DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

TEMA: DESARROLLO DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN SEGURA DE IMÁGENES OCULTAS EN UN VIDEO USANDO IMÁGENES MOSAICO SECRETAS POR TRANSFORMACIÓN DE COLOR REVERSIBLE.

AUTOR: GARCÉS PICO, RÓMULO PATRICIO

DIRECTOR: ING. ACOSTA BUENAÑO, FREDDY ROBERTO

SANGOLQUÍ

2020

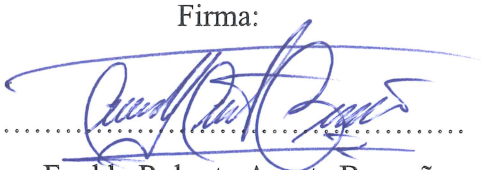
DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"DESARROLLO DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN SEGURA DE IMÁGENES OCULTAS EN UN VIDEO USANDO IMÁGENES MOSAICO SECRETAS POR TRANSFORMACIÓN DE COLOR REVERSIBLE"** fue realizado por el señor Garcés Pico Rómulo Patricio el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas - ESPE, razón por la cual me permito acreditar y autorizar al señor **RÓMULO PATRICIO GARCÉS PICO** para que lo sustente públicamente.

Sangolquí, 15 de enero del 2020

Firma:



Ing. Freddy Roberto Acosta Buenaño
Director del proyecto
C. C: 1709439887

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, **GARCÉS PICO, RÓMULO PATRICIO**, con cédula de identidad Nro. 1718826462, declaro que el contenido, ideas y criterios del trabajo de titulación: **"DESARROLLO DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN SEGURA DE IMÁGENES OCULTAS EN UN VIDEO USANDO IMÁGENES MOSAICO SECRETAS POR TRANSFORMACIÓN DE COLOR REVERSIBLE"** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas - ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 15 de enero del 2020

Firma:

.....

Rómulo Patricio Garcés Pico
C. C: 1718826462

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **GARCÉS PICO, RÓMULO PATRICIO** autorizo a la Universidad de las Fuerzas Armadas - ESPE publicar el trabajo de titulación: **"DESARROLLO DE UNA TÉCNICA ESTEGANOGRÁFICA PARA LA TRANSMISIÓN SEGURA DE IMÁGENES OCULTAS EN UN VIDEO USANDO IMÁGENES MOSAICO SECRETAS POR TRANSFORMACIÓN DE COLOR REVERSIBLE"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 15 de enero del 2020

Firma:

.....

Rómulo Patricio Garcés Pico
C. C: 1718826462

DEDICATORIA

"No nos cansemos de hacer el bien, porque a su debido tiempo cosecharemos si no nos damos por vencidos." Gálatas 6:9

A mis padres, con todo cariño y amor. Por su apoyo constante, por llenar mi vida con sus valiosos consejos, por el amor, trabajo y sacrificio, que me ha permitido llegar a cumplir hoy un sueño más. A mi padre, por buscar siempre las maneras de ofrecerme lo mejor, por haber trabajado duro y sin importar el cansancio siempre tener una sonrisa que ofrecer, por enseñarme a ver el lado positivo en todo momento y motivarme a seguir adelante. Se que hoy me ve orgulloso desde el cielo. A mi madre, por haber confiado en mí, porque al inicio de este viaje hubo momentos en los que pensé rendirme y tirar la toalla, pero su apoyo me motivó a continuar y me enseñó que incluso la tarea más grande se puede lograr si se hace un paso a la vez. A mi hermana, por su cariño y apoyo incondicional durante todo este proceso, por estar conmigo en todo momento. Y aunque en la mayoría del tiempo no coincidamos, y seamos polos opuestos, me has enseñado mucho acerca de la vida. A mi esposa, por todo el amor que me ha brindado, por haber sacrificado su descanso y levantarse junto a mí en las madrugadas, por apoyarme en todo momento y sobre todo cuando más lo he necesitado, y haber estado junto a mí durante todos estos años, ayudándome a ser la mejor versión de mí.

