto al momento de realizar la decodificación, de los datos insertados, es imposible obtener los datos del mensaje oculto incrustado. A pesar de esto es muy fácil realizar un software, el cual utilice el método de ocultamiento de datos mediante LSB.

2.7.3 Técnica de Espectro Ensanchado (*Spread Spectrum*)

Desde la década de 1950 se han desarrollado tecnologías de la comunicación en un intento por proporcionar un medio de baja probabilidad de intercepción y eliminación de las interferencias en las comunicaciones. (Noda, Niimi, & Kawaguchi, 2015) definen como técnicas de propagación de espectro como medios de transmisión en la que la señal ocupa un ancho de banda superior a la mínima necesaria para él envió de información: la extensión de banda se lleva a cabo por medio de un código que es independiente de la de los datos y una recepción sincronizada con el código en el receptor se utiliza para la inversión de la dispersión y los datos posteriores a la recuperación. Aunque la potencia de la señal a ser transmitida puede ser grande, la relación señal a ruido en cada banda de frecuencia será pequeña. Aunque partes de la señal pueden ser destruidas en varias bandas de frecuencia, la señal debe estar presente lo suficientemente en las otras bandas para poderla recuperar. Por lo tanto, SS hace que sea difícil de detectar y/o eliminar una señal. Esta situación es muy similar a un sistema de esteganografía que trata de difundir un mensaje secreto sobre alguna cubierta con el fin de que sea imposible de percibir. Dado que las señales difundidas tienden a ser difíciles de eliminar. Normalmente, en un canal de comunicación se desea que toda la información está restringida a una región estrecha del espectro de frecuencia para conservar el ancho de banda disponible y reducir la potencia. La técnica de espectro ensanchado hace lo contrario: busca codificar toda la información utilizando la mayor cantidad de componentes de frecuencia como sea posible. Esto permite la recepción de la señal, aunque haya interferencia en algunas frecuencias. La técnica de espectro

disperso (Spread- Spectrum SS) fue introducida por (Dixon, 1994), para calmar el problema del ocultamiento LSB contra los ataques. El método agrega una secuencia pseudo-aleatoria dispersa en la imagen. La secuencia pseudo-aleatoria es construida a partir del mensaje a ser ocultado. El método y sus variaciones propuestas para aplicaciones de marcas de agua son robustas contra ataques tales como compresión, ruido aditivo y operaciones de procesamiento de señales.

Sin embargo, en general es bien sabido que la capacidad de inserción de la técnica SS es baja, especialmente para las implementaciones de detección a siegas. Esto es porque los métodos aditivos no utilizan el hecho de que la señal huésped es conocida por el codificador. Por lo que la señal misma termina siendo el ruido o interferencia en el sistema.

Son las estadísticas de correlación. Si la señal portadora original está disponible en el receptor, el desempeño puede ser mejorado con solo substraer la señal portadora original de los datos antes correlacionados con los patrones

2.7.4 Esteganografía de segmentación de la complejidad de los planos de bits (BPCS)

La esteganografía BPCS se introdujo por Niimi (Ingemar, Miller, Bloom, Fridrich, & Kalker, 2008), para superar las deficiencias de técnicas esteganográficos tradicionales como la del bit menos significativo (LSB), la técnica BPCS realiza el ocultamiento de la información en las regiones ruidosas que hay en los planos de bits de la imagen-

encubridora. Para incrustar el mensaje secreto, el algoritmo BPCS primero segmenta cada plano de bits en bloques para después medir la complejidad de estos. El propósito de medir la complejidad es para tener un parámetro que nos indique el grado de información significativa que hay en cada bloque. La esteganografía BPCS usa una medida de complejidad basada en el cambio de valor de un píxel con respecto a sus vecinos, en una imagen binaria. Más adelante (capitulo III) se describirá de manera detallada este método.

2.8 Métodos en el dominio de la transformada

Una transformación es la operación que un sistema realiza. Por lo tanto, los sistemas y las transformaciones están estrechamente vinculados. Una transformación puede tener una inversa, que restaura al valor original.

En general, los métodos de sustitución (dominio espacial) tienden a proporcionar mayor capacidad de inserción que los métodos en el dominio de la transformada (también conocidos como dominio de la frecuencia), sin embargo, estos últimos son más robustos contra ataques, tales como compresión, recorte o algún otro procesamiento de imagen (M. Statler, 2015).

Los métodos en el dominio de la frecuencia utilizan transformaciones como la DFT (Discrete Fourier Transform), la DCT (Discrete Cosine Transform), la transformada Z, o

la transformada Wavelet como medio para ocultar el mensaje secreto en áreas significativas de la imagen.

Las técnicas de modificación LSB son una manera fácil para insertar información, pero también son vulnerables a pequeñas modificaciones en la cubierta, un atacante puede simplemente aplicar técnicas de procesamiento de señales a fin de destruir completamente la información secreta, en muchos casos usando un sistema de pérdida de compresión produce pérdida total de la información. En la mayoría de los casos, cualquier pequeño cambio significaría la perdida de la información, pero esto ha sido tomado en cuenta en el desarrollo de sistemas esteganográficos, que insertan la información en el dominio de la frecuencia de la imagen.

Los métodos en el dominio de la transformada esconden los mensajes en partes significativas e la imagen contenedora, lo cual los hace más robustos a ataques como las compresiones, los recortes y a algunos procesamientos de imágenes, más robustos que los métodos de sustitución como el LSB. De cualquier forma, aunque estos métodos son más robustos a diferentes tipos de procesamiento de señal, éstos mantienen la imperceptibilidad con respecto al sistema de visión humano (Velasco, López, Nakano, & Pérez, 2007).

2.8.1 Transformada Wavelet

El termino Wavelet se ha propuesto que se introduzca al español por ondeleta o función localizable en el tiempo. Tiene aplicaciones en numerosas áreas que impliquen

el análisis de señales, en muchos casos desplazando a la Transformada de Fourier (Sánchez G, 2013, pág. 466). Vista desde una perspectiva del análisis o procesamiento de señales puede ser considerada como una herramienta matemática para la representación y segmentación de señales, análisis tiempo-frecuencia e implementación de algoritmos sencillos y rápidos desde el punto de vista computacional. Las características propias de la transformada wavelet nos otorgan la posibilidad de representar señales en diferentes niveles de resolución, representar en forma eficiente señales con variaciones de picos abruptos, así como analizar señales no estacionarias. Nos permite conocer el contenido en frecuencia de una señal y cuando estas componentes de frecuencia se encuentran en la señal.

Tradicionalmente las señales se representan mediante la transformada de Fourier. Una nueva opción es utilizar ondeletas (wavelets) en vez de ondas largas. Las wavelets son una alternativa, no un reemplazo. Estas nuevas transformadas son más locales: encuentran un compromiso entre tiempo y frecuencia. Por lo que ingenieros y matemáticos han explorado varias transformaciones que tienen funciones básicas de duración limitada. Estas funciones básicas varían de posición, así como en frecuencia. Son ondas de duración limitada y se refiere a ellas como wavelets.

Las transformadas basadas en ellas se llaman Transformadas Wavelet. La Figura 2.7 ilustra la diferencia entre ondas y wavelets. Las primeras son dos ondas coseno que difieren en frecuencia y posición de eje (Castleman, 2002).

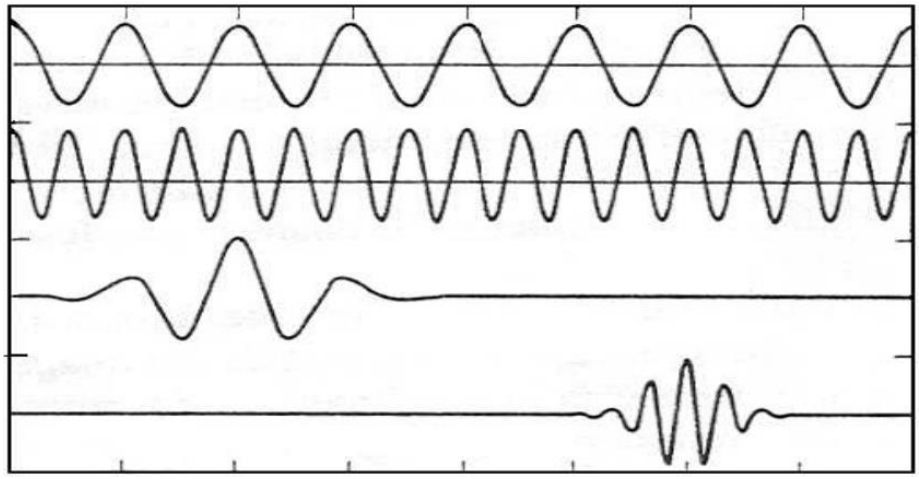


Figura 2.6 Ondas cosenoidales (arriba) y wavelets (abajo). (Walter & Cova , 2006)

Las wavelets proporcionan una herramienta matemática flexible para problemas prácticos en ciencia e ingeniería. En la última década se han aplicado con éxito al análisis de señales en disciplinas tan diversas como la medicina, la ingeniería eléctrica, teledetección y muchas otras. Una de las principales virtudes de las wavelets es que permiten modelar mejor procesos los cuales dependen fuertemente del tiempo y cuyo comportamiento no tiene por qué ser suave.

2.8.2 ¿Qué hace la wavelet?

Permite realizar análisis localizados en el tiempo de una gran señal, brindando la posibilidad de encontrar discontinuidades o picos de corta duración que de otra manera seria complicado detectar y tratar. El análisis FFT por sí solo no detecta estos eventos y debe recurrir a la transformada corta quien a través de la elección de una ventana de ancho adecuado permite el estudio de manera aceptable. El análisis Wavelet es capaz

de mostrar aspectos de los datos que con otras técnicas del análisis de señales no pueden ser apreciadas y se dejan pasar por alto, como son: la tendencia, puntos de ruptura y discontinuidades en las derivadas de orden superior.

2.8.3 Familias de Wavelets

Las transformadas wavelets comprenden un amplio conjunto de formas. A lo largo del tiempo se han ido desarrollando diferentes versiones de wavelets, lo que han dado lugar a familias de wavelets. Las diferentes familias de wavelets hacen diferencias entre que tan compactas están las funciones básicas localizadas en el espacio y que tan finas son. (Pereira, 2007).

Entre las familias de wavelets más comunes se encuentran las siguientes:

2.8.3.1 Wavelet Haar

Las funciones que actualmente se denominan “wavelets Haar” se han utilizado desde 1910 cuando se introdujeron por el matemático húngaro Alfred Haar. Estas funciones consisten simplemente en un breve impulso positivo seguido de un breve impulso negativo. Aunque los impulsos breves de las wavelets de Haar son excelentes para la enseñanza de la teoría de las wavelets, no resultan de tanta utilidad en la mayoría de aplicaciones, ya que producen líneas irregulares con picos en lugar de curvas suaves.

Este tipo de wavelet son es las más simples y antiguas de todas las wavelets (S. Taubman & W. Marcellin, 2002).

La wavelet Haar está dada por:

$$s(t) = \begin{cases} 1, & 0 < t < 0.5 \\ -1, & 0.5 < t < 1 \\ 0, & en\ otro\ caso \end{cases} \quad (2.2)$$

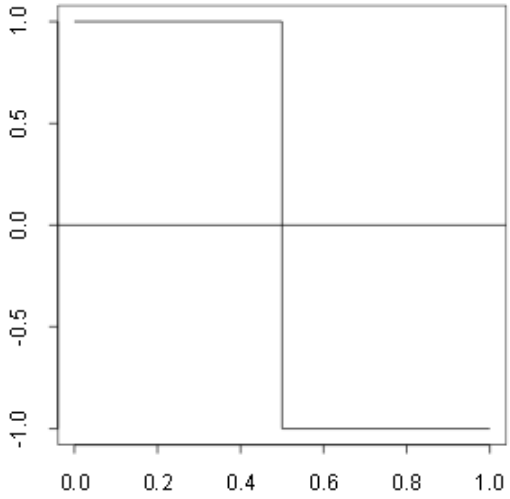


Figura 2.7 Wavelet Haar.

2.8.3.2 Wavelet de Morlet

En 1984, Jean Morlet introdujo el trabajo de Dennis Gabor a la comunidad de la sismología y, con Goupillaud y Grossmann, lo modificó para mantener la misma forma de ondas sobre la igualdad intervalos de octava, dando lugar a la primera formalización de

la transformada wavelet continua. Posteriormente, se conocerían como wavelets de Morlet. Independientemente de que los componentes se dilaten, compriman o desplacen en el tiempo, mantienen la misma forma. Se pueden construir otras familias de wavelets adoptando una forma diferente, denominada wavelet madre, y dilatándola, comprimiéndola o desplazándola en el tiempo.

La Wavelet Morlet se representa mediante la siguiente expresión:

$$mor = e^{-\frac{x^2}{2}} cos5x \tag{2.3}$$

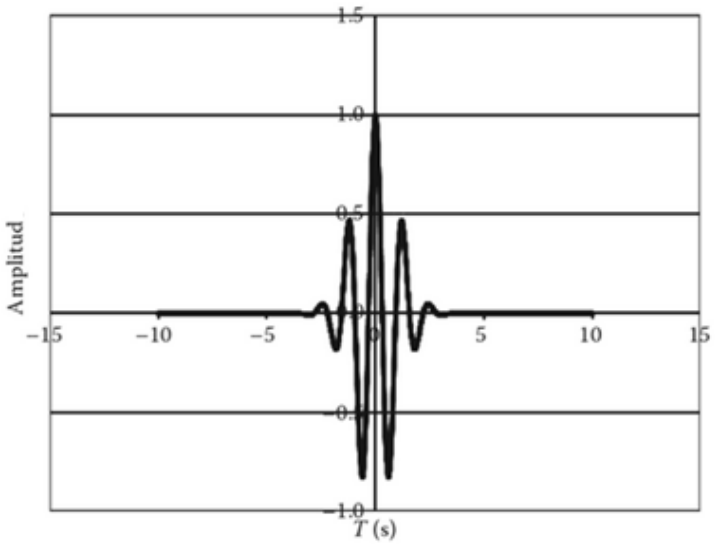


Figura 2.8 Wavelet Morlet.

2.8.3.3 Wavelet de Daubechies

La última gran salva de la revolución de las wavelets se disparó en 1987, cuando Ingrid Daubechies, mientras visitaba el Courant Institute de la Universidad de Nueva York

y, posteriormente, durante su trabajo en los laboratorios AT & T Bell, descubrió una clase completamente nueva de wavelets, que no sólo eran ortogonales (como las de Meyer) sino que también se podían implementar mediante sencillas ideas de filtrado digital, de hecho, mediante cortos filtros digitales.

La familia de la wavelet Daubechies es ortogonal, sin embargo, asimétrica, que introduce una distorsión de fase grande. Esto significa que no se puede utilizar en aplicaciones en las que la información de fase de una señal que se le mantenga. También es una wavelet base de soporte compacto con una anchura de apoyo dada de 2N-1, en donde N es el orden de la base wavelet (Daubechies 1992).

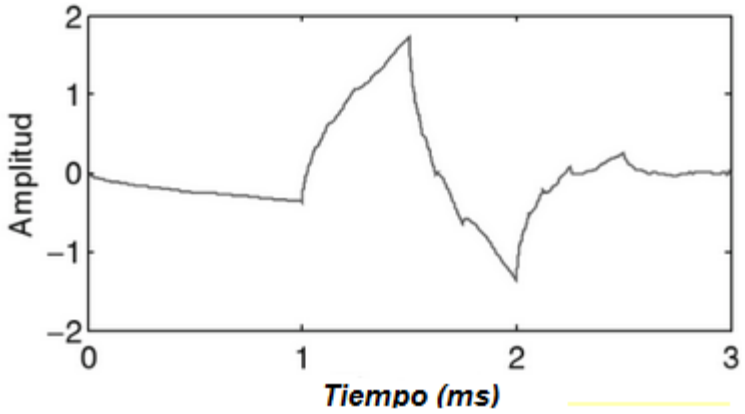


Figura 2.9 Wavelet Daubechies.

2.8.3.4 Otras familias Wavelets

Existen otro tipo de wavelets como las de Coiflet y Symmlet, las cuales son subclases de wavelets que se distinguen por el número de coeficientes y por el número

de niveles de iteración. En la familia de wavelets de Coiflet existen Coiflets con dos momentos de desvanecimiento y otras con tres momentos de desvanecimiento y está relacionada con el número de coeficientes (Martínez Giménez, Peris Manguillot, & Ródenas Escribá, 2004).

La transformada Wavelet es una herramienta matemática que promete no solo tener múltiples aplicaciones en el procesamiento de señales, sino que además está siendo usada en Control de Procesos y detección de anomalías sintomáticas en medicina e ingeniería.

La transformada wavelet resulta especialmente eficiente para extraer información de señales no periódicas o de vida finita. Otra de las ventajas de dicha transformada, frente a otros métodos, es el de poder disponer de una amplia familia de wavelets, lo cual permite tratar señales de diversa índole. La elección de la wavelet dependerá del tipo de señal que se analice. Algunos de los principales problemas que afectan al tratamiento de señales e imágenes digitales, y en los que las wavelets constituyen una potente herramienta para afrontarlos, son la reducción del ruido (en señales de audio y en imágenes), la compresión de señales (de vital importancia tanto en la transmisión de grandes cantidades de datos como en su almacenamiento) o la detección de determinados objetos en imágenes o irregularidades locales en ciertos tipos de señales (electrocardiogramas, vibraciones de motores, etc.) (Areitio Bertolin, 2010). Esta moderna

teoría ha experimentado un gran desarrollo en las dos últimas décadas mostrándose muy eficiente donde otras técnicas, como, por ejemplo, la transformada rápida de Fourier, no resultaban satisfactorias. En esta última se maneja una base de funciones bien localizada en frecuencia, pero no en tiempo, mientras que la mayoría de las wavelets presentan una buena localización en tiempo y en frecuencia, disponiendo incluso de bases de wavelets con soporte compacto.

2.8.4 Representación de la Transformada Wavelet

De manera muy general, la Transformada Wavelet de una función $f(t)$ es la descomposición de $f(t)$ en un conjunto de funciones $\psi_{s,\tau}(t)$, que forman una base y son llamadas las "Wavelets" (Hernández, 2009).

La transformada Wavelet se define como:

$$W_f(s,T) = \int f(t)\, \psi *_{s,T} (t) dt. \tag{2.4}$$

Las Wavelets $\psi_{s,T}(t)$ son generadas a partir de la traslación y cambio de escala de una misma función wavelet $\psi(t)$, llamada la "Wavelet madre", y se define como:

$$\psi_{s,T}(t) = \frac{1}{\sqrt{s}} \psi \left(\frac{t-T}{s} \right) \tag{2.5}$$

Donde s es el factor de escala, y τ es el factor de traslación.

Las wavelets $\psi_{s,T}(t)$ geneeradas de la misma función wavelet madre $\psi(t)$ tienen diferente escala s y ubicación T, pero tienen la misma forma. Se utilizan siempre factores de escala s>0. Las Wavelets son dilatadas cuando la escala s>1, y son contraídas cuando s<1. Así, cambiando el valor de ***s*** se cubren rangos diferentes de frecuencias. Valores grandes del parámetro ***s*** corresponden a frecuencias de menor rango, o una escala grande de $\psi_{s,T}(t)$. Valores pequeños de ***s*** corresponden a frecuencias de menor rango o una escala muy pequeña de $\psi_{s,T}(t)$ (Mitra, 2011).

También pueden mencionarse el soporte compacto, que es la propiedad que la señal prototipo sea de duración finita y la propiedad de simetría, la cual permite que los filtros sean de fase lineal. La ortogonalidad es la propiedad que se logra cuando el producto punto de dos vectores es igual a cero y es importante en los estudios encontrar este tipo de características para que los análisis sean estables.

2.8.5 Wavelets ortonormales y discretas

Cuando la función $f(t)$ es continua y las wavelets son continuas con factor de escala y traslación discretas, la Transformada Wavelet resulta en una serie de coeficientes wavelets, y es llamada la descomposición en Series Wavelet (UNICEN, 2006).

La función $f(t)$ puede ser reconstruida desde los coeficientes wavelets decretos $W_f(s,T)$, de la siguiente manera:

$$f(t) = A \sum_s \sum_T W_f(s,T)\, \psi_{s,T}(t) \tag{2.6}$$

donde A es una constante que no depende de $f(t)$.

A estas funciones wavelets continuas con factores de escala y traslación de las wavelets discretas pueden ser expresados como:

$$s = s_0^i \quad \text{y } T = kT_0 s_0^i \tag{2.7}$$

Donde el exponente i y la constante k son enteros, y s_0>1 es un paso fijo de dilatación.

El factor de traslación *T* depende del paso de dilatación *s, Ec. (2.7). Entonces, a partir de la* Ec. (2.7) y con la Ec. (2.5), las correspondientes wavelets discretas quedan expresadas como:

$$\psi_{i,k}(t) = s_0^{\frac{-1}{2}} \psi\left(s_0^{-i}\left(t - kT_0 s_0^i\right)\right) = s_0^{\frac{-1}{2}} \psi\left(s_0^{-i} t - kT_0 s_0^i\right) \tag{2.8}$$

Através de la Ec. (2.4), la Transformada Wavelet de una función continua es realizada a frecuencias y tiempos discretos que corresponden a muestreos con distintas traslaciones (tiempo) y distintas dilataciones (o cambios de escala).

2.9 Tipos de transformadas Wavelet

Existen tres tipos de transformada Wavelet: continua (CWT), semidiscreta (SWT) y discreta (DWT). La diferencia entre ellas principalmente en la forma en que los parámetros de desplazamiento y escala son discretizados. A continuación, se describen brevemente estos tres tipos.

2.9.1 La transformada continua (cwt)

La transformada Wavelet continua permite el análisis de una señal en un segmento localizado en esta y consiste en expresar una señal continua como una expansión de términos o coeficientes del producto interno entre la señal y una Función Wavelet Madre $\psi(t)$ (S. Taubman & W. Marcellin, 2002).

Una Wavelet Madre es una función localizada, perteneciente al espacio $L^2(R)$, que contiene todas las funciones con energía finita y funciones de cuadrado integrable definidas

$$f \in L^2 \Rightarrow \int |f(t)|^2 \, dt = E < \infty \tag{2.9}$$

De esta manera se cuenta con una única ventana modulada y a partir de esta se genera una completa familia de funciones elementales mediante dilataciones o contracciones y traslaciones en el tiempo $\psi_{u,s}(t)$, denominados átomos wavelet o wavelet hijas que cumplen con todas las condiciones de la forma:

$$\psi_{u,s}(t) = \frac{1}{\sqrt{s}}\,\psi\left(\frac{t-u}{s}\right) \tag{2.10}$$

La Wavelet Madre debe cumplir con la condición de admisibilidad:

$$C_\psi = \int_0^\infty \frac{\left|\hat{\psi}(\omega)\right|^2}{\omega}\,d\omega < \infty \tag{2.11}$$

Lo que la función quiere decir que la función $\psi(t)$ este bien localizada en el tiempo, es decir, que la función oscile alrededor de un eje y su promedio sea cero, matemáticamente $\int_{-\infty}^{\infty}\psi(t)\,dt = 0$, y que la transformada de Fourier $\hat{\psi}(\omega)$ sea un filtro continuo pasa banda, con rápido decremento hacia el infinito y hacia $\omega = 0$.

La transformada Wavelet de una función $f(t)$ a una escala s y una posición u, es calculada por la correlación de $f(t)$ con una $\psi_{u,s}(t)$ de la forma:

$$CWTf(u,s) = \langle f, \psi_{u,s}\rangle = \int_{-\infty}^{\infty} f(t)\psi_{u,s}(t)dt \tag{2.12}$$

$$CWTf(u,s) = \int_{-\infty}^{\infty} f(t)\frac{1}{\sqrt{s}}\,\psi\left(\frac{t-u}{s}\right)dt \tag{2.13}$$

Para escalas pequeñas $(s < 1)$, con la CWT se obtiene información localizada en el dominio del tiempo de $f(t)$ y para escalas $(s < 1)$ la información de $\hat{f}(\omega)$ se presenta localizada en el dominio de la frecuencia.

La transformada wavelet maneja un plano de tiempo-escala, pero también puede ser tiempo-frecuencia, para esto se reúne al Teorema de Parseval y de esta manera es posible definir la transformada Wavelet en el dominio de la frecuencia

$$CWTf(u,s) = \int_{-\infty}^{\infty} \hat{f}(\omega)\sqrt{s}\,\overline{\psi^*}(s\omega)e^{j\omega u}d\omega \tag{2.14}$$

Para poder introducir el término de escala y frecuencia, es necesario ante todo definir una constante (c), que permite realizar un cambio de variable de una escala s a una frecuencia ω:

$$s \longrightarrow \omega = \frac{c}{s} \tag{2.15}$$

Con este cambio de variable es posible observar que la CWT localiza de forma simultánea la señal $\hat{f}(\omega)$ en el dominio de la frecuencia (Torres Maya, 2005).

De igual manera, es posible realizar una Transformada Wavelet inversa, que permita reconstruir la señal, a partir de la CWT (que preserva la energía de la señal) y las $\psi_{u,s}(t)$

$$f(t) = C_\psi \int_0^{\infty} \int_{-\infty}^{\infty} CWTf(u,s)\psi_{u,s}(t)\frac{duds}{s^2} \tag{2.16}$$

2.9.2 Transformada Wavelet semidiscreta

En la práctica, es más conveniente considerar la WT en algunos valores discretos de a y b. Por ejemplo, la escala diáctica corresponde a la definición de los parámetros a=2^j, b=$2^j k$, con (j, k) ϵ Z^2 denominándose transformaa Wavelet semidiscreta (SWT).

La transformada será reversible si se cumple:

$$A\|f\|^2 \leq \sum_{a,b}|\langle f, \psi(\tau, s)\rangle|^2 \leq B\|f\|^2 \quad (2.17)$$

Donde A y B son dos constantes positivas y $f(t)$ sigue siendo una función continua.

2.9.3 Transformada wavelet discreta

La transformada wavelet discreta es muy usada en compresión de imágenes, procesamiento y análisis. Dada un conjunto de funciones básicas ortonormales, se calcula la transformada wavelet discreta, justo como lo haríamos con cualquier otra transformada unitaria, obteniendo una función wavelet básica que sea adecuada. Coma la expansión en series wavelet de la sección anterior delinea una función de una variable continua en una secuencia de coeficientes. Si la función se expande a una secuencia de números, como muestras de una función continua $f(x)$, los coeficientes resultantes son llamados wavelet discreta. Por lo que veremos tres técnicas para el desarrollo de la transformada wavelet discreta: (1) Teoría de bancos de filtros, (2) Multiresolución o análisis en tiempo-escala y (3) Codificación de sub-banda. Para casos más simples, las

series de expansión definidas anteriormente se vuelve el par de transformadas de la DWT.

$$W_{\varphi}(j_0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \varphi_{j_0}, k(x) \tag{2.18}$$

$$W_{\varphi}(j_0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \varphi_{j}, k(x) \tag{2.19}$$

Para j $\geq j_0$ y

$$f(x) = \frac{1}{\sqrt{M}} \sum_k W_{\varphi}(j_0, k) \varphi_{j0,\ k}(x) + \frac{1}{\sqrt{M}} \sum_{j=j0}^{\infty} W_{\psi}(j, k) \psi_{j,\ k}(x) \tag{2.20}$$

Aquí para $f(x) = \varphi_{j0,\ k}(x)$ y $\psi_{j,\ k}(x)$ son funciones de la variable discreta $x = 0, 1, 2, \ldots, M-1$, $j = 0, 1, 2 \ldots, 2^j - 1$.

2.9.4 Transformada Wavelet entera

En aplicaciones como procesamiento digital de imágenes, los datos de entrada son a menudo números enteros. Eso explica que una transformada wavelet entera evita operaciones de punto flotante, y si las entradas se ven afectadas por ruido, este ruido no

puede tener un valor arbitrario real, por lo que su distribución no puede ser Gaussiana. Las principales aplicaciones de DWT son la compresión de señales y eliminación de ruido, pero el principal defecto que tiene la DWT es que los coeficientes de Wavelets son generalmente números en punto flotante y si se introduce alguna cantidad de ruido por pequeña que sea no se podrá reconstruir la señal original de manera perfecta, debido a un error de cuantización que se introduce en el proceso. Con el fin de solucionar el problema, desarrollaron una transformada no lineal de Wavelet, la cual realiza un mapeo de datos enteros a los coeficientes de Wavelets (Torres Maya, 2005).

La IWT o transformada wavelet entera tiene un enfoque más eficiente para compresión sin pérdidas. Los coeficientes en esa transformación son representados por los números de precisión finita que permite una codificación sin pérdidas. Esta wavelet transforma mapas enteros a enteros. En caso de DWT, si la entrada se compone de números entero (como en el caso de las imágenes), la salida resultante ya no consiste en números enteros. Así la reconstrucción perfecta de la imagen original se vuelve difícil. Sin embargo, con la introducción de Wavelet transforma ese mapa entero a enteros. La sub-banda de LL en el caso de IWT parece ser una copia estrecha con menor escala de la imagen original, mientras que en el caso de DWT la sub-banda LL resultante se distorsiona ligeramente.

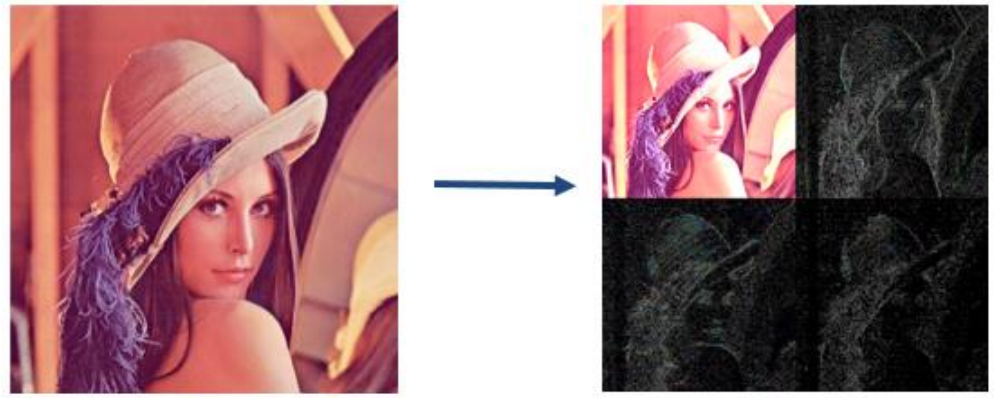
La IWT es una modificación básica de algunas transformaciones lineales, en la cual cada salida de los filtros es redondeada al entero más cercano.

2.10 La transformada wavelet discreta aplicada a una imagen digital.

La DWT aplicada a imágenes proporciona una matriz de coeficientes, conocidos como coeficientes wavelet. Si a una imagen le aplicamos la DWT obtenemos cuatro tipos de coeficientes: aproximaciones, detalles horizontales, detalles verticales y detalles diagonales. La aproximación contiene la mayor parte de energía de la imagen, es decir, la información más importante, mientras que los detalles tienen valores próximos a cero.

La transformada wavelet discreta se describe como un árbol dinámico estructurado por sub bandas y la idea básica consiste en tomar una señal original y separarla en dos frecuencias altas y bajas. La parte de las altas frecuencias en una imagen representa los bordes y se les denomina sub bandas de detalle; la parte de las bajas frecuencias se conoce como sub bandas de información.

Para una transformación bidimensional, la sub banda pasa baja $W_{\varphi}(j_0, m, m)$ o componente DC es más comúnmente identificada como la banda LL; de manera similar $W^{D}\varphi(j_0, m, m)$ representa el contenido de alta frecuencia en direcciones vertical y horizontal y es identificado como HH, por otra parte $W^{H}\varphi(j_0, m, m)$ representa el contenido de baja frecuencia en dirección en dirección vertical y contenido de baja frecuencia en dirección horizontal (S. Taubman & W. Marcellin, 2002).



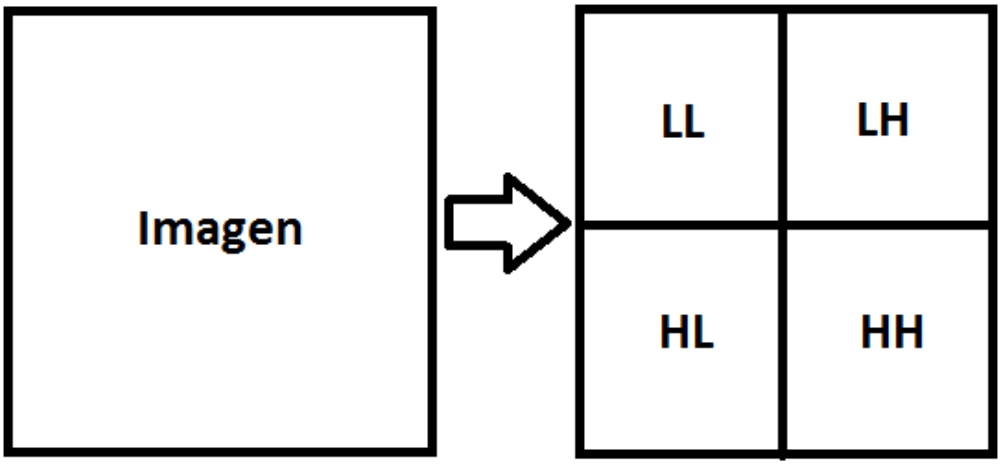


Figura 2.10 DWT en una imagen digital

Cuando la DWT se aplica a una imagen da lugar a cuatro bandas de frecuencias denominadas LL, HL, LH y HH. En la banda HL se encuentra el resultado de aplicar el filtro paso alto a las filas, y paso bajo a las columnas, mientras que en la LH tenemos el caso contrario. La banda HH es el resultante de aplicar el filtro paso alto por filas y columnas, mientras que por último, la banda LL se obtiene a partir del filtro paso bajo

tanto por filas como por columnas. En la figura 2.10 puede verse un ejemplo de la imagen Lena transformada.

2.11 Estegoanálisis

El estegoanálisis es la ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distintas tapaderas, así como la posibilidad de localizar la información útil dentro de la misma (existencia y tamaño) (Ashok Ambardar, 2003). El estegoanálisis tiene el objetivo principal de detectar la presencia de mensajes ocultos en algún medio digital. Se puede definir al estegoanálisis como el arte de descubrir y hacer a los mensajes ocultos inútiles para una comunicación efectiva. Para ocultar información en algún medio digital es necesario manipular alguna de sus propiedades, lo cual degrada al archivo original de alguna forma, estas degradaciones se pueden considerar como una firma del método de esteganografía que se usó para ocultar la información, por medio de estas firmas se puede saber si un archivo digital contiene algún tipo de información oculta, y así derrotar al esquema de esteganografía.