Rómulo Patricio Garcés Pico

AGRADECIMIENTO

"Estén siempre alegres, oren sin cesar, den gracias a Dios en toda situación, porque esta es su voluntad para ustedes en Cristo Jesús." 1 Tesalonicenses 5:16-18

Agradezco a Dios, por haberme dado la oportunidad de estudiar en una de las mejores universidades de mi país, por darme salud, tener una familia maravillosa, por todas las bendiciones que me ha dado, y sobre todo porque nunca me ha dejado solo, siempre he podido voltear a ver al cielo, sonreír y decir, "Yo sé que fuiste tú". ¡Gracias Dios! Agradezco a mis padres, por cada mañana que se levantaron de su cama, para salir a buscar un mejor futuro para sus hijos, por cada día que con esfuerzo llevaron la comida al hogar y sobre todo por haber estado a mi lado apoyándome desde que nací ¡Mil gracias! Agradezco a mi padre, porque muchas veces me ayudó con mis estudios, por acompañarme, por estar siempre presente, por haber sacrificado tanto para que culmine esta meta, fue y siempre será un gran apoyo. ¡Gracias papito! Agradezco a mi madre, por ser mi apoyo y mi sustento, porque cuando ni yo creía en mí, ella sí. Gracias por apostar por mí, por la confianza, por los sacrificios, y por creer siempre que llegaría lejos. "Gracias mamitita" Agradezco a mi hermana, por haber forjado mi carácter, por hacerme una persona valiente, que no teme a las adversidades de la vida, porque cuando necesité que me exijan y corrijan mi camino estuviste ahí. "Gracias ñaña" Agradezco a mi esposa, porque han pasado más de 5 años desde que nos conocimos, y durante todo ese tiempo ha estado a mi lado, gracias por haber confiado en mí, por buscar lo mejor para mí, por llenar mi vida de amor, alegría y porque hemos aprendido mucho juntos, y has hecho de mí una mejor persona. "Gracias amor"

ÍNDICE DE CONTENIDOS

CARÁTULA i

CERTIFICACIÓN ii

AUTORÍA DE RESPONSABILIDAD iii

AUTORIZACIÓN iv

DEDICATORIA v

AGRADECIMIENTO vi

ÍNDICE DE CONTENIDOS vii

ÍNDICE DE TABLAS xiii

ÍNDICE DE FIGURAS xiv

ÍNDICE DE ECUACIONES xviii

RESUMEN xix

ABSTRACT xx

CAPITULO 1 1

1. INTRODUCCIÓN 1

1.1. Antecedentes 1

1.2. Justificación e Importancia 2

1.3. Alcance del Proyecto 4

1.4. Objetivos 5

1.4.1 General 5

1.4.2. Específicos 5

1.5. Contenido 5

CAPITULO 2 7

2. MARCO TEÓRICO 7

2.1. Procesamiento de señales 7

2.2. Muestreo 9

2.3. Cuantificación 10

2.4. Codificación 10

2.5. Información 11

2.6. Transmisión de la información 13

2.7. Seguridad de la información 14

2.8. Ocultación de la información 15

2.9. Métodos para ocultar información 15

2.10. La criptografía y la esteganografía 17

2.11. Diferencia entre encriptar y cifrar 21

2.12. Imágenes digitales 22

2.13. Tipos de imágenes digitales 22

2.13.1. Imágenes vectoriales 22

2.13.2. Imagen bitmap 24

2.14. Parámetros de la imagen 26

2.14.1. Media 27

2.14.2. Desviación estándar 27

2.14.3. Histograma 27

2.15. Mediciones de la calidad de la imagen 28

2.15.1. RMSE (Root Mean Square Error) 28

2.16. Capacidad de incrustación 28

2.17. Esteganografía 29

2.17.1. Tipos de técnicas esteganográficas en imágenes 29

2.17.2. Esteganografía en el dominio espacial 30

2.18. Imágenes como medio portador dentro de la esteganografía 32

2.19. Compresión de imágenes digitales 34

2.19.1. Formato JPG (Joint Photographic Experts Group) 34

2.19.2. Formato GIF (Graphics Interchange Format) 35

2.19.3. Formato PNG (Portable Network Graphics) 35

2.20. Audio como medio portador dentro de la esteganografía 36

2.21. Técnicas de esteganografía en audio 37

2.21.1. Codificación del bit menos significativo 37

2.22. Formatos de Audio 37

2.22.1. Formato WAV (Waveform Audio File) 37

2.22.2. Formato WMA (Windows Media Audio) 37

2.22.3. Formato MP3 (MPEG Audio Layer III) 38

2.23. Video como medio portador dentro de la esteganografía 38

2.23.1. Componentes del Video 38

2.24. Formatos de Video 39

2.24.1. Formato AVI (*Audio Video Interleaved)* 39

2.24.2. Formato MPEG (*Moving Pictures Expert Group*) 40

2.24.3. Formato MOV 40

2.24.4. Formato WMV (*Windows Media Video*) 40

CAPITULO 3 42

3. DISEÑO DEL PROGRAMA 42

3.1. Descripción general 42

3.2. Definición del video portador de la información 43

3.3. Definición de las imágenes secretas a ser ocultas 43

3.4. Conversión del video portador, desde su formato original a formato AVI 45

3.5. Descomposición del video portador de la información 47

3.6. Detección de cambios de escena en la secuencia de fotogramas 49

3.7. Identificación de las imágenes portadoras de la información 52

3.8. Descartar fotogramas compuestos uniformemente 53

3.9. Definición del par imagen secreta / imagen portadora más apto para procesar 54

3.10. Transformación de la imagen secreta en la imagen portadora 56

3.11. Organización de la información de recuperación.....60

3.12. Encriptación de la información 60

3.13. Incrustación de datos en el audio 61

3.14. Creación del estego audio.....62

3.15. Construcción del estego-video 62

3.16. Recuperación de la información oculta 62

3.17. Desencriptación de la información recuperada 63

3.18. Reconstrucción de vectores e imágenes secretas 63

3.19. Procesamiento posterior a la recuperación de la imagen 64

CAPITULO 4 66

4. ANÁLISIS DE RESULTADOS 66

4.1. Métodos de conversión de videos 66

4.2. Algoritmo para detección de cambios de escena.....66

4.3. Pruebas del algoritmo de detección de cambios de escena 69

4.4. Pares a procesar definidos por el algoritmo 72

4.5. Encriptación de datos 72

4.6. Incrustación de información en el audio 73

4.7. Construcción del estego video 76

4.8. Capacidad de incrustación 76

4.9. Imágenes recuperadas 80

4.10. PSNR (Peak Signal to Noise Ratio) 86

4.11. RMSE (Root Mean Square Error) 88

4.12. SSIM (Structural Similarity Index) 91

4.13. Análisis de histogramas 93

4.14. Resultados del MOS (Mean Opinion Score) 98

CAPITULO 5 103

5. CONCLUSIONES Y RECOMENDACIONES 103

5.1. Conclusiones 103

5.2. Recomendaciones 104

5.3. Trabajos futuros 105

Referencias 105

Anexos 109

ÍNDICE DE TABLAS

Tabla 1 Tabla resumen de las técnicas esteganográficas en el dominio espacial.....31

Tabla 2 Valores del modelo RGB para generar colores básicos 32

Tabla 3 Definición de características del sonido.....36

Tabla 4 Tabla de las muestras tomadas de cada fotograma para realizar las pruebas.....52

Tabla 5 Valor promedio del SSIM según el tipo de cambio de escena.....53

Tabla 6 Resultados de la comparación con varias muestras de cada fotograma 68

Tabla 7 Porcentaje de mejora del algoritmo original 68

Tabla 8 Resultados del cálculo de la desviación estándar de varios fotogramas 70

Tabla 9 Desviaciones estándar medidas en los fotogramas uniformes iniciales del video 72

Tabla 10 Medición de parámetros estadísticos al estego-audio y el audio recuperado.....73

Tabla 11 Tamaño de los vectores generados por la transformación de cada imagen secreta....80

Tabla 12 PSNR entre las imagen objetivo, estego-imagen e imagen recuperada 87

Tabla 13 RMSE entre la imagen objetivo, la estego-imagen y la imagen recuperada.....89