Todas las técnicas de esteganografía en imágenes digitales pueden ser representadas por la ecuación 2.21 (Ashok Ambardar, 2003).

$$C = p + t \tag{2.21}$$

Tomado en cuenta el umbral de la perceptibilidad de la visión humana en una imagen, t es la cantidad de información en la imagen que puede ser manipulada sin causar una distorsión perceptible. P representa la otra porción de la información, que si es modificada provocaría una distorsión. Finalmente, C es alguna imagen con potencial para ser la cubierta del mensaje secreto. El tamaño de t está disponible tanto para el usuario del sistema esteganográfico como para algún atacante que espera poder destruir la información. Siempre y cuando t se mantenga en las regiones imperceptibles, existe alguna t' que puede ser usada por el atacante en C' = p + t', donde no existe una diferencia perceptible entre C y C', este ataque puede ser para remplazar o remover las regiones que ocupa t. Una variación de este ataque fue presentada en (Kovacevic & Vetterli, 1995), si se agrega información extra al medio digital de tal forma que no se note, existe la posibilidad de que parte de esta información agregada, remueva o sobre escriba a la información oculta en la cubierta. Incrustar la información en áreas más perceptibles de la cubierta, harían a la información más robusta, pero esto también provocaría la aparición de marcas, que advertirían la presencia de un mensaje oculto. Algunas degradaciones o distorsiones ocurren durante el proceso, pero éstas no son fácilmente detectadas por el sistema de visión humana.

Los ataques y el análisis en la información ocultada pueden tomar varias formas: detección, extracción, confusión (falsificando, ocultar mensajes sobre información ya existente), y des habilitación de la información ocultada.

Los estegoanálistas pueden realizar los siguientes ataques:

• ***Ataque sobre el estego-objeto***. Solo los estego-objetos están disponibles para el análisis.

• ***Ataque de cubierta conocida***. El original objeto-cubierta y el estego-objeto ambos están disponibles.

• ***Ataque de mensaje conocido***. En un cierto punto, el mensaje oculto puede llegar a ser conocido por el atacante. Analizando el estego-objeto por patrones que corresponden a mensajes ocultos, puede ser un beneficio para futuros ataques contra esos sistemas. Aún con el mensaje, esto puede ser muy difícil y puede incluso ser considerado equivalente al ataque sobre el estego-objeto.

• ***Ataque de selección del estego***. Las herramientas esteganográficas (algoritmos) y el estego-objeto son conocidos.

• ***Ataque de selección del mensaje***. El esteganoanálista genera un estego-objeto de alguna herramienta esteganográfica o de un algoritmo a partir de un mensaje seleccionado. El objetivo de este ataque es determinar los patrones correspondientes en el estego-objeto que pueden señalar el uso de herramientas esteganográficas o algoritmos específicos.

• ***Ataque del estego conocido***. El algoritmo esteganográfico (herramienta) es conocido y tanto el original y estego-objeto están disponibles.

Capitulo III – Algoritmos propuestos

3.1 Introducción

Como se vio en el capítulo anterior, las técnicas de inserción de información en imágenes digitales están divididas en dos categorías: las técnicas en el dominio espacial y las técnicas en el dominio de la transformada. En el presente capítulo se describen los Algoritmos esteganográficos propuestos, el primer algoritmo implementa la segmentación compleja de mapas de bit BPCS por sus siglas en inglés de (Bit Plane Complexity Segmentation), en el dominio espacial, dicho método se conforma de una serie de pasos como es la obtención de la complejidad y la segmentación de los planos de bits con los cuales se obtienen los bloques sustituibles de la imagen contenedor por el mensaje secreto. El segundo Implementa al BPCS en el dominio de la transformada Wavelet.

3.2 Esteganografía de segmentación de la complejidad de los planos de bits (BPCS) en el dominio espacial

El método Bit Plane Complexity Segmentation (BPCS) es un método moderno, se apoya en el hecho de que el sistema visual humano es sensible a los patrones, pero incapaz de identificar ruido blanco aleatorio. Por tanto, si se desea implementar un algoritmo BPCS, la imagen tendrá que dividirse en bloques de 8x8, y se calcula la complejidad de los mismos, la complejidad es una medida que se adquiere comparando la variación de valor en binario entre pixeles vecinos de forma horizontal y vertical. Cualquier zona con complejidad por encima de un cierto umbral puede ser sustituida por

datos insertados. Más adelante se describirá a detalle el proceso de la obtención de la complejidad. Esta técnica funciona con colores reales de 24 bits o con imágenes en escala de grises de 8 bits. No funciona con imágenes con paletas de colores, debido que los cambios pequeños en el valor de un pixel pueden originar drásticas consecuencias en el color del pixel en la imagen.

La esteganografía BPCS aborda el límite de inserción enfocándose a disfrazar los artefactos visuales que se producen por el proceso esteganográfico, según algunos estudios optométricos han demostrado que el sistema visual humano es muy bueno para distinguir anomalías en áreas homogéneas, pero es menos apto para distinguirlas en áreas visualmente complejas.

Cuando la imagen se descompone en planos de bits la complejidad de cada región puede medirse. Las áreas de baja complejidad son homogéneas o formas simples que aparecen como áreas uniformes con pocos cambios entre uno y cero. Las áreas complejas de la imagen aparecerán con forma parecida a regiones de ruido con muchos cambios entre uno y cero. Esas regiones aparentemente aleatorias en cada plano de bits pueden ser reemplazadas por la información a insertar la cual es idealmente parecida al ruido (Hernández Chamorro, 2010).

El método BPCS se basa en la simple idea de que los planos de bits superiores también podrían utilizarse para incrustar la información siempre que se ocultan en las regiones “complejas”. Este método necesita de una medida de complejidad que pueda

ser aplicada a cada región de los planos de bits, dicha medida es variable, por lo cual varios autores han propuesto medidas de complejidad, por ejemplo, Kawaguchi describió a la complejidad de cada subdivisión de los planos de bits como el número de las transiciones de uno a cero y cero a uno, ambos de manera horizontal y verticalmente (Kawaguchi & Eason, 1998). El hecho de medir la complejidad es para tener un parámetro que nos indique el grado de información significativa que hay en cada bloque.

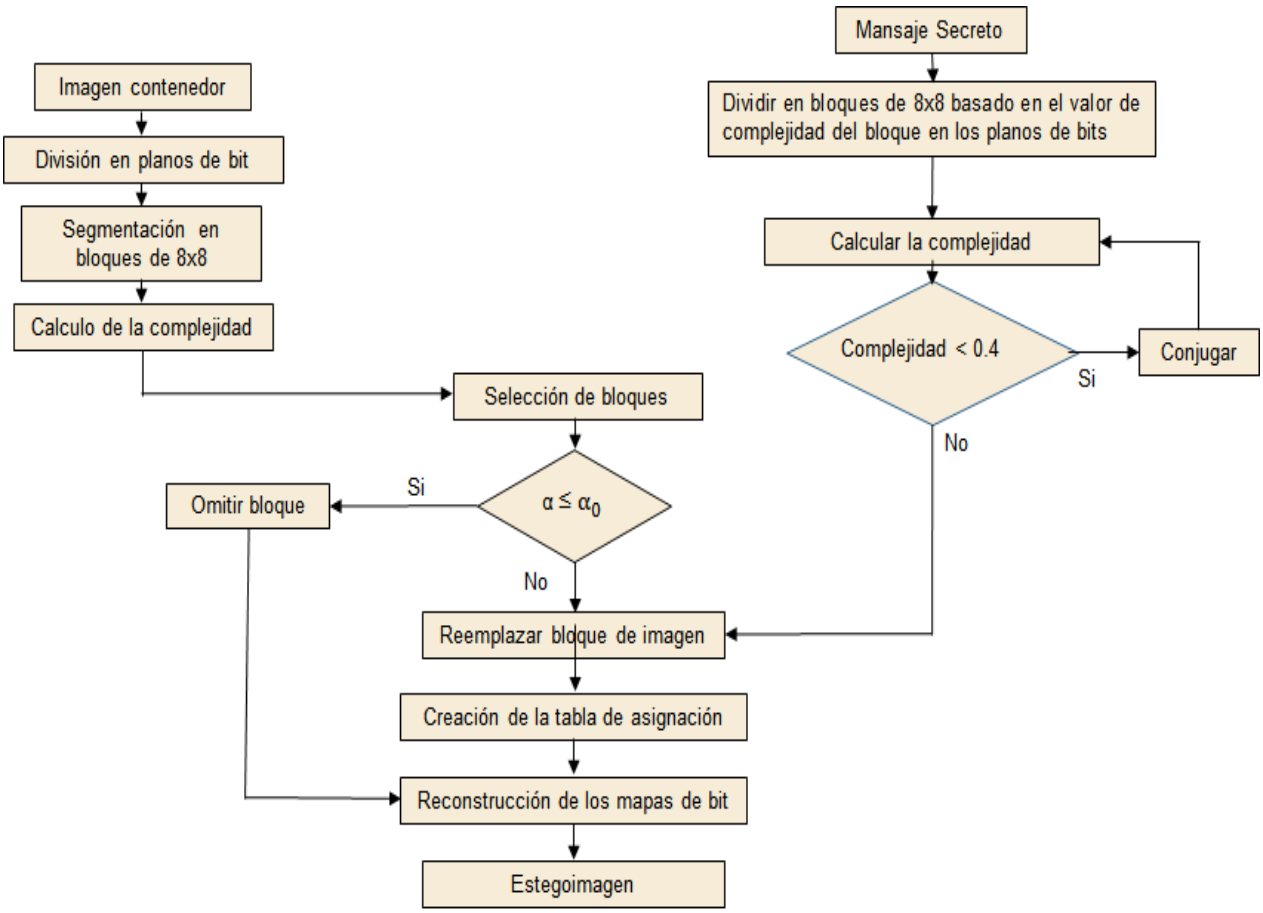


Figura 3.1 Proceso esteganográfico basado en el Algoritmo BPCS usando imagen a escala de grises como portador e imágenes o texto como mensaje

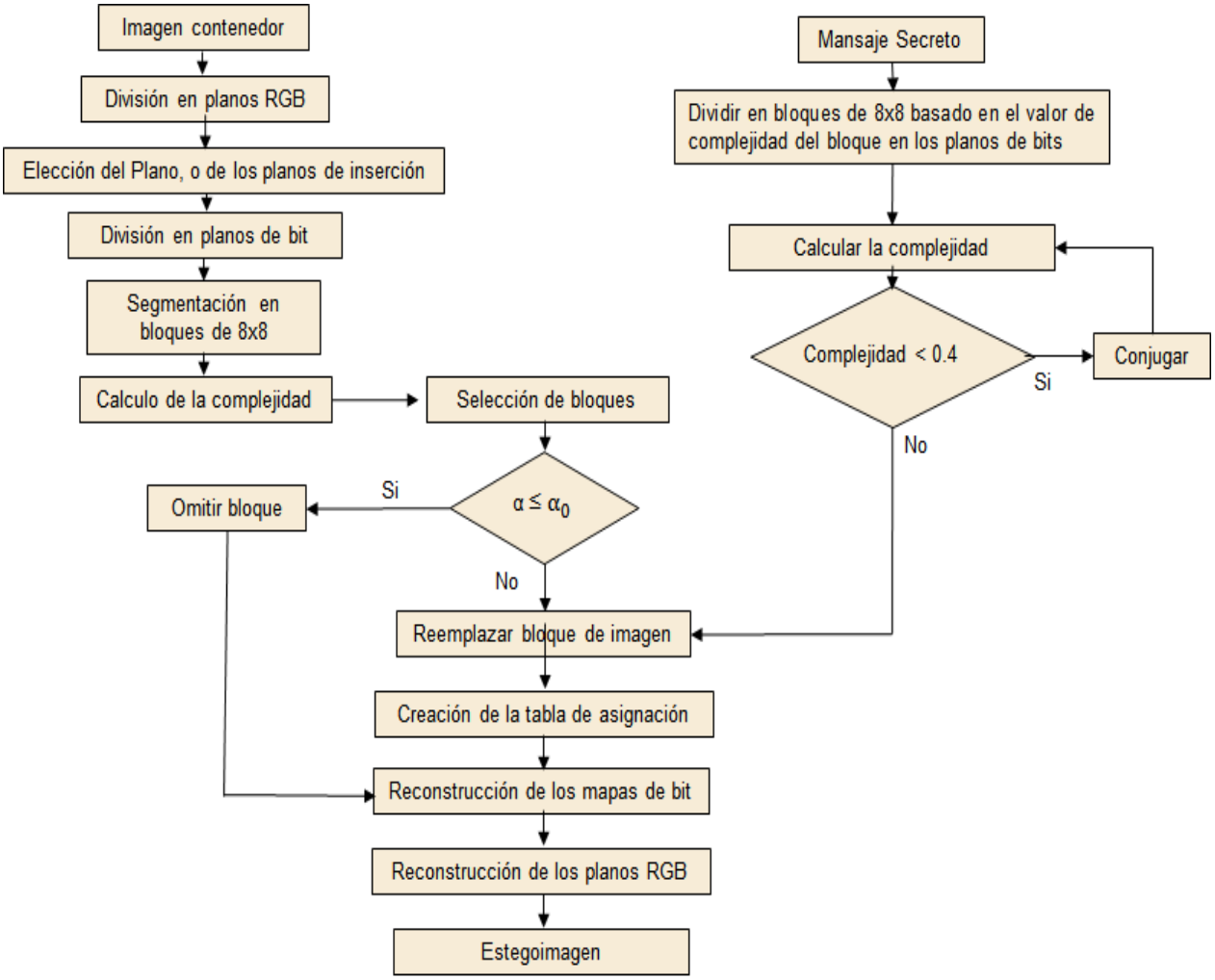


Figura 3.2 Proceso esteganográfico basado en el Algoritmo BPCS usando imagen a color como portador e imágenes o texto como mensaje.

3.2.1 Descripción del proceso de inserción del algoritmo BPCS en el dominio espacial

A continuación, se describen los pasos mostrados en las figuras 3.1 y 3.2 en los cuales se utilizan imágenes digitales en escala de grises y a color como medio contenedor

o portadora de mensaje, el mensaje puede ser texto o una imagen digital en escala de grises.

3.3 Descomposición de una imagen en mapas de bits

Un plano de bits de una señal discreta digital (imagen) es un conjunto de bits correspondientes a una posición de bit dada en cada uno de los números binarios que representan la señal (Gutierrez, 2015).

La codificación en mapas de bits se basa en el concepto de descomposición de una imagen multinivel (monocromática o en color) en una serie de imágenes binarias, una por cada bit usado en la representación de la intensidad del pixel. Los niveles de gris de una imagen con una escala de grises de m bits se puede representar como un polinomio en base 2:

$$a_{m-1}2^{m-2} + a_{m-2}2^{m-2} + \cdots + a_1 2^1 + a_0 2^0 \quad (3.1)$$

Donde a_i, i=0,..., m-1 cualquiera de los dos es 0 o 1. El plano de bits de orden cero se genera a partir de cada uno de los bits a_0 de todos los pixeles, mientras que el plano de bits de orden m-1 contiene los bits a_{m-1}. Por ejemplo, para el caso de una imagen de 8 bits, el plano de bit más significativo de un pixel es representado por un 1 si la correspondiente intensidad del pixel es igual o mayor que 128. Se puede observar que una imagen binaria puede ser representada en un sólo plano de bit. Una descomposición de un plano de bit para una imagen de 8 bits se representa a continuación en la figura 4.3.

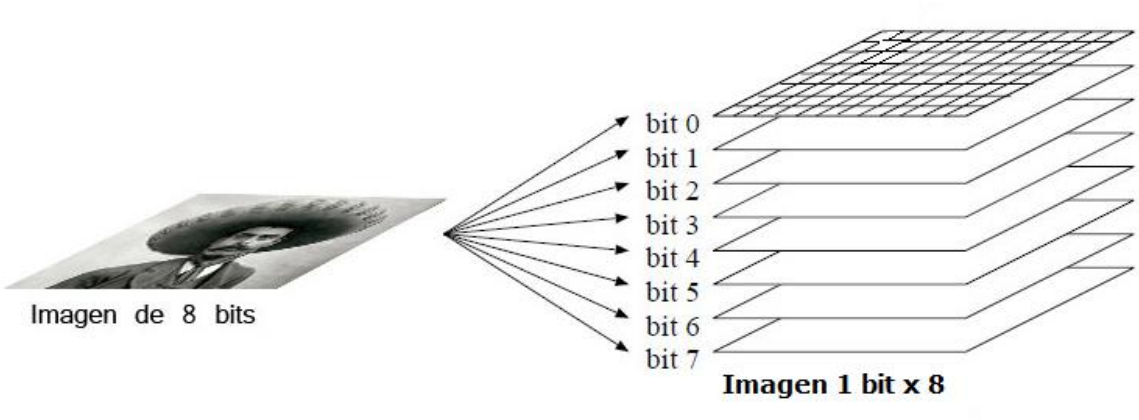


Figura 3.3 Descomposición de mapas de bits.

3.3 Descomposición de una imagen digital a color en planos RGB

Las imágenes representadas en el modelo de color RGB consisten en tres componentes de imágenes, una para cada color primario. El número de bits que se utiliza para representar cada pixel en el espacio RGB es llamado profundidad de pixel.

Considerando una imagen RGB en el que cada imagen roja, verde y azul es una imagen de 8 bits. Bajo estas condiciones cada pixel de color RGB se dice que tiene 24 bits de profundidad (3 planos imagen por el número de bits por plano). El número total de colores de una imagen RGB de 24 bits es $(2^8)^3$=16, 777, 216 (Martínez, 2016).