Tabla 14 SSIM medido.....91

Tabla 15 Resumen de respuestas de las preguntas 1 y 2 98

ÍNDICE DE FIGURAS

Figura 1. Características de una señal Analógica 7

Figura 2. Diagrama de bloques de un sistema de tratamiento digital de señales. 8

Figura 3. Muestreo periódico de una señal analógica. 9

Figura 4. Cuantificación y codificación de una señal 10

Figura 5. Clasificación de los datos por su tipo de contenido 12

Figura 6. Proceso para adquirir conocimiento 13

Figura 7. Transmisión de información en la actualidad 14

Figura 8. Comparación entre la esteganografía y criptografía 17

Figura 9. Esquema del problema del prisionero 18

Figura 10. Ejemplo de envío del mensaje sin ser ocultado 18

Figura 11. Ejemplo de mensaje cifrado enviado 19

Figura 12. Ejemplo de mensaje enviado con información oculta dentro 19

Figura 13. Ejemplo de información oculta encontrada por el receptor 20

Figura 14. Ejemplo de uso de esteganografía en la actual red internet 21

Figura 15. Ejemplo de imagen vectorial 23

Figura 16. Zoom de la imagen vectorial sin afectar su calidad 23

Figura 17. Ejemplo de imagen tipo mapa de bits (bitmap) 24

Figura 18. Imagen bitmap pixelada debido al cambio de escala 25

Figura 19. Tipos de técnicas esteganográficas en imágenes 29

Figura 20. Estructura del modelo RGB 32

Figura 21. Imagen (5 pixeles de ancho x10 pixeles de alto) con modelo RGB 33

Figura 22. Valores generados al leer la imagen mostrada en la Figura 21. 33

Figura 23. Ejemplo de una imagen capturada a una tasa de 60 y 120 fps 39

Figura 24. Imagen secreta sobre movilización desde Carondelet 44

Figura 25. Imagen secreta sobre ruta de transporte desde cuarteles 44

Figura 26. Imagen secreta sobre personas buscados por las autoridades 45

Figura 27. Imagen secreta sobre retratos hablados 45

Figura 28. Programa de conversión de formato desarrollado en Matlab® 46

Figura 29. Archivo generado por la descomposición del video 47

Figura 30 Carpeta donde se almacenan los 2639 fotogramas del video portador 48

Figura 31 Ejemplo de proporción aurea en una imagen 49

Figura 32 Ejemplo de detección del punto áureo en una imagen 50

Figura 33 Cuadrícula con puntos áureos de una imagen 51

Figura 34 Ejemplo del uso de la regla de los tercios 51

Figura 35 Fotogramas compuestos uniformemente extraídos del video portador 54

Figura 36 Resultado de la comparación entre fotogramas portadores e imágenes secretas 55

Figura 37. Imagen tipo mosaico generada para la transformación 56

Figura 38 Diagrama de bloques de algoritmo Ya-Lin – Wen-Hsiang 57

Figura 39 Ejemplo de imagen generada por la división en bloques 58

Figura 40 Ejemplo de imagen generada por la división en bloques 58

Figura 41 Todas las 16 imágenes generadas por la división en bloques 59

Figura 42 Información relevante respecto a la inserción de bits en el audio 59

Figura 43 Referencia del modelo de Cifrado de César 61

Figura 44 Primeros 25 fotogramas del video portador estructurados uniformemente 71

Figura 45 Fotogramas con información relevante al video 71

Figura 46. Señal del audio original y estego-audio en el dominio del tiempo 74

Figura 47. Señal del audio original en el dominio de la frecuencia 74

Figura 48. Comparación del audio original y el estego-audio en el dominio de la frecuencia . 75

Figura 49. Comparación del audio original y recuperado en el dominio de la frecuencia 75

Figura 50 Características del audio del video portador 77

Figura 51 Cálculo del tamaño en disco del audio 78

Figura 52. Propiedades del archivo de audio generado 78

Figura 53. Imagen objetivo (fotograma portador) nro.1 81

Figura 54. Imagen secreta par de la imagen objetivo (fotograma portador) nro. 1 82

Figura 55. Proceso de transformación de la imagen secreta con imagen objetivo nro. 1 82

Figura 56. Estego-imagen generada nro. 1 83

Figura 57. Imagen secreta recuperada nro. 1 83

Figura 58. Imagen objetivo (fotograma portador) nro. 2 84

Figura 59. Imagen secreta par del fotograma portador nro. 2 84

Figura 60. Proceso de transformación de la imagen secreta con la imagen objetivo nro. 2 85

Figura 61. Estego-imagen generada nro. 2 85

Figura 62. Imagen secreta recuperada nro. 2 86

Figura 63 Resultado del cálculo PSNR con la imagen procesada nro. 1 87

Figura 64 Resultado del cálculo PSNR con la imagen procesada nro. 2 88

Figura 65 Resultado del cálculo RMSE con la imagen recuperada 1 90

Figura 66 Resultado del cálculo PSNR con la imagen recuperada 2 90

Figura 67 Resultado del cálculo SSIM con la imagen procesada nro. 1 92

Figura 68 Resultado del cálculo SSIM con la imagen recuperada 2 93

Figura 69 Histograma del canal R de la imagen objetivo y la estego-imagen nro.1 94

Figura 70. Histograma del canal G de la imagen objetivo y la estego-imagen nro.1 95

Figura 71. Histograma del canal B de la imagen objetivo y la estego-imagen nro.1 95

Figura 72. Histograma del canal R de la imagen secreta y la imagen recuperada nro.1 96

Figura 73. Histograma del canal G de la imagen secreta y la imagen recuperada nro.1 97

Figura 74. Histograma del canal B de la imagen secreta y la imagen recuperada nro.1 97

Figura 75 Resultados de la primera pregunta del MOS 98

Figura 76 Resultados de la segunda pregunta del MOS 99

Figura 77 Resultados de la tercera pregunta del MOS 100

Figura 78 Resultados de la cuarta pregunta del MOS 101

Figura 79 Resultados de la cuarta pregunta del MOS 102

ÍNDICE DE ECUACIONES

Ecuación 1. Función de interpolación 9

Ecuación 2. Modelo para expresar una imagen digital.....26

Ecuación 3. Cálculo de fotogramas que componen el video.....48

Ecuación 4. Cálculo de la relación costo beneficio del algoritmo mejorado 69

Ecuación 5. Cálculo de la cantidad de muestras tomadas 77

Ecuación 6. Cálculo de la cantidad de muestras tomadas 77

Ecuación 7. Cálculo de la cantidad de bits utilizados para cuantificar.....77

RESUMEN

En el presente trabajo de investigación, se desarrolla una técnica esteganográfica que utiliza un método de transformación de color reversible, para convertir varias imágenes denominadas secretas en determinadas imágenes objetivo y ocultar estas en la secuencia de cuadros de un video. Las imágenes objetivo también llamadas fotogramas portadores, corresponden a los cambios de escena del video, los cuales se detectan automáticamente por un algoritmo. Una vez que se determina que imagen secreta se transformará en determinada imagen objetivo, se divide cada una en bloques de 8x8 pixeles, para obtener imágenes tipo mosaico. Los bloques de la imagen secreta tipo mosaico se ordenan en base a la desviación de cada bloque de la imagen objetivo tipo mosaico, se transforman sus propiedades de color y se rota cada bloque determinado ángulo para generar una estego-imagen la cual se asemeja a la imagen objetivo. Para revertir la transformación y recuperar la imagen secreta, se utiliza un vector que contiene los índices, medias y ángulos iniciales de cada imagen secreta y el vector se oculta en el audio del video portador, previamente, este vector pasa por un proceso de encriptación, para mejorar la seguridad. Se reemplazan en la secuencia de cuadros las imágenes objetivo por las denominadas estego-imágenes, se crea un estego-video con la secuencia de cuadros que contiene las estego-imágenes y el audio con la información oculta. Finalmente, se realizan mediciones objetivas y subjetivas, para medir la calidad de reconstrucción de las imágenes secretas y el nivel de detección de la información oculta.

PALABRAS CLAVE:

- **ESTEGANOGRAFÍA**
- **MOSAICO**
- **TRANSFORMACIÓN DE COLOR REVERSIBLE**
- **CRIPTOGRAFÍA**
- **AUDIO**

ABSTRACT

In the present research work, a steganographic technique is developed that uses a reversible color transformation method, to convert several so-called secret images into certain objective images and hide these in the sequence of frames of a video. The target images, also called carrier frames, correspond to the video scene changes, which are automatically detected by an algorithm. Once it is determined which secret image will be transformed into a certain objective image, each one is divided into blocks of 8x8 pixels, to obtain mosaic images. The blocks of the mosaic-like secret image are ordered based on the average of each block of the mosaic-like objective image, their color properties are transformed and each determined angle block is rotated to generate a stego-image which resembles the objective image To reverse the transformation and recover the secret image, a vector is used that contains the indexes, means and initial angles of each secret image and the vector is hidden in the audio of the carrier video, previously, this vector goes through an encryption process, To improve security. In the sequence of frames, the target images are replaced by the so-called stereo-images, a video-stereo is created with the sequence of frames containing the stereo-images and the audio with the hidden information. Finally, objective and subjective measurements are made to measure the reconstruction quality of the secret images and the level of detection of the hidden information.

KEYWORDS:

- **STEGANOGRAPHY**
- **MOSAIC**
- **REVERSIBLE COLOR TRANSFORMATION**
- **CRYPTOGRAPHY**
- **AUDIO**

CAPITULO 1

1. INTRODUCCIÓN

1.1. Antecedentes

El ocultamiento de información ha sido utilizado por la humanidad a lo largo de la historia, desde la antigua Grecia donde se enviaban esclavos con mensajes ocultos en sus cabezas que eran rasuradas y tatuadas antes de esperar a que crezca su cabello, para posteriormente ser enviados al receptor deseado. En la actualidad, el avance tecnológico permite disponer de herramientas informáticas, con capacidad de manipular señales digitales y lograr así implementar técnicas esteganográficas que vienen a ser oportunidades de desarrollo en el ámbito de las comunicaciones digitales.