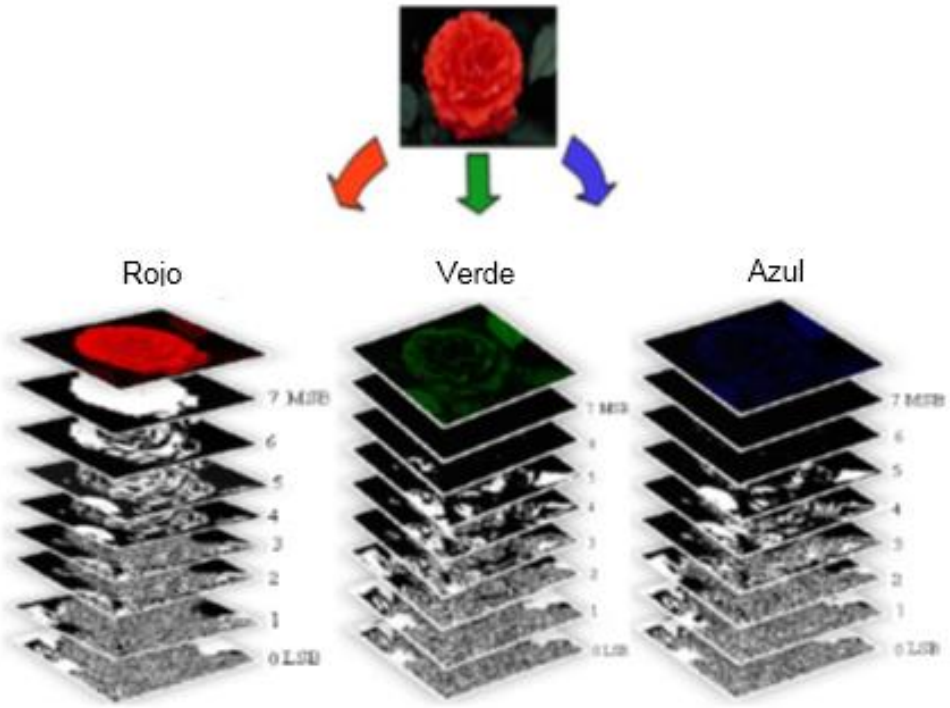


Figura 3.4 Planos RGB de una imagen a color (N S & R C , 2011).

Una vez cargada la imagen contenedora, el proceso de separación de planos utilizando Matlab 2011ª, se realizó de la siguiente manera:

ImagenContenedor = imread('lena.bmp');

>>Im_R = ImagenContenedor(:,:,1);
>>Im_G = ImagenContenedor (:,:,2);
>>Im_B = ImagenContenedor (:,:,3);

En una imagen a color RGB se obtienen 24 planos de bit (8 planos para R, 8 planos para G, 8 planos para B), como se muestra en la figura 3.4.

3.4 División en bloques 8 x 8

La técnica BPCS divide los planos de bits en regiones, típicamente de tamaño 8x8. Por ejemplo: Considerando que la imagen portadora es de tamaño n x n. La segmentación se realizó tomando en cuenta la forma en que leemos, es decir nos posicionamos en un renglón y cuando este termina saltamos al siguiente.

En términos de matrices quedaría de la siguiente manera:

Iniciamos en la fila (1, 8), columna (1, 8) lo que formaría el primer bloque, a continuación, damos saltos de 8 en 8 en la columna, es decir la siguiente seria la posición fila (1, 8) columna (9, 16) hasta llegar a la posición fila (1, 8) columna (n-7, n). Al llegar a esta posición incrementamos en 8 en la fila, la siguiente seria fila (9, 16) hasta fila (n-7, n).

$$\begin{bmatrix} \boldsymbol{fila}\ (\mathbf{1},\mathbf{8}), \boldsymbol{columna}\ (\mathbf{1},\mathbf{8}) & \dots & \boldsymbol{fila}\ (\mathbf{1},\mathbf{8})\ \boldsymbol{columna}\ (\boldsymbol{n}-\mathbf{7},\boldsymbol{n}) \\ \vdots & \ddots & \vdots \\ \boldsymbol{fila}\ (\boldsymbol{n}-\mathbf{7},\boldsymbol{n}), \boldsymbol{columna}\ (\mathbf{1},\mathbf{8}) & \dots & \boldsymbol{fila}\ (\boldsymbol{n}-\mathbf{7},\boldsymbol{n}), \boldsymbol{columna}\ (\boldsymbol{n}-\mathbf{7},\boldsymbol{n}) \end{bmatrix}$$

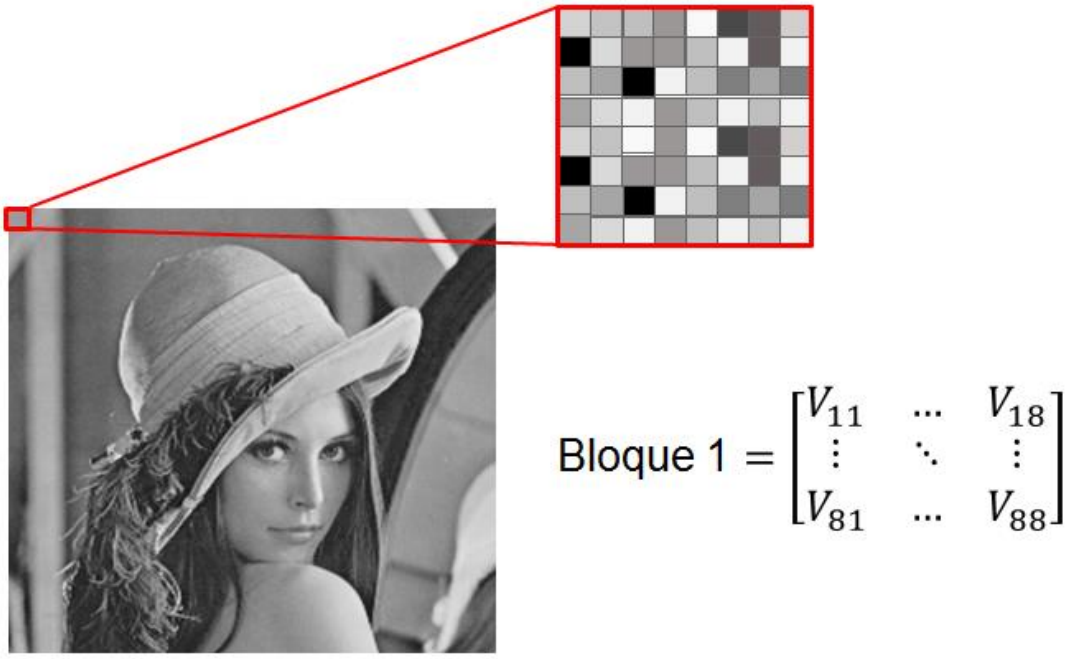


Figura 3.5 Segmentación en bloques. El plano de bit es dividido den bloques de 8x8 del cual se guardará su posición en coordenadas, en un arreglo llamado Bloque n, donde n es el número de bloque.

3.5 Conversión de Código Binario Puro (PBC) a Código Gris Canónico (CGC).

Debido que el funcionamiento para la incrustación del algoritmo esteganográfico BPCS se ejecuta después de que la imagen contenedor ha sido transformada de PBC a CGC, es importante explicar dichos códigos. El Código binario puro es la representación de un número decimal codificado en binario, se compone de un arreglo de conjunto de bits, donde cada conjunto de bits corresponde a un digito decimal. El código Gray es otro tipo de código basado en un sistema binario, pero de una construcción muy distinta a la de los demás códigos. Su principal característica es que 2 números sucesivos, cualesquiera, solo varían en 1 bit.

La conversión de PBC a CGC se consigue mediante un proceso que consiste en:

El bit más significativo (MSB) en Gray se toma directamente de la MSB en binario. El resto de los bits de Gray proviene de una operación XOR entre el precedente bit binario (b (i-1)) y la corriente binaria de bits (b (i)). En el caso mostrado en el ejemplo anterior:

La operación XOR produce un 1 si los bits son diferentes, y produce un 0 si los bits son iguales. Así, un binario puro '11101' se convierte en un '10011' en código Gray.

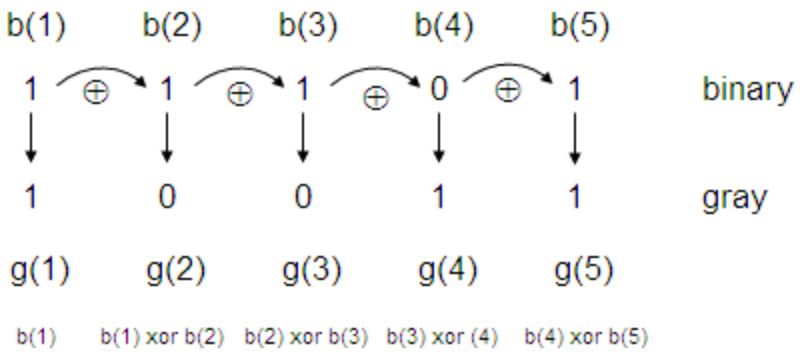


Figura 3.6 Conversión PBC a CGC.

La ventaja de CGC es que en el paso entre dos dígitos sucesivos sólo se produce el cambio de un simple bit. La figura 3.7 representa el código Gray con sus respectivos valores en decimal y en binario:

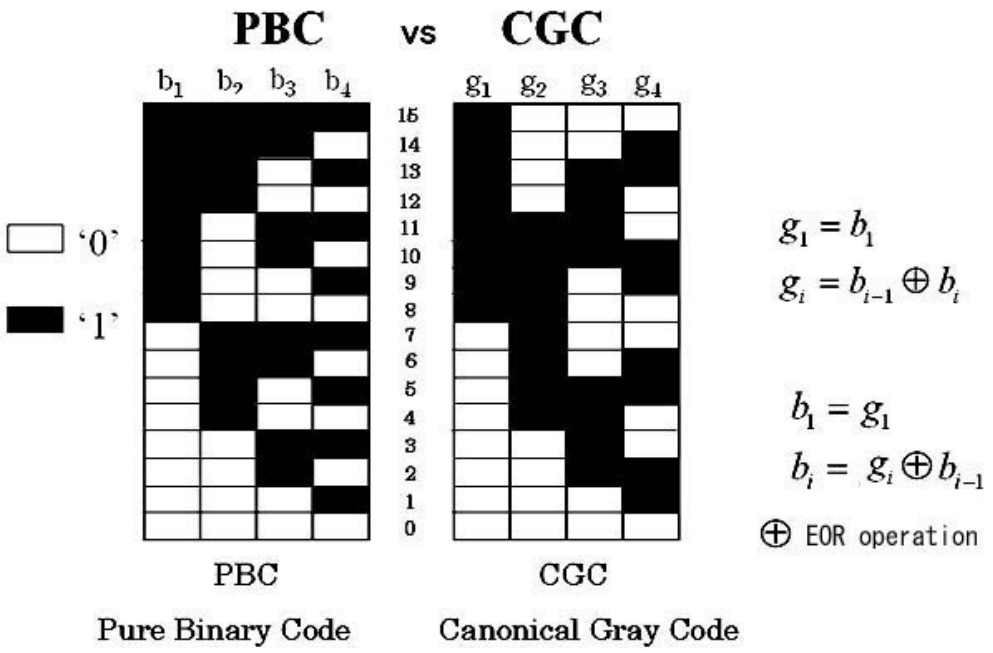


Figura 3.7 PBC vs CGC en imagen binaria. Imagen (Eiji Kawaguchi, 2015).

El código CGC es mejor que el PBC en la producción de la estego-imagen, pues tiene un “mejor aspecto”. La razón es debido a que los planos de la imagen común están representados por codificación en binario puro (PBC), provee una región mucho mayor para esconderse. Pero PBC sufre de “acantilado de Hamming”, en el que un pequeño cambio en el color afecta a muchos bits de valor de color. Ejemplo: considérese una imagen en escala de grises, la cual tiene valores de gris diferentes (127 y 128). Estos dos niveles de gris afectan con un pequeño cambio en gris con la imagen, pero la representación de 127 como 01111111 y 10000000 128 tiene una gran diferencia en la representación de pixeles. Tanto los pixeles parecen idénticos a ojo humano, pero son muy diferentes en representación de bits. Esto se llama “Hamming Cliff” (SHRIKANT S & SANJAY L, 2010).

Las siguientes imágenes ilustran la diferencia de los puntos de vista de una sola imagen bmp. El lado izquierdo es de PBC, y el derecho de CGC.

Figura 3.8 Comparación de una imagen a color entre PBC y CGC (Eiji Kawaguchi, 2015).

3.6 Complejidad

El nivel de complejidad para realizar la inserción de datos secretos en las regiones ruidosas. Como se mencionó anteriormente en la esteganografía BPCS, Kawaguchi propuso que la complejidad α de cada subdivisión de un plano de bit es definida como el número de las transiciones de uno a cero y cero a uno, ambos horizontalmente y verticalmente. Para cualquier cuadrado de los pixeles de n x n, la complejidad máxima está definida en la ecuación 3.2:

$$\alpha_{max} = 2n(n-1) \tag{3.2}$$

Donde α_{max} es la complejidad máxima, y n es el número de píxeles por renglón o columna en un bloque de n x n.

La complejidad de los planos de bits está definida como el número de transiciones de uno a cero y cero a uno horizontal y vertical. Así mismo el valor de complejidad mínimo es 0.

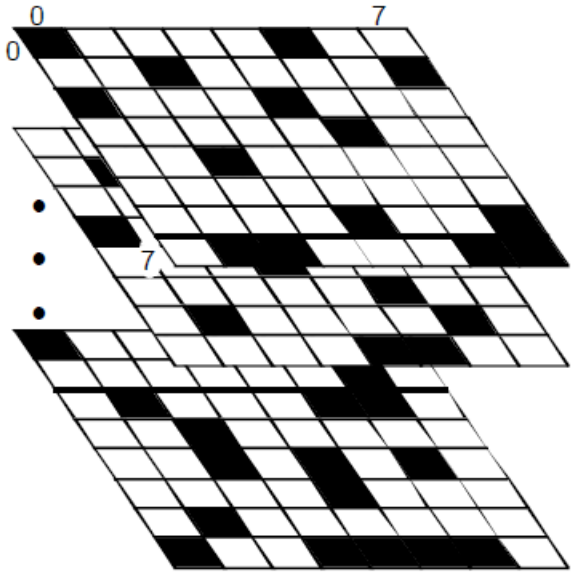
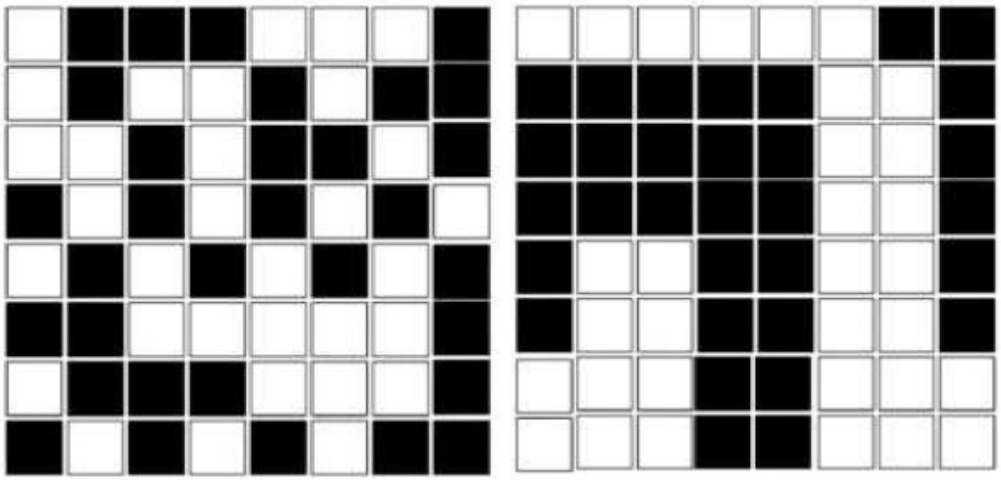


Figura 3.8 Imagen de la posición de pixel (0,0) tiene el valor binario 01001110. En este plano de bits, negro es un 0 y blanco es un 1. Se puede observar al primer plano de bits en la posición (0,0), hay un cero (negro), en el segundo plano, hay uno (blanco), y así sucesivamente hasta el último plano de bits (Rituraj Rusia, Munendra Kumar , & R. K, 2014).



a) Bloque complejo b) Bloque informativo

Figura 3.9 a) Bloque ruidoso de complejidad 69 b) bloque informativo de complejidad 29. Rituraj Rusia. et al (2014).

En la figura 3.9 el blanco representa un uno y el negro un cero. Ambos cuadrados tienen el mismo número de unos y de ceros, pero muy diferente complejidad. Esto demuestra que uno contiene una información más visual que el otro. El cuadrado a), se considera un bloque complejo porque tiene visualmente muy poca información, por lo tanto, puede ser sustituido por datos secretos y puede tener un pequeño efecto en la calidad de la imagen. Si el cuadro visualmente más informativo b) fuera sustituido, causaría la distorsión en los bordes y en las formas definidas.

Utilizando una medida de complejidad, se pueden determinar las regiones ruidosas de cada plano de bit, el parámetro que determina que bloques son complejos es llamado umbral α_0 un valor típico está definido en la siguiente ecuación 3.3:

$$\alpha_0 = 0.3\alpha_{max} \tag{3.3}$$

Algunas otras implementaciones BPCS adoptan una medida similar de complejidad que es descrita de la siguiente manera:

$$\alpha = \frac{k}{\alpha_{max}} \tag{3.4}$$

Donde k es la longitud total del borde en blanco y en negro de la imagen (es decir, el número de cambios de blanco a negro a lo largo de las filas y las columnas) y α_{max} es el número máximo posible de cambios de blanco a negro, para bloques de 8x8 es de 112. El valor sobre el rango $0 \leq \alpha \leq 1$. Comúnmente la ecuación 3.4 define de manera global, es decir, α se calcula sobre el área de toda la imagen dándonos la complejidad global de una imagen binaria. Sin embargo, también se puede usar α para una complejidad en una imagen local (por ejemplo, en un bloque de área de 8x8).