Esta oportunidad de desarrollar técnicas para ocultar información ha sido analizada en varios trabajos de investigación, siendo el de (Ya-Lin Lee, Wen-Hsiang Tsai, 2014), uno de los más importantes al crear una técnica que permite ocultar información dentro de imágenes, utiliza una transformación de color la cual puede revertirse. Esta misma técnica se ha analizado y evaluado en el trabajo de (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016) logrando transformar una imagen secreta en una imagen objetivo o portadora, con resultados bastante óptimos. Posteriormente, fue utilizado en (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018) este concepto, para seleccionar manualmente dos cambios de escena de un video portador y ocultar 2 imágenes secretas en las mismas.

En realidad, el principal problema de ocultar información es la capacidad de incrustación, ya que al aplicar técnicas esteganográficas, debemos considerar que no se puede modificar toda la información del medio portador, puesto que afectaría al sistema y sería detectable. Por ejemplo, en la técnica desarrollada en (Ya-Lin Lee, Wen-Hsiang Tsai, 2014) es necesario disponer de un vector que contiene toda la información para recuperar la imagen original, y este vector debe ser insertado en alguna parte de la información transmitida al receptor. Este técnica, convierte la imagen que se desea transmitir en una imagen tipo mosaico dividiendo la imagen en bloques, transforma sus propiedades y ahora luce como la imagen objetivo seleccionada en base a determinados parámetros, luego aplica una transformación de color la cual es reversible y de esta manera lograr recuperar la imagen original.

En los trabajos de (Carlos Eduardo Rodríguez Guayaquil, Freddy Acosta B., 2016), (Cristian Marcelo Vasco Estupiñan, Freddy Roberto Acosta Buenaño., 2018) se han utilizado algunas técnicas para ocultar información, existen gran variedad de técnicas esteganográficas, pero las técnicas de dominio espacial son las más utilizadas ya que tienen baja complejidad y gran capacidad de incrustación, su desventaja es generar demasiadas pérdidas debido a la compresión de imágenes. Una de las técnicas más utilizadas, es la conocida como LSB (*Least Significant Bit*), por ser una técnica sencilla que implica la sustitución del bit menos significativo de cada vector que compone una señal. Esta variación es prácticamente imperceptible, pero genera irregularidades estadísticas en el medio portador.

1.2. Justificación e Importancia

La necesidad de ocultar información y transmitir mensajes de forma segura, en el ámbito militar donde la comunicación es un punto clave para la coordinación de fuerzas, con influencia en el éxito

o fracaso de misiones. Así como, la exposición de información privilegiada de ciertas empresas vulnerables y con hackers que ejecutan ataques cada vez más sofisticados, son factores que motivan a realizar una investigación en cuanto a los métodos que existen para transmitir mensajes sin ser detectados. La transmisión de mensajes ocultos ha estado inmersa en el desarrollo histórico de la humanidad, su importancia e impacto se puede ver en la reducción de la segunda guerra mundial, en donde gracias al matemático Alan Turing se descifró la máquina enigma, logrando acortar la guerra y de esa manera evitar miles de muertes, así como millones en recursos.

En la Universidad de las Fuerzas Armadas - ESPE se han realizado investigaciones, en las cuales se analizan diferentes técnicas de esteganografía, las más importantes son: utilizar las zonas ruidosas de la imagen mediante transformaciones de color reversible (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016); utilizar técnicas de esteganografía para ocultar texto dentro de archivos de audio (Carlos Eduardo Rodriguez Guayaquil, Freddy Roberto Acosta Buenaño, 2016) y ocultar información en un video (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018).

Tomando en cuenta estos preliminares, el trabajo de investigación se enfoca al desarrollo de una técnica esteganográfica, para transmitir de manera segura varias imágenes que se han ocultado en un video, y para recuperar la información en el receptor de una manera confiable, se desea insertar en el audio, un flujo de bits que contiene parámetros de la transformación de la imagen, este flujo de bits pasará por un proceso de criptografía, con lo cual se busca proteger la información, evitando la intercepción, acceso, modificación e introducción de información extra no autorizada.

1.3. Alcance del Proyecto

Desarrollar un algoritmo genérico para cualquier video, con el cual se podrá separar la señal de audio y los fotogramas que lo componen, luego detectará automáticamente sus cambios de escena, va a generar una base de datos de los fotogramas portadores (cambios de escena detectados), y comparará esta información con las imágenes que se desean ocultar. Posteriormente, se combina con un método de transformación de imágenes, que utiliza las características del color; un método de encriptación de bajo costo computacional; y una técnica de incrustación de información en el audio del video portador, para generar un estego-video que contiene información oculta imperceptible a simple vista. El estego-video será analizado, y se recuperará la información oculta, tanto de los fotogramas como el audio, y finalmente, se evaluarán las características de las imágenes recuperadas a comparación de las originales. Para la evaluación de la calidad del audio y video generado, se aplicará un MOS (*Mean Opinion Score*) para determinar si la técnica desarrollada, da como resultado un video sin alteraciones significantes al original. Para evaluar la calidad y similitud de las imágenes recuperadas, se calculará el valor RMSE (*Root Mean Square Error*), PSNR (*Peak Signal to Noise Ratio*) y el SSIM (*Structural Similarity Index*) entre las imágenes recuperadas y las imágenes originales. La capacidad de incrustación de la técnica estará determinada por los resultados de las pruebas ejecutadas, los análisis de la información que se está insertando en el audio y los resultados del MOS respecto a la calidad del audio generado. La efectividad de la técnica esteganográfica desarrollada, se comprobará con el análisis de los resultados, se mostrará de manera cuantitativa cuantas imágenes se han podido ocultar, cuantas de estas se han logrado recuperar y cuál es la similitud de las imágenes recuperadas y las originales.

1.4. Objetivos

1.4.1 General

Desarrollar un algoritmo que permita insertar varias imágenes secretas dentro de un video y enviar información en el audio para mejorar la reconstrucción de las imágenes en el receptor.

1.4.2. Específicos

- Investigar, analizar y definir el método esteganográfico adecuado para el ocultamiento de información dentro de un archivo multimedia de video.
- Procesar un archivo de video y separarlo en sus componentes de audio y secuencia de frames, identificar los cambios de escena de la secuencia de frames y establecer cuál será la cantidad de imágenes que se pueden ocultar en el video.
- Analizar y determinar la técnica criptográfica adecuada para la codificación del flujo de bits insertado en el audio.
- Aplicar el método esteganográfico, generar un estego-video y reconstruir en el receptor, las imágenes secretas con ayuda de la información oculta en el audio.
- Determinar la eficiencia de los métodos y técnicas utilizadas, usando encuestas subjetivas en una muestra considerable de personas, analizar los resultados de la experiencia de los usuarios, y mediante el uso de herramientas objetivas determinar la calidad del algoritmo desarrollado.

1.5. Contenido

El presente trabajo de investigación está estructurado en cinco capítulos, los cuales se detallan a continuación:

El Capítulo 1 presenta la información previa al trabajo de investigación, nos da una breve introducción al tema desarrollado, pone a consideración del lector los antecedentes, la justificación, el alcance y los objetivos de la investigación, así como un pequeño resumen para entregar una idea clara de lo desarrollado en los demás capítulos.

El Capítulo 2 es el fundamento teórico de toda la investigación subsiguiente. Describe, estudia y analiza los temas más importantes para implementar de manera práctica los objetivos de la investigación. Pone a consideración del lector, la revisión de conceptos de procesamiento digital de señales, transmisión de señales digitales, técnicas esteganográficas con ejemplos de su aplicación y el manejo de archivos multimedia.

El Capítulo 3 describe detalladamente el método aplicado para el desarrollo práctico del presente trabajo de investigación, contiene información específica sobre los criterios utilizados para la implementación de cada etapa del algoritmo.

El Capítulo 4 muestra los resultados obtenidos luego de la implementación del algoritmo. Contiene el detalle de las pruebas ejecutadas, el análisis de los resultados, así como las herramientas que han sido utilizadas para evaluar a la técnica desarrollada.

El Capítulo 5 pone a consideración del lector, las conclusiones, recomendaciones y los trabajos futuros que se proponen a partir de los resultados del trabajo de investigación.