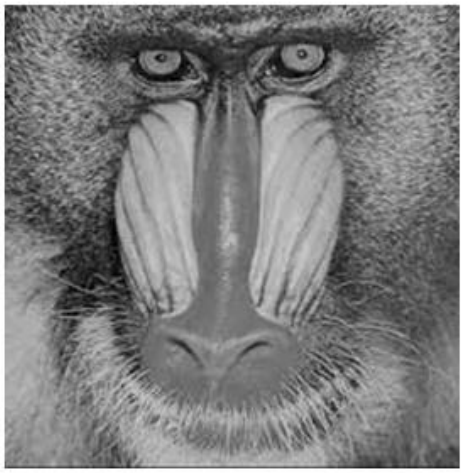
Kawaguchi abordó este tema con el problema de umbral de imagen y propuso tres tipos de medidas de complejidad.

El problema fundamental en la obtención del umbral es como seleccionarlo, los métodos más sencillos y más usados se basan en imágenes que tienen histogramas de

intensidad bimodal, en la cual se puede escoger un punto en el valle del histograma, no es conveniente suponer que todas las imágenes tienen tal historial bimodal (Hioki Hirohisa, 2001).

3.7 Mensaje a insertar

El mensaje insertado puede ser una imagen digital en escala de grises o un archivo de texto, en ambos casos se debe segmentar en bloques de 8 x 8 con el fin de reemplazar a los bloques de la imagen contenedor.



Imagen

Texto

Figura 3.10 Mensaje a insertar

3.8 Conjugación de una imagen binaria

Una imagen binaria consiste de regiones informativas y regiones similares al ruido, los patrones informativos son simples, mientras que las similares al ruido son complejas.

Si los datos secretos son similares al ruido, entonces se incrusta directamente en regiones similares al ruido de la imagen contenedor. Si los datos en secreto son informativos, entonces tiene que someterse a la operación de conjugación con el fin de transformar a patrón complejo.

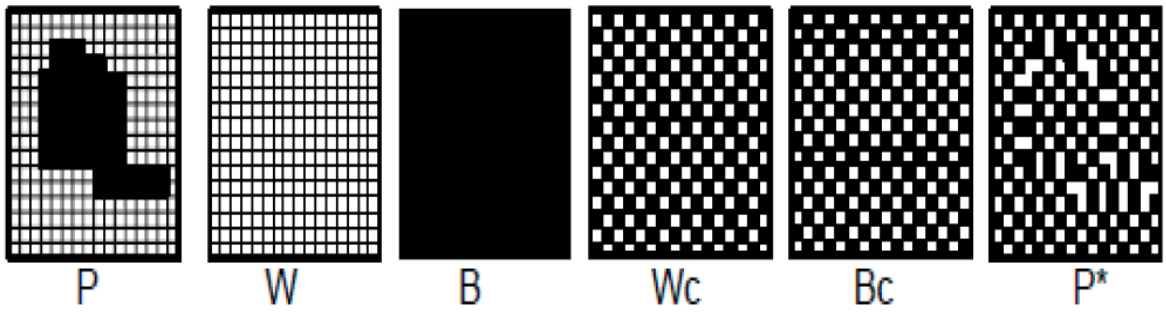


Figura 3.11 Ilustración de la operación Conjugación (SHRIKANT S & SANJAY L, 2010).

Sea P una imagen en blanco y negro de tamaño 2^N x 2^N con negro como el área de primer plano y el blanco como el área de fondo. W y B denotan todo blanco y negro, respectivamente. Introducimos dos patrones de ajedrez Wc y Bc, donde Wc tiene un pixel blanco en la posición superior izquierda, y Bc es su complemento, es decir, el pixel superior izquierdo es de color negro (ver figura 3.11). Consideramos pixeles blancos y negros que tienen un valor de “1” y “0”, respectivamente.

P se interpreta como sigue. Los pixeles en el primer plano tienen el patrón B, mientras que los pixeles en el área de fondo tienen el patrón W. Ahora definimos P* como el conjugado de P que satisface:

La forma área en el primer plano es el mismo que P.

El área en primer plano tiene el patrón Bc.

El área de fondo tiene el patrón Wc.

Una de la propiedad importante de conjugación es $\propto (P^*)$ =1 -∝(P), es decir, si la complejidad de P es 0.6 es patrón informativo, entonces la complejidad P^* es de 0.4 es patrón complejo. SHRIKANT S et al. (2010).

¿Por que conjugar?

Los bloques del mensaje que no satisfagan el valor de complejidad deben ser conjugados para no alterar la estegoimagen (imagen con mensaje oculto).

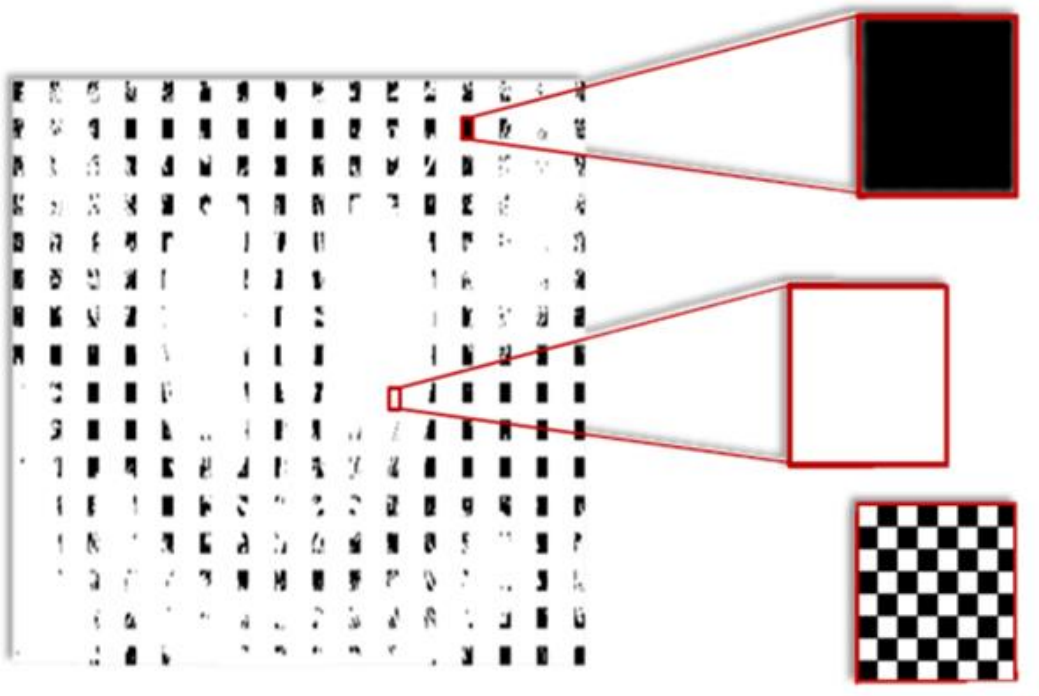


Figura 3.12 Segmentación de imagen mensaje.

3.9 Incrustación del mensaje

En el proceso de inserción se verifica la complejidad de cualquier bloque del mensaje secreto. Si la complejidad es mayor o igual al umbral de complejidad 0 α, los datos secretos se insertan tal cual, en los bloques ruidosos de la imagen, pero si la complejidad es menor que el umbral, se realiza la operación de conjugación de los datos antes de la inserción, la figura 3.13 muestra este proceso. Ahora toda la información insertada tiene una complejidad mayor o igual que el umbral, y toda la información original de la imagen tiene una complejidad menor que el umbral.

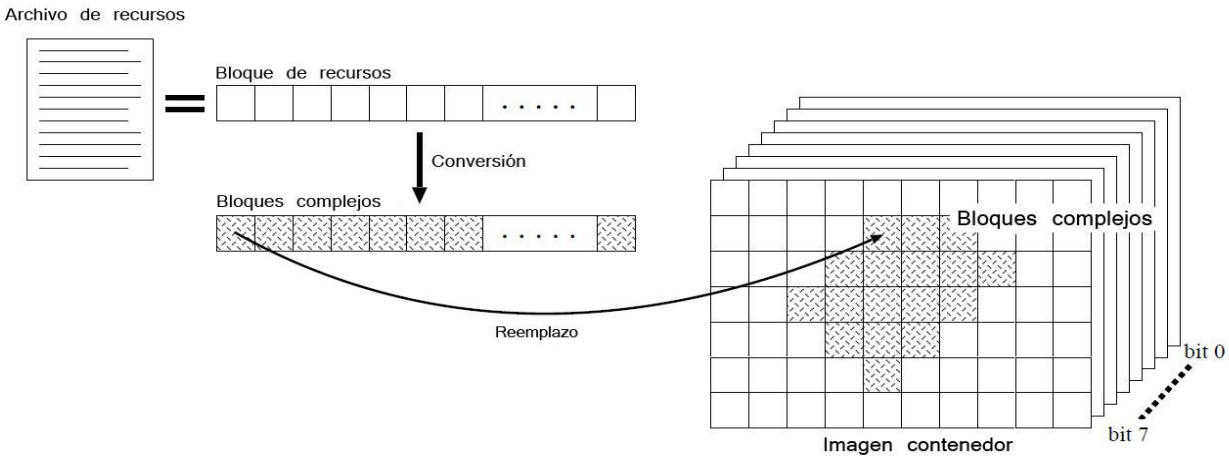


Figura 3.13 Proceso de inserción.

El anterior proceso puede usarse para recuperar una imagen binaria que ha pasado por una operación de conjugación. El único problema sigue siendo el conocer cuáles regiones han pasado por la operación de conjugación. El problema se resuelve mediante un mapa de conjugación el cual lleva un registro de las regiones que han

pasado por la operación de conjugación, las únicas regiones para las cuales la conjugación tiene una complejidad $1-\alpha_0$. Si vemos al mapa de conjugación como una cadena de bits, está se puede generar mediante la adición de un “1” a la cadena, cada vez que se conjuga una región de información se está insertando a fin de que su complejidad sea mayor o igual al umbral.

Un problema con la inserción de mapa de conjugación dentro de la imagen viene de la posibilidad de que una región del mapa de conjugación puede en sí misma requerir de una conjugación. Una solución simple es almacenar el mapa de conjugación sin conjugación en alguna parte de la imagen de bajo nivel predefinida, sin importar la complejidad. Debido a que se sabe que el mapa de conjugación existe ahí, este puede ser fácilmente extraído.

Otra alternativa es reservar un bit de cada región de tal forma que los datos del mapa de conjugación sirvan como un bit indicador. Por ejemplo, si la región pasa por un proceso de conjugación durante la inserción, el bit indicado cambiará a uno, de otra forma permanecerá en cero. El mapa de conjugación puede entonces ser agregado al final de los datos insertados, pero la inserción de las regiones del mapa de conjugación no agrega más información al mapa de conjugación.

3.9.1 Incrustación de texto

Para incrustar texto en una imagen es importante considerar que el código ASCII extendido utiliza 8 bits para representar los caracteres, aunque inicialmente empleaba un bit adicional (bit de paridad) que se usaba para detectar errores en la transmisión (Wikipedia, 2016). Por ejemplo, datos de texto en ASCII extendido de 8 bits, siempre tienen un cero en el bit más significante y los otros bits toman un conjunto limitado de valores. Aunque ciertamente hay otras maneras de evitar la regularidad de la información, tal vez la mejor solución es simplemente realizar una compresión y/o cifrado. Al realizar tanto la compresión como el cifrado de los datos de información antes de la inserción, es mejor realizar la compresión primero, ya que los datos cifrados típicamente producen muy poca compresión, al extraer la información de la imagen se requiere de las operaciones inversas, es decir, en orden contrario (Torres Maya, 2005).

Cuando los datos secretos son reemplazados directamente en la cubierta sin hacer algún procesamiento, como es el cifrado o compresión, la información secreta es convertida en matrices binarias mostradas en la figura 3.14. El mensaje secreto a ocultar corresponde a un archivo de texto en formato .TXT, del cual se toman palabras de 8 Bytes y se representa en su correspondiente código ASCII, cada uno de los valores ASCII es convertido en forma binaria de 8 bits, es decir si al codificar la letra “e” su representación en código ASCII es de “101” y puede representarse en forma binaria como “01100101” , el conjunto de 8 caracteres forman matrices binarias de 64 bits, en la siguiente figura 3.14 se puede visualizar el procedimiento, el cual consiste en tomar bloques de 8 caracteres,

que pueden incluir espacios, tabulaciones y todos aquellos elementos que están incluidos dentro del código ASCII.

Mensaje secreto: (PROCESAMIENTO DIGITAL DE IMÁGENES)

P	R	O	C	E	S	A	M	I	...

8 Bytes

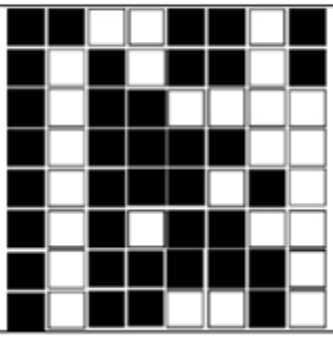
Palabra 8 bits	Código ASCII	Código Binario 1 byte	Imagen Binaria
P	50	00110010	
R	82	01010010	
O	79	01001111	
C	67	01000011	
E	69	01000101	
S	83	01010011	
A	65	01000001	
M	77	01001101	

Figura 3.14 Representación binaria de un bloque secreto.

Existe un problema cuando los datos son insertados directamente en la cubierta debido a que es posible que la información secreta insertada, pensando que los datos son aleatorios por naturaleza, pudiera tener una complejidad menor que $\propto_0$. Cuando se realiza el proceso de extracción del mensaje secreto, la medida de complejidad de una

determinada región podría ser ignorada erróneamente, debido a que ahora el bloque del mensaje secreto tiene una baja complejidad colocándola en la categoría de datos de imagen original que simplemente fue estructurada sin cambio alguno.

3.10 Proceso de extracción del mensaje secreto

Al algoritmo de extracción de la información se le aplica el proceso inverso, es decir, como primer paso se realiza una descomposición en planos de bit de la estego-imagen, estos se dividen en bloques de 8 x 8, después se calcula la complejidad de los planos de bit en cada región. Se lee el mapa de conjugación y se realiza una segunda operación de conjugación sobre el bloque complejo, para obtener su forma original, es decir (P*)* = P. De esta forma se obtiene el mensaje.

El proceso de extracción se representa en los siguientes diagramas:

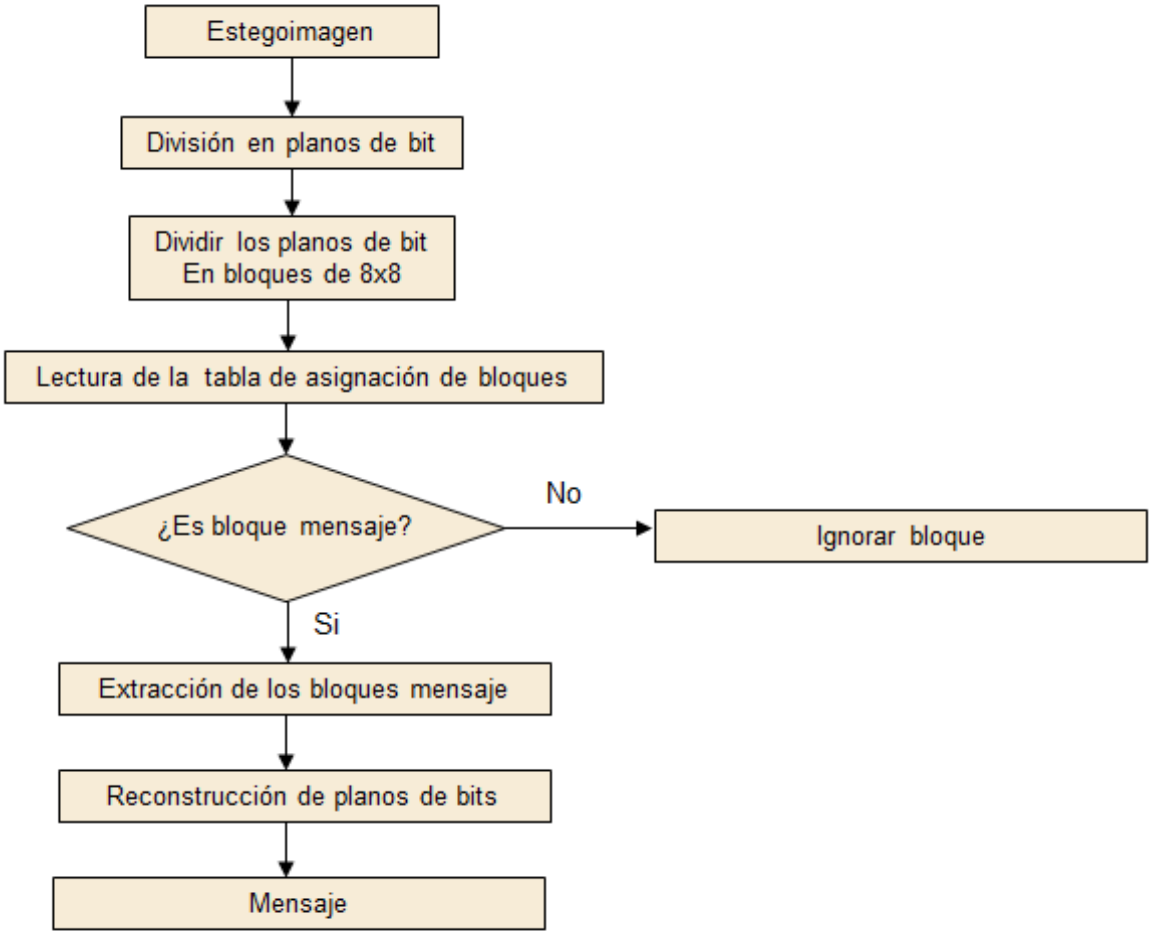


Figura 3.15 Proceso de extracción Algoritmo BPCS en imágenes en escala de grises

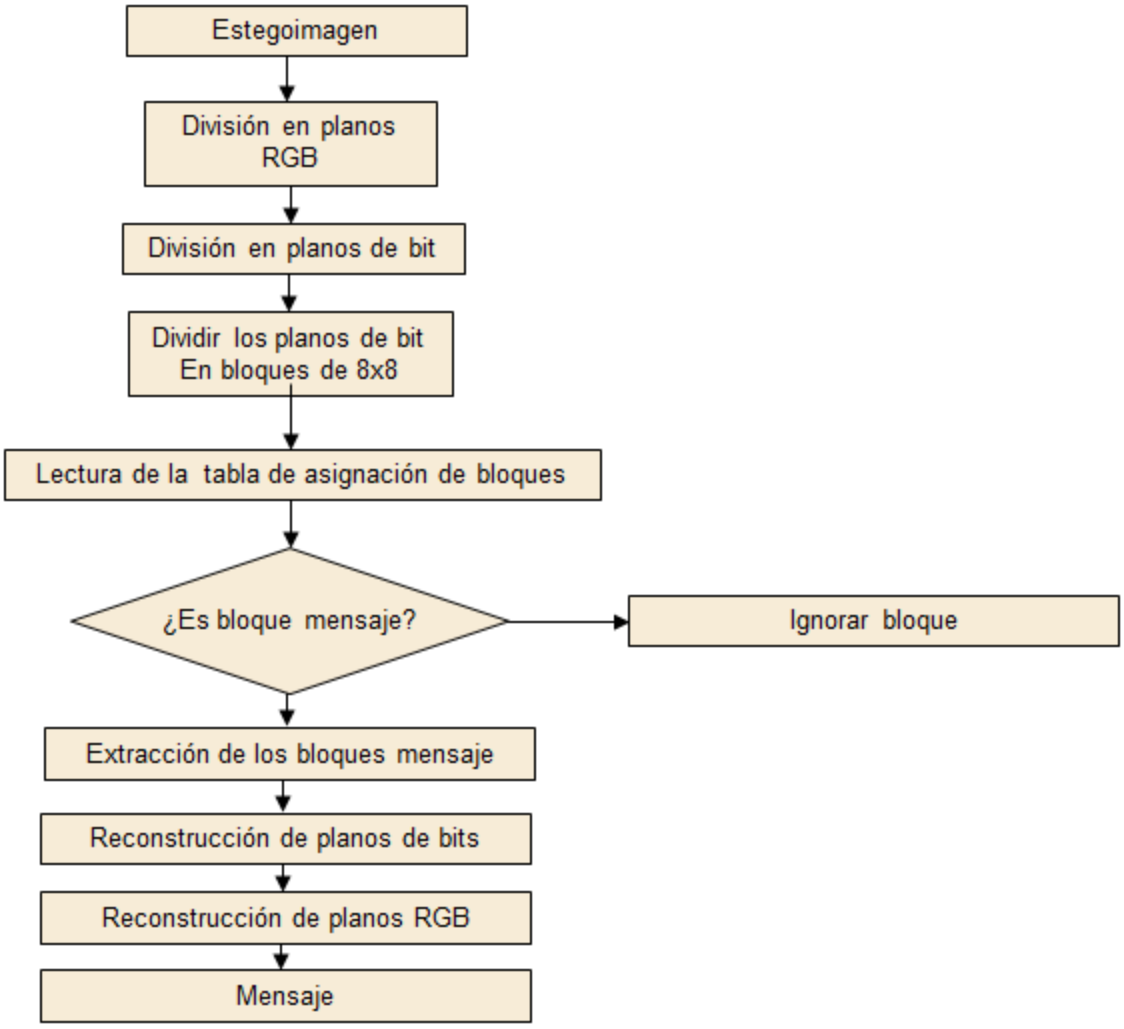


Figura 3.16 Proceso de extracción Algoritmo BPCS en imágenes a color

3.11 Algoritmo BPCS en el dominio de la Transformada

En el capítulo anterior se describieron las familias Wavelet, así como también los tipos de transformaciones. Respecto al análisis realizado a las transformadas (Fourier, Coseno, Wavelet), se concluyó que la Transformada Wavelet se puede implementar

sobre numerosas bases. Las diferentes categorías de wavelets (continuas, ortogonales, etc.) y los varios tipos de funciones wavelets dentro de cada categoría proveen una gran cantidad de opciones para analizar una señal de interés, Esto permite elegir la base de funciones cuya forma se aproxime mejor a las características de la señal que se desea representar o analizar (UNICEN, 2006).

En el presente trabajo se decidió emplear las bases wavelets de Daubechies en la Transformada Wavelet para la implementación del algoritmo BPCS, esto debido a que la Daubechies tienen la propiedad de formar una base ortonormal y poseen soporte compacto. Por esta razón son adecuadas para el análisis de señales con soporte finito (por ejemplo: electrocardiogramas, sismogramas, etc.) y en particular para el análisis y procesamiento de imágenes digitales.

Los nombres de las ondas de la familia Daubechies se escriben dbN, donde N es el orden, y en el db el "apellido" de la onda. La wavelet db1, como se mencionó anteriormente, es el mismo que Haar wavelet. Aquí están las funciones wavelet psi de los siguientes nueve miembros de la familia:

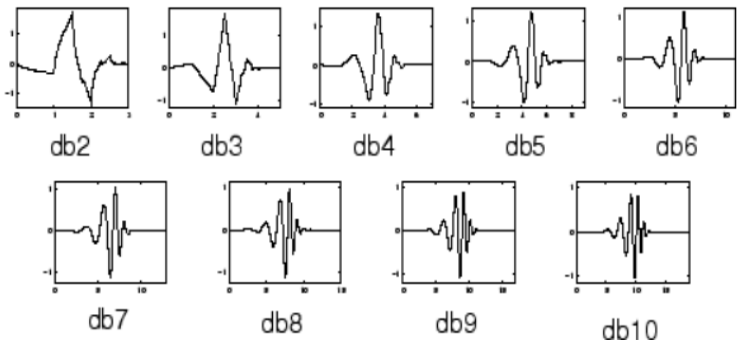


Figura 3.17 Tipos de Daubechies según su orden. (The MathWorks, 2016)

3.11.1 Estenografía mediante la Transformada Wavelet Discreta (DWT)

La selección de la wavelet para el procesamiento de señales e imágenes siempre se ha cuestionado entre los investigadores, de hecho, la investigación de las familias de wavelets para la estenografía es todavía un problema abierto.

El análisis Wavelet permite descomponer la señal en aproximaciones y detalles, a éste proceso se le conoce con el nombre de análisis. Este filtrado nos proporciona el doble de datos de los que son necesarios.

El origen de la DWT se remonta al año 1976 cuando Croiser, Esteban y Galand crearon una técnica para descomponer discretamente señales en el tiempo, en el mismo año Crochiere, Weber y Flanagan realizaron un trabajo similar para la codificación de señales de audio. El nombre que se utilizó para este tipo de análisis fue codificación de sub-bandas. Posteriormente en 1983, Burt definió una técnica muy similar a la anterior que denominó “codificación piramidal” y que actualmente se conoce como “análisis multiresolución”. En 1989, Vetterli y Le Gall mejoran el esquema de codificación de sub-bandas disminuyendo la redundancia existente en el algoritmo piramidal

La transformada discreta wavelet (DWT) es muy similar a la transformada discreta de Fourier (DFT), pero en lugar de usar funciones seno y cosen como esta última, utiliza otro tipo de funciones denominadas de escala y wavelets. Estas funciones reúnen la

doble característica de ortogonalidad (para que la reconstrucción sea igual que la transformación), así como soporte compacto en el espacio (UNICEN, 2006).

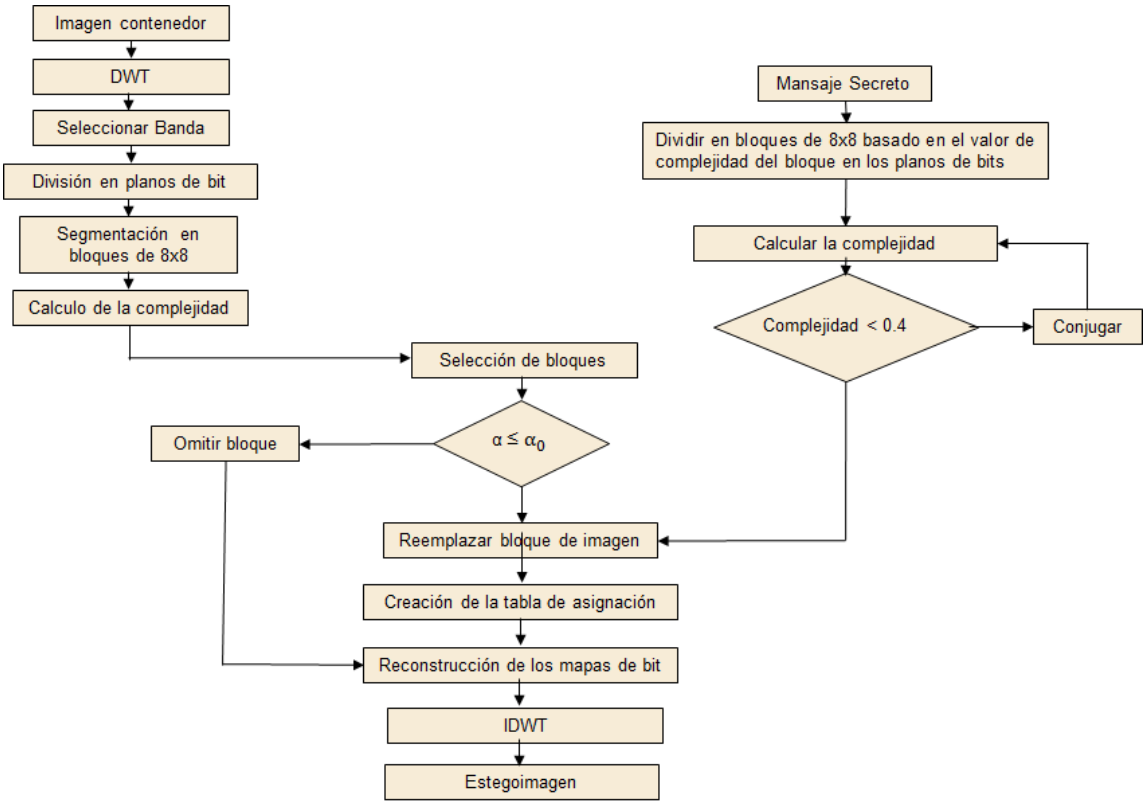


Figura 3.18 Proceso esteganográfico basado en el algoritmo BPCS en el dominio de la transformada.

En la figura anterior podemos observar el proceso esteganografico en el cual se utiliza la transformada wavelet discreta, de la familia Daubechies 2. Al aplicar la transformación wavelet a la imagen contenedor se pasa del dominio espacial al frecuencial, y como su nombre lo dice se obtienen bandas de frecuencia de la imagen contenedor, estas bandas son denominadas LL, HL, LH y HH. En la banda HL se encuentra el resultado de aplicar el filtro paso alto a las filas, y paso bajo a las columnas,

mientras que en la LH tenemos el caso contrario. La banda HH es el resultante de aplicar el filtro paso alto por filas y columnas, mientras que, por último, la banda LL se obtiene a partir del filtro paso bajo tanto por filas como por columnas.

Figura 3.19 Bandas de frecuencia de la transformación wavelet.

Una vez aplicada la transformación wavelet cada una de las 4 bandas puede descomponerse en mapas de bit, por lo que para realizar la inserción del mensaje oculto debe elegirse la banda para la inserción, en realidad una vez que se obtienen las bandas el procedimiento es casi el mismo que el aplicado en el dominio espacial, a excepción de la aplicación de la inversa de la transformada para reconstruir la imagen contenedor por medo de las bandas de frecuencia.

En el caso de usar una imagen contenedor a color el procedimiento se describe en la Figura 3.20. Como se mencionó en el capítulo anterior, una imagen a color puede descomponerse en tres planos (R, G y B), y de cada uno de estos pueden obtenerse las

bandas de frecuencia correspondiente, es decir, (LLR, LLG, LLB), (HLR, HLG, HLB), (LHR, LHG, LHB), (HHR, HHG, HHB).

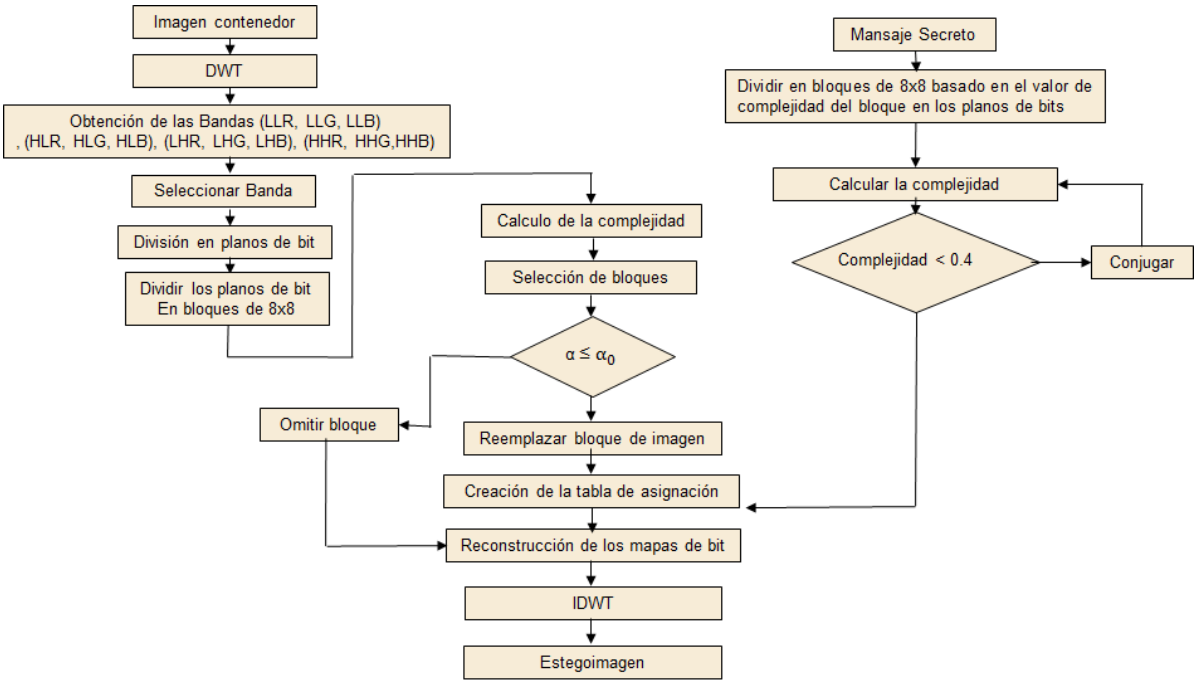


Figura 3.20 Proceso Esteganográfico basado en el algoritmo BPCS en el dominio de la transformada aplicado a imágenes a color.

La extracción del mensaje es similar en el procedimiento que se aplica en el dominio espacial, a excepción de la aplicación de la transformación wavelet a la estegoimagen, después se divide en bloques de 8 x 8 y se lee el mapa de asignación, una vez que se identifican los bloques mensaje se extraen y se reconstruyen formando el mensaje.

El proceso de la extracción es descrito en las Figuras 3.21 y 3.22 que a continuación se presentan.

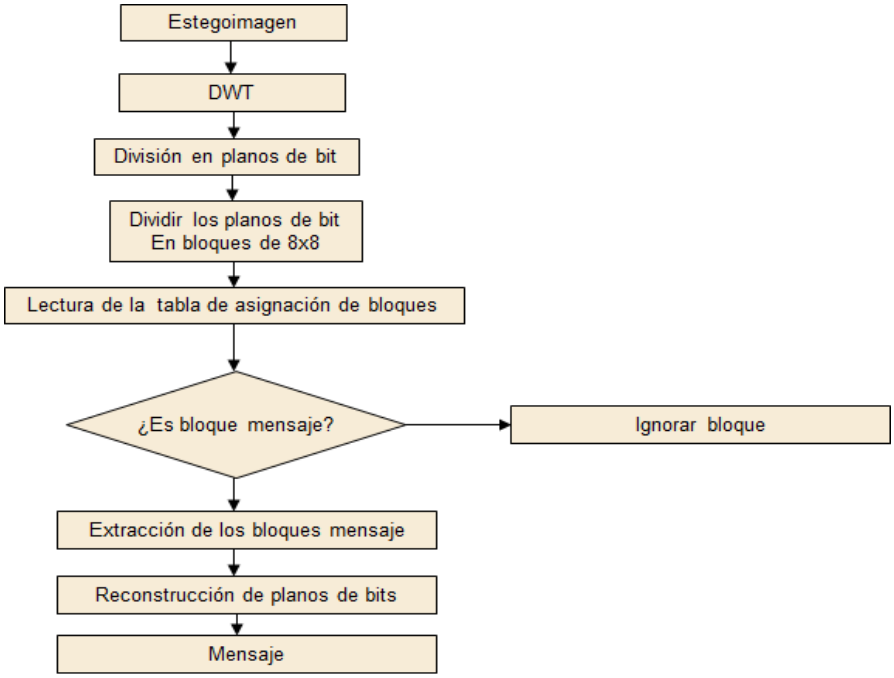


Figura 3.21 Proceso de extracción Algoritmo BPCS en el dominio de la frecuencia aplicado a imágenes en escala de grises

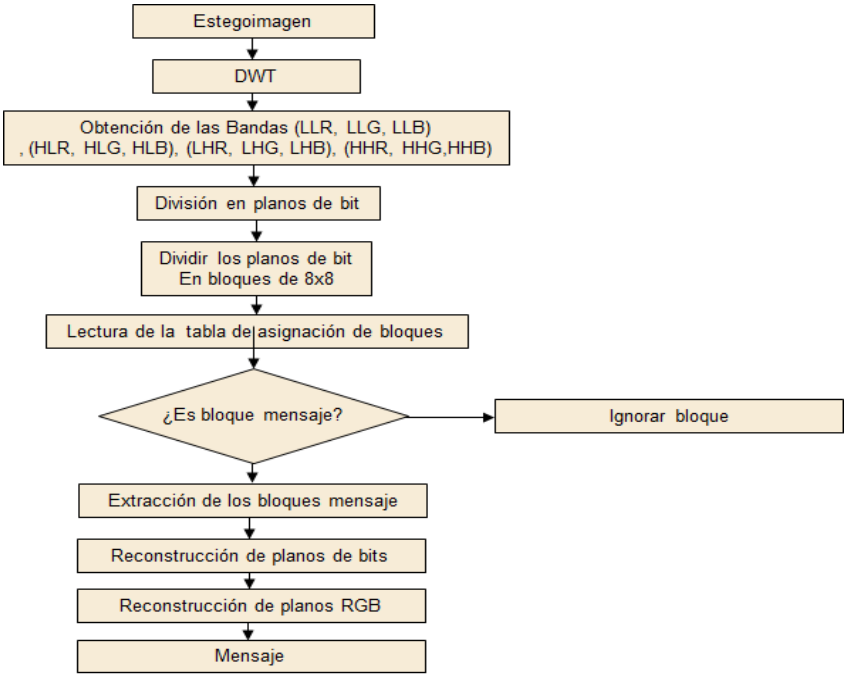


Figura 3.22 Proceso de extracción Algoritmo BPCS en imágenes a color

Capítulo IV – Parámetros de evaluación del sistema Esteganográfico

Con el fin de comparar la calidad de la imagen original con la modificada, y para poder saber el grado de integridad, imperceptibilidad y capacidad de inserción se definirán los parámetros que a continuación se presentan.

Es importante contar con medidas con la cuales se evalué la calidad de la Estegoimagen (imagen con mensaje incrustado) en comparación con la imagen original, y por medio de estas medidas determinar la eficiencia del método utilizado. A estas medidas se les llama comúnmente medidas de similitud ya que en ellas se expresa la similitud entre dos imágenes, o en el campo del procesamiento de imágenes se les conoce como medidas de calidad.

4.1 MSE (Error Cuadrático Medio)

El error cuadrático medio representa la diferencia entre los puntos originales y los nuevos puntos calculados en el proceso de transformación. La escala de transformación indica en qué medida se puede escalar el mapa de bits de dicha imagen que se está digitalizando hasta igualarse con las coordenadas de la imagen real, es decir, a una aproximación entre el valor original y el nuevo valor que se modificó en la imagen, y está representada por la siguiente expresión:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[(|R(i,j) - R'(i,j)|^2 + |G(i,j) - G'(i,j)|^2 + |B(i,j) - B'(i,j)|^2)/3].$$

(4.1)

Donde R(i,j), G(i,j), B(i,j) representan los valores de los planos de la imagen original y R'(i,j), G'(i,j), B'(i,j) representan los valores de los planos de la imagen restaurada o filtrada.

4.2 Relación Pico Señal a Ruido "PSNR"

La Relación Señal a Ruido Máxima o PSNR (del inglés Peak Signal-to-NoiseRatio) es un término utilizado en ingeniería para definir la relación entre la máxima energía posible de una señal y el ruido que afecta a su representación fidedigna. Debido a que muchas señales tienen un gran rango dinámico, el PSNR se expresa generalmente en escala logarítmica, utilizando como unidad el decibel. El uso más habitual del PSNR es como medida cuantitativa de la calidad de la reconstrucción en el ámbito de la compresión de imágenes. (Roncagliolo B, 2016)

Puede calcularse por medio de la siguiente ecuación:

$$PSNR = 10 * log\left[\frac{(255)^2}{MSE}\right] db \qquad (4.2)$$

4.3 Medida de capacidad de ocultación

La capacidad de ocultación de datos indica la cantidad máxima de información que puede ser escondido y recuperado con éxito por el sistema de esteganografía. Debido a que el número de bits ocultos varía dependiendo del tamaño de la imagen portadora, para medir la capacidad oculta, utilizamos bits por pixel (bpp), el cual está dado de la siguiente manera:

$$bpp = \frac{Numero\ de\ bits\ del\ mensaje\ oculto}{Numero\ de\ bits\ de\ la\ imagen\ portador} \quad (4.3)$$

4.4 BER: (Bit Error Rate)

Es una de las medidas más frecuentes en sistemas de transmisión digitales y se define como la relación entre el número de bits errados al ser recibidos por el receptor y el número de bits totales transmitidos en un determinado intervalo de tiempo durante una comunicación. Esta medida también se denomina fracción de errores por bit, el término tasa se refiere a una cantidad que varía con el tiempo y la cual está definida mediante la siguiente ecuación:

$$BEER = \frac{Bits\ erroneos}{Texto\ aculto\ en\ bits\ (bits)} \quad (4.4)$$

Capítulo V - Resultados

5.1 Software de implementación

La implementación se realizó por medio de Matlab 7.12.0, el cual es un entorno de cálculo técnico de altas prestaciones para cálculo numérico y visualización. Integra:

- Análisis numérico
- Cálculo matricial
- Procesamiento de señales
- Gráficos

Se eligió Matlab ya que cuenta con un entorno fácil de usar, donde los problemas y las soluciones son expresados como se escriben matemáticamente, sin la programación tradicional. El nombre *MATLAB* proviene de “MATrix LABoratory” (Laboratorio de Matrices). *MATLAB* es un sistema interactivo cuyo elemento básico de datos es una matriz que no requiere dimensionamiento. Esto permite resolver muchos problemas numéricos en una fracción del tiempo que llevaría hacerlo en lenguajes como *C*, *BASIC* o *FORTRAN*. *MATLAB* ha evolucionado en los últimos años a partir de la colaboración de muchos usuarios. (Laguna, 2016)

5.2 Resultados en el dominio espacial

Imagen	Tamaño	Imagen	Tamaño	Valor de	PSNR	MSE
Lena	512 x 512	Baboon	512 x 512	.35	43.3155 dB	0.7636
Boat	512 x 512	Clown	256 x 256	.35	43.4380 dB	0.7424
Peppers	512 x 512	Lena	128x128	.35	43.3405 dB	0.7592
Clown	512 x 512	Peppers	512 x 512	.45	42.1841 dB	0.9908
Baboon	512 x 512	Lena	256 x 256	.45	42.3848 dB	0.9461
Cameraman	512 x 512	Clown	128x128	.45	41.6908 dB	1.1100
Barbara	512 x 512	walkbridje	512 x 512	.5	39.0900 dB	2.0203
Peppers	512 x 512	Clown	256 x 256	.5	40.8663 dB	1.3421
Cameraman	512 x 512	Barbara	128x128	.5	37.2508 dB	3.0856
goldhill	512 x 512	Boat	128x128	.55	35.7418 dB	4.3676
Lena	512 x 512	Baboon	128x128	.6	___	___

Tabla 1. Parámetros de evaluación BPCS dominio espacial con una imagen en escala de grises como portador y una imagen en escala de grises como mensaje.

Imagen contenedor	Tamaño	Imagen mensaje	Tamaño	Número de mensajes	Valor de Umbral	PSNR	MSE
Lena	512x512	Baboon	512x512	1	.35	52.8861	0.2529
Lena	512x512	Baboon	256x256	2	.35	49.8758	0.5058
Lena	512x512	Boat	128x128	3	.35	48.1369	0.7548
Lena	512x512	Baboon	512x512	1	.45	52.0281	0.3081

Lena	512x512	Baboon	256x256	2	.45	49.0178	0.6163
Lena	512x512	Boat	128x128	3	.45	46.9326	0.9961
Lena	512x512	Baboon	512x512	1	.5	50.5212	0.4359
Lena	512x512	Baboon	256x256	2	.5	47.5109	0.8719
Lena	512x512	Boat	128x128	3	.5	44.7421	1.6494

Tabla 2. Parámetros de evaluación BPCS dominio espacial con una imagen a color como portador y una imagen en escala de grises como mensaje.

Imagen	Imagen Original	Nivel 1
Lena **512 x512** **α= 0.35**	No te salves Mario Benedetti No te quedes inmóvil al borde del camino no congeles el júbilo no quieras con desgana no te salves ahora ni nunca no te salves no te llenes de calma no reserves del mundo sólo un rincón tranquilo no dejes caer los párpados pesados como juicios no te quedes sin labios no te duermas sin sueño no te pienses sin sangre no te juzgues sin tiempo.	N o te salves Mario Benedetti No te quedes inm~Æ || al borde del camino no congeles el j~Æ+bilo no quieras con desgana no te salves ahora ni nunca no te salves no te llenes de calma no reserves del mundo sºlo un rincón +ranquilo no dejes caer los p žíý+, padDs pesados como juicios no te quedes sin labios no te duermas sin su~Æ~Æ no te pienses sin sangre no te juzgues sin tiempo.
PSNR		32.956 dB

Tabla 3. Evaluación de la inserción de texto en el dominio de la transformada.

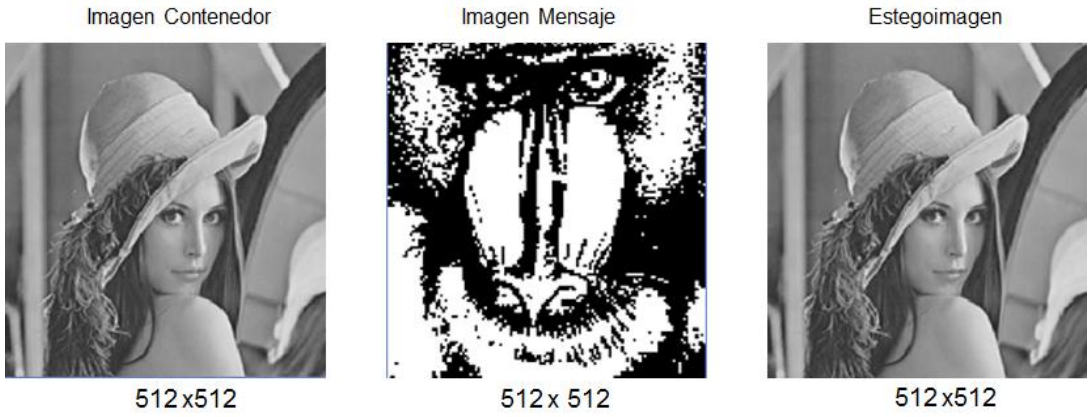


Figura 5.1 Inserción mediante el algoritmo BPCS en imagen en escala de grises como portador y una imagen binaria como mensaje.

Resultados de la inserción BPCS en el dominio espacial aplicado a una imagen en escala de grises, con una complejidad de .3 obteniendo: PSNR de 43.9261 dB y MSE de 2.6125.

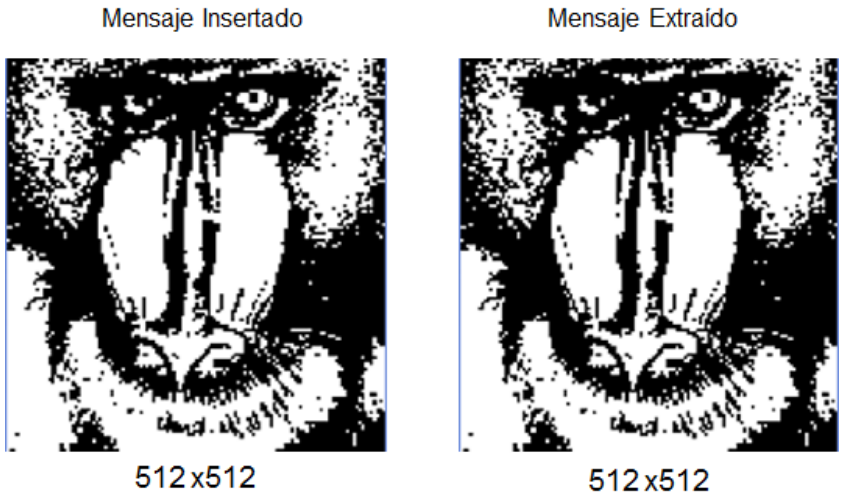


Figura 5.2 Mensaje insertado vs Mensaje extraído. En la comparación de las figuras puede observarse que ambas figuras son idénticas ante la comparación visual.

5.3 Resultados en el dominio Frecuencial

Tamaño de imagen	Tamaño del mensaje	Valor de Umbral	Banda	MSE	PSNR
512 x 512	64x64	0.4	xar	8.7150	38.7281 dB
512 x 512	64x64	0.4	xag	12.8959	37.0263 dB
512 x 512	64x64	0.4	xab	4.1557	41.9444 dB
512 x 512	64x64	0.4	xhr	0.0694	59.7184 dB
512 x 512	64x64	0.4	xhg	0.0669	59.8740 dB
512 x 512	64x64	0.4	xhb	0.0726	59.5242 dB
512 x 512	64x64	0.4	xvr	0.1236	57.2113 dB
512 x 512	64x64	0.4	xvg	0.1460	56.4881 dB
512 x 512	64x64	0.4	xvb	0.1246	57.1747 dB
512 x 512	64x64	0.4	xdr	0.0171	65.8109 dB
512 x 512	64x64	0.4	xdg	0.0157	66.1707 dB
512 x 512	64x64	0.4	xdb	0.0172	65.7699 dB

Tabla 4. Evaluación en imagen en escala de grises aplicando la transformación wavelet, e insertando una imagen de tamaño inferior a la portadora.

Imagen Contenedor	Tamaño	Numero de mensajes	Tamaño	Valor de umbral	PSNR	MSE
Lena	512 x 512	1	128x128	.5	50.52 dB	0.43
Lena	512 x 512	2	128x128	.5	47.51 dB	0.87
Lena	512 x 512	3	128x128	.5	44.76 dB	1.64

Tabla 5. Evaluación en imágenes a color aplicando la transformación wavelet en el primer nivel.

Imagen	Nivel 1			Nivel 2		
	PSNR (dB)	Máxima capacidad (bpp)	Bit Error Rate	PSNR (db)	Maxima Capacidad (bpp)	Bit error Rate
Baboon	42.181	6.253	0.1349	38.953	4.921	0.5973
Lena	39.750	7.954	0.2956	36.594	7.932	0.4221
Clown	48.673	14.531	0.5982	34.592	12.564	0.6214
Barbara	49.876	10.562	0.1994	45.854	9.073	0.4310

Tabla 6. Evaluación en la transformada Resultados de la inserción BPCS en la transformación wavelet en el nivel 1 y nivel 2.

Figura 5.3 Inserción de imagen en imagen mediante BPCS en el dominio de la transformada.

Resultados de la inserción BPCS en el dominio de la transformada a una imagen en escala de grises como portador y una imagen binaria como mensaje, con una complejidad de .35 obteniendo: PSNR de 43.3594 dB y MSE de 0.7559.

Figura 5.4 Mensaje insertado vs Mensaje extraído BPCS DWT

En la comparación de las figuras puede observarse que en la figura de lado derecho (mensaje extraído) aparecen dos artefactos los cuales fueron adheridos por error.

Figura 5.5 Inserción de imagen en imagen mediante BPCS

En la figura se aprecia la imagen contenedora, la estegoimagen y los mensajes insertados con α=0.4, MSE 0.7847 y PSNR 47.9682.

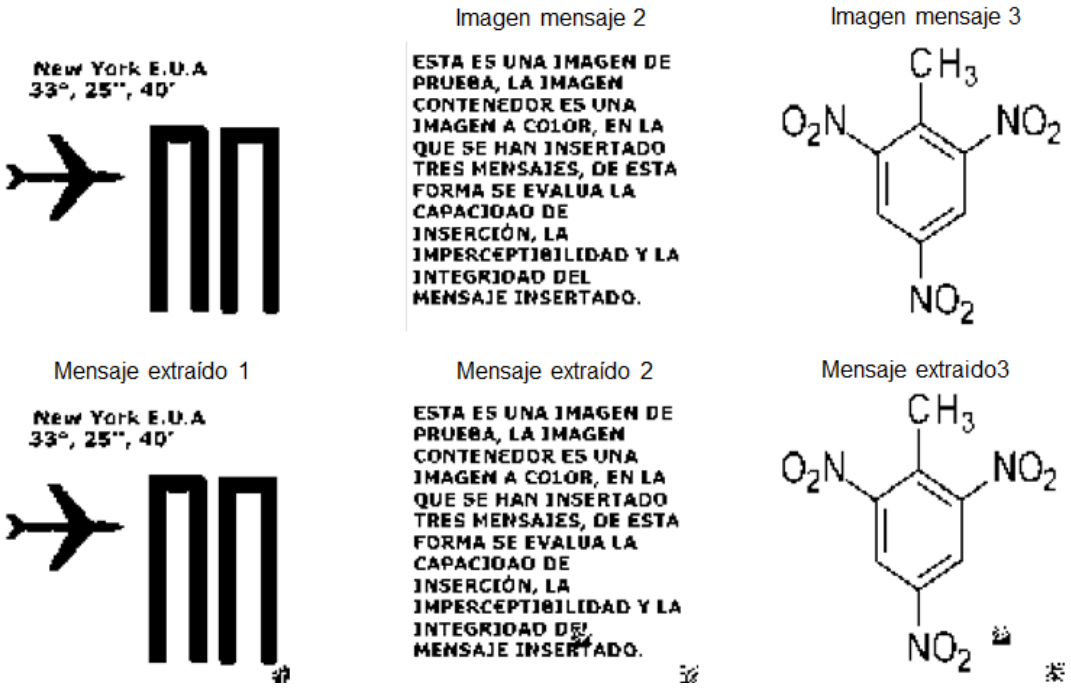


Figura 5.6 Extracción de imagen en imagen mediante BPCS.

En la figura se puede apreciar el mensaje, aun cuando se han adherido algunos artefactos

Figura 5.7. Inserción de imagen en imagen mediante BPCS en el dominio de la transformada DWT.

Resultados de la inserción BPCS en el dominio de la transformada a una imagen portador a color y una imagen mensaje en escala de grises, con una complejidad de .35 obteniendo: PSNR de 44.3594 dB y MSE de 0.7339

a) Imagen con el PSNR bajo (29.9821 dB) b) Imagen con el PSNR alto (45.003 dB)

Figura 5.8 Inserción mediante DWT en imagen a color.

Resultados de la inserción BPCS en la transformación wavelet en el nivel 1 aplicado a una imagen a color, donde puede apreciarse en el recuadro blanco de la figura a), que se aprecian a simple vista artefactos debido a que se eligió la banda de aproximación LL con una complejidad de .5 y el resultado es un PSNR de 29.9821 dB, a diferencia de la figura b), en la cual no se aprecian artefactos y se obtuvo un PSNR de 45.003 dB.

Imagen	Texto Original	Extracción - Nivel 1	Extracción - Nivel 2
Lena 512 x512 α= 0.35	Existen antecedentes a cerca de la esteganografía que resultan fascinantes, los cuales son mencionados por Heródoto de Halicarnaso, en su obra “Los Nueve Libros de la Historia”, en el texto se narra como un famoso tirano griego llamado Histieo rapo a su más fiel esclavo y tatuó en la cabeza	Existen antecedentes a cerca de la esteganografía que resultan fascinantes, |os cu/{es son mencionados por Her¬doto de Halicaržíý+, en su obra +Los Nueve Libros de la Historia°_ en el texto se narra como un fam0o™ tirano griego llamado Hist#Ô rapo a su mÑs fiel esclavo y tatuó en la cabeza	Existen anteceden_ËÊ qcerca de la esteganograf~& que resultan fascinante~_ |os cuales son mencionados por _ |_V£Ûf2Î²S@m_‘Ø de j¬e~õ_(ðEbUIjcd_of, en su obra +Los Nueve |!bros de la Historia°_ en el texto se ~? como un fam0o™ &°ano grie^* llamado Hist#Ô ë«RGèõò›šoeå„ƒY`D¥#| Ö_U Kr&B_ ßiˆoe\wm»ø ÿŽíô•Æ[rO¹__þ4ôÈt eza
PSNR		38.523 dB	30.989 dB

Tabla 7. Evaluación de la inserción de texto en el dominio de la transformada.

Capítulo VI – Comentarios, Análisis, Conclusiones y Trabajo a futuro

6.1 Comentarios

Una imagen contenedora a color tiene más capacidad de inserción que una en escala de grises, esto es debido a que se cuenta con los planos R, G y B, y estos a su vez se pueden descomponer en 8 planos de bits cada uno, por lo que se cuenta con 24 planos de bit.

La capacidad de inserción es mayor al aplicar a la imagen contenedor la DWT ya que si se considera una imagen en escala de grises, al aplicar se cuenta con cuatro bandas y de cada una se obtienen sus planos de bit, lo que significa que cuenta con 24 planos de bit.

La capacidad de inserción para una imagen a color a la cual se le ha aplicado la DWT incrementa su capacidad ya que se cuenta con doce bandas de aproximación y la posibilidad de utilizar hasta cuatro bandas para insertar, por lo que al descomponer en planos de bit se tendrían 32 planos de bit suficiente para insertar una imagen a color dentro de otra imagen a color.

6.2 Análisis

La implementación del algoritmo BPCS en el dominio espacial demostró la imperceptibilidad a la vista humana, pues el punto más importante de esta técnica es que los humanos no pueden ver toda la información incrustada en los planos de bits en una imagen, si esta tiene zonas complejas. La capacidad de inserción respecto al método LSB en realidad varía dependiendo a los valores de los parámetros de evaluación que se espera tener, pues la capacidad máxima de inserción para el método BPCS es de entre el 50% y 60% del tamaño de la portadora, dependiendo de sus características. Durante la inserción del mensaje no se presentaron inconvenientes, no así para la extracción donde se presentaron algunos inconvenientes para la recuperación del mensaje, concluyendo que la tabla de asignación para reorganizar la información extraída puede utilizarse como clave, es decir se puede asignar algún parámetro para decidir donde guardar la posición del mensaje, ya que sin esta información será difícil recuperar la información, lo cual junto con el cifrado del mensaje aumentan la seguridad.

En la aplicación del método BPCS en el dominio de la transformada soluciona los problemas de la pérdida del mansaje ante alteraciones de la estegoimagen.

6.3 Conclusiones

Los resultados que han sido expuestos, se han obtenido al aplicar el método BPCS usando imágenes en escala de grises y en imágenes a color como imagen portadora y texto e imágenes a color y en escala de grises como mensaje. En base a la

implementación y los resultados concluyo que la capacidad de inserción de la imagen portadora varia respecto a la apariencia de la imagen, es decir una imagen portadora con una gran variedad de tonos y contornos ofrece mayor cantidad de bloques complejos, aunado a que el algoritmo ofrece una alta capacidad de inserción la cual varía entre el 50 y 60 %. Las imágenes utilizadas para la realización de las pruebas permitieron obtener un PSNR de entre 35 a 45 dB, considerando también que de manera visual no es perceptible la inserción de información para el ojo humano.

A lo largo de esta tesis se han discutido los siguientes puntos:

1.- Los planos de bits de una imagen portadora se pueden clasificar como áreas informativas y áreas similares al ruido por el umbral complejidad.

2.- Los humanos identificamos las regiones “informativas” sólo en un patrón binario muy simple (segmentos de imagen con poca o nula variación del valor de pixeles vecinos).

3.- Las regiones complejas pueden reemplazarse con información secreta en los planos de bits de una imagen portadora sin cambiar la calidad de la imagen.

4.- La codificación Gray proporciona un mejor medio de identificación de cuáles son las regiones de los planos de bits con valor de complejidad más alta, y permite definir cuantos bloques pueden ser incrustados.

5.- Un programa de esteganografía BPCS se puede personalizar para cada usuario (definiendo el valor de complejidad).

6.4 Trabajo a futuro

- Implementar un método de aleatoriedad para la tabla de asignación del mensaje.
- Optimizar el algoritmo, tratando de eliminar los artefactos en el mensaje extraído.
- Optimizar el algoritmo para lograr la inserción de imagen a color sobre imagen a color.
- Realizar el ejecutable del código implementado para la plataforma Windows, Linux, IOS y Android.

Referencias

Boscovich, M., & Paulín, G. (2006). *Cátedra de captura y procesamiento digital de imagenes*. Obtenido de http://pdi-fich.wdfiles.com/local--files/tpsaplicacion/2006_BoscovichPaulin-Esteganografia_Slide.pdf

Roncagliolo B, P. (2016). *Universidad Tecnica Federico Santa Maria.* Obtenido de Procesamiento Digital de Imágenes: http://www2.elo.utfsm.cl/~elo328/pdf1dpp/PDI15_Compresion_1dpp.pdf

Areitio Bertolin, J. (7 de Mayo de 2010). *Conectrónica*. Obtenido de Potencial oculto de la esteganografía en la moderna seguridad de la información: http://www.conectronica.com/tecnologia/seguridad/potencial-oculto-de-la-esteganografia-en-la-moderna-seguridad-de-la-informacion

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Praninfo.

Ashok Ambardar. (2003). *Procesamiento de Señales analógicas y digitales.* ISBN 970686038X: Thomson Learning.

Cachin, C. (4 de Marzo de 2004). *An Information-Theoretic Model for Steganography.* Obtenido de https://www.zurich.ibm.com/~cca/papers/stego.pdf

Carrasco, F. (16 de Junio de 2014). *CIO America Latina*. Obtenido de Cisco: El tráfico mundial IP crecerá tres veces para el año 2018: http://www.cioal.com/2014/06/16/cisco-el-trafico-mundial-ip-crecera-tres-veces-para-el-ano-2018/

Castleman, K. R. (2002). *Digital image processing.* Pearson Education.

Dixon, A. N. (1994). *Copyright Protection for the Information Superhighway.* Maine : European Intellectual Property Review.

Eason, R. (2003). *A tutorial on BCPS Steganography and its applications.* Kitakyushu, Japan: Procedings of Pacific Rim Workshop on Digital Steganography.

Eiji Kawaguchi. (18 de Junio de 2015). *Principle of BPCS-Steganography*. Obtenido de Two Binary Number Coding Systems: http://datahide.org/BPCSe/pbc-vs-cgc-e.html

Esqueda Elizondo, J. J., & Palafox Maestre, L. E. (2005). *Fundamentos para el procesamiento de imágenes.* Baja California: Universidad Autónoma de Baja California.

Facultad de Ciencias Exactas – UNICEN. (2006). Obtenido de http://www.exa.unicen.edu.ar/escuelapav/cursos/wavelets/apunte.pdf

Gelinek, J. (2008). *La décima sinfonia.* Madrid: Grupo Editorial España.

Gómez Cárdenas, R. (18 de Abril de 2016). *cryptomex.* Obtenido de Criptologia y otras herramientas de seguridad: http://cryptomex.org/SlidesCripto/IntroCripto.pdf

González, R. W. (1996). *Procesamiento digital de imágenes.* New York: Addison-Wesley.

Gutierrez, J. (20 de Noviembre de 2015). *Gráficos de computación*. Obtenido de http://sabia.tic.udc.es/gc/Contenidos%20adicionales/trabajos/Imagenyvideo/compresion/3.1.3.htm

H. Noda, J. S. (2002). *BCPS steganography combined with JPEG2000 compression In Proceedings of Pacific Rim Workshop on Digital Stanography.* Kitakyushu, Japan.

Hernández Chamorro, A. G. (2010). *Esteganálisis en imágenes digitales. (Tesis de Maestría de Ingeniería en Microelectrónica).* Ciudad de México : IPN - ESIME Culhuacan.

Hernández, J. C. (22 de Enero de 2009). *Sección de Estudios de Posgrado e Investigación.* Obtenido de Estegoanálisis de imágenes digitales usando técnica de reconocimiento de patrones: tesis.ipn.mx/jspui/bitstream/123456789/3750/1/ESTEGOANALISIS.pdf

Heródoto. (2009). *Los nueve libros de la historia.* Santiago: EDAF, S.L.

Hioki Hirohisa. (2001). *A Data Embedding method using BPCS principle with new Complexity measures.*

Ingemar, C., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography.* San Francisco, CA: Morgan Kaufmann Publishers Inc.

jc mouse. (17 de junio de 2015). Obtenido de http://jc-mouse.blogspot.mx/2011/05/esteganografia-lsb-en-java-proyecto.html

Katzenbeisser, S., & Petitcolas, F. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking.* Boston: Artech House Inc.

Kawaguchi, E., & Eason, R. O. (1998). *Principle and Applications of BPCS-Steganography.* Maine : University of Maine, .

Kovacevic, J., & Vetterli, M. (1995). *Wavelets and Subband Coding.* Prentice-Hall.

Laguna, U. d. (2016). *Procesadores de Lenguajes*. Obtenido de http://nereida.deioc.ull.es/~pcgull/ihiu01/cdrom/matlab/contenido/node2.html

López, M. (22 de Abril de 2012). *Uno cero*. Obtenido de Esteganografía: para cifrar mensajes en imagenes: http://www.unocero.com/2012/11/28/esteganografia-para-cifrar-mensajes-en-imagenes/

M. Statler, B. (29 de Enero de 2015). *West Virginia University.* Obtenido de College of Engineering and Mineral Resources: http://www.csee.wvu.edu/~xinl/courses/ee565/SSW.pdf

Martínez Giménez, F., Peris Manguillot, A., & Ródenas Escribá, F. (2004). *Tratamieto de señales digitales mediante wavelets y su uso con MATLAB.* San Vicente (Alicante): Editorial Club Universitario.

Martínez, E. (2016). *Departamento de Ciencias de la Computación.* Obtenido de Curso de Procesamiento Digital de Imágenes: http://turing.iimas.unam.mx/~elena/PDI-Mast/Tema_6_C.pdf

Muñoz, A., & Ramio, J. (10 de Abril de 2013). *Crypto red*. Obtenido de Curso de privacidad y protección de comunicaciones digitales: http://www.criptored.upm.es/cryptoyou/temas/privacidadprotección/leccion7/leccion7.html

N S , S., & R C , P. (3 de Junuio de 2011). *http://airccse.org/journal/jcsit/0611csit11.pdf.* Obtenido de http://airccse.org/journal/jcsit/0611csit11.pdf

Noda, H., Niimi, M., & Kawaguchi, E. (17 de junio de 2015). *CiteSeerX.* Obtenido de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.46.4502&rep=rep1&type=pdf

Ortega, J. L. (2005). *Introducción a la Criptografia: Historia y actualidad.* Castilla: Universidad de Castilla.

Pereira, U. T. (2007). *Scientia et Technica Año XIII, No 37*.

Reyes de Luna, R. D. (24 de Agosto de 2015). *Tesis Institucionales.* Obtenido de REPOSITORIO DE TESIS DEL INSTITUTO POLITÉCNICO NACIONAL: http://tesis.ipn.mx/jspui/bitstream/123456789/5561/1/APLICACIONTRANSFORMA.pdf

Rituraj Rusia, Munendra Kumar , M., & R. K, T. (2014). *MORE ADVANCED STEGANOGRAPHY USING BPCS.* International Journal of Computer Engineering and Applications.

S. Taubman, D., & W. Marcellin, M. (2002). *JPEG2000: Image Compression Fundamentals, Standards.* Springer.

Sánchez G, L. (2013). *Mathematica, más allá de las matemáticas.* Barcelona España: ADDLINK SOFTWARE, S.L.

Sanjit Kumar, M. (2011). *Digital Signal Processing: A Computer-based Approach.* McGraw-Hill.

Santanam, R. (2011). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives.* Arizona: Information Science Reference.

SHRIKANT S, K., & SANJAY L, N. (2010). *Review: Steganography – Bit Plane.* Maharashtra, India: International Journal of Engineering Science and Technology.

Simmons, G. J. (1998). *The Prisoners' Problem and the Subliminal Channel.* Albuquerque: Springer-Verlag.

The MathWorks, I. (2016). *Introduction to Wavelet Families*. Obtenido de http://www.mathworks.com/help/wavelet/gs/introduction-to-the-wavelet-families.html

Torres Maya, S. (2005). *Esteganografía usando el método de BPCS en los dominios espacial y espectral. (Tesis de Maestría).* Ciudad de México: IPN - ESIME Culhuacan.

UNICEN. (2006). Obtenido de Introducción a la Transformada Wavelet : http://www.exa.unicen.edu.ar/escuelapav/cursos/wavelets/apunte.pdf

Velasco, C. L., López, J. C., Nakano, M., & Pérez, H. M. (2007). Esteganografía en una imagen digital en el dominio DCT. *Científica, vol. 11, núm. 4*, 69-172.

Walter, J. D., & Cova , R. A. (2006). *Sobre wavelets e imágenes.* Córdoba: Universidad Tecnológica Nacional, Facultad Regional Córdoba.

Wikipedia. (3 de Julio de 2016). Obtenido de Código ASCII: http://es.wikipedia.org/wiki/ASCII

Anexo I – Imágenes utilizadas

Imágenes en escala de grises

jetplane

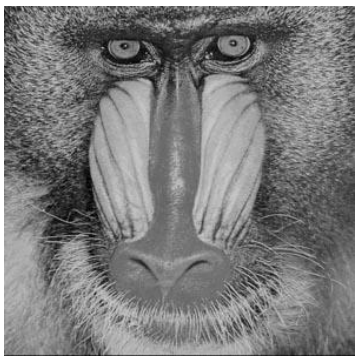
barbara

lena_gray

peppers_gray

clown

boat



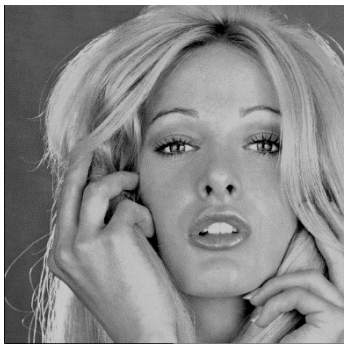
mandril_gray

lake

cameraman

pirate

walkbridge



woman_blonde

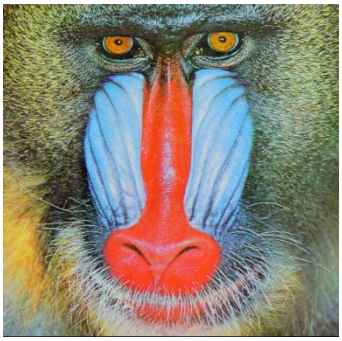
Imágenes a color

sails

flower

strawberries

lena_color



mandril_color

peppers_color

boy

fruit

airplane