CAPITULO 2

2. MARCO TEÓRICO

2.1. Procesamiento de señales

Una señal se define como magnitudes físicas o variables detectables mediante las cuales se pueden transmitir mensajes o información. En la Figura 1 se puede observar algunas características de una señal senoidal. Las señales eléctricas constituyen el tipo de señales que se pueden medir con mayor facilidad, y que se pueden representar de forma más simple. Es por eso que se busca transformar variables físicas en señales eléctricas, por ejemplo: la temperatura, la humedad, la voz y la intensidad de la luz. Matemáticamente, las señales se representan como funciones de una o más variables independientes. (Soliman, Samir S., 1999)

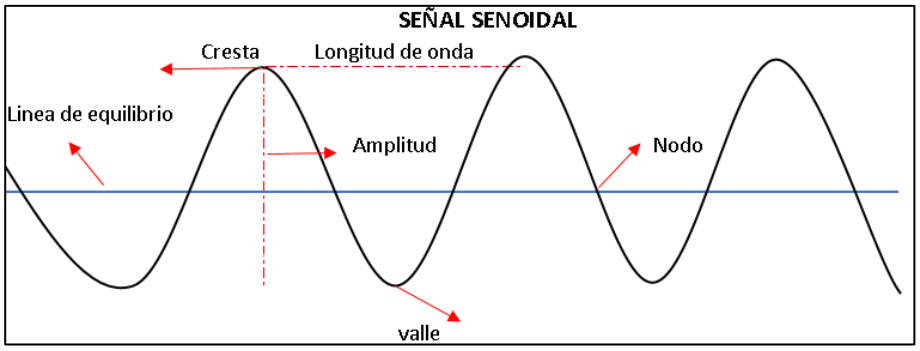


Figura 1. Características de una señal Analógica
Fuente: (CJmagnate, 2017)

Para un sistema de tratamiento digital de señales se deben disponer de algunos elementos básicos. El tratamiento digital de señales proporciona un método alternativo de procesar una señal analógica, como se ilustra en la Figura 2. Para poder realizar un tratamiento digital, es necesario

disponer de una interacción entre la señal analógica y el procesador digital. Esta se denomina convertidor analógico-digital (A/D). La salida del convertidor A/D es una señal digital que es adecuada como entrada del procesador digital. El procesador digital de señales puede ser una computadora digital programable grande o un pequeño microprocesador programado para realizar las operaciones deseadas sobre la señal de entrada.

En aplicaciones en las que la salida digital del procesador digital de señal tenga que entregarse al usuario en formato analógico, como por ejemplo en los sistemas de comunicación por voz, tendremos que proporcionar otra interacción entre el dominio digital y el analógico. Una interacción así es un convertidor digital-analógico (D/A). De este modo, la señal que se proporciona al usuario está en forma analógica, como ilustra el diagrama de bloques de la Figura 2. Sin embargo, existen otras aplicaciones prácticas que implican el análisis de la señal, en las que la información deseada se encuentra en formato digital y, por tanto, no es necesario emplear un convertidor D/A. Por ejemplo, en el procesamiento digital de las señales de radar. (John G. Proakis y Dimitris G. Manolakis, 2007)

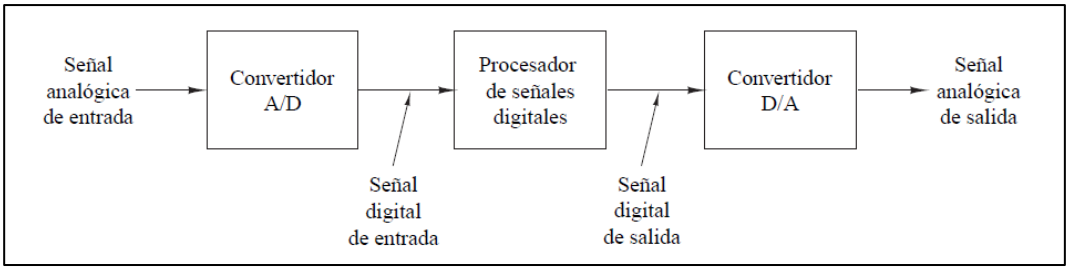


Figura 2. Diagrama de bloques de un sistema de tratamiento digital de señales.
Fuente: (John G. Proakis y Dimitris G. Manolakis, 2007)

2.2. Muestreo

Consiste en la conversión de una señal continua en el tiempo en una señal discreta en el tiempo, obtenida mediante la toma de muestras de la señal continua en el tiempo, en instantes discretos de tiempo. Por tanto, si $x_a(t)$ es la entrada del muestreador, la salida será $x_a(nT) \equiv x(n)$, donde T es el intervalo de muestreo, como se muestra en la Figura 3. (John G. Proakis y Dimitris G. Manolakis, 2007)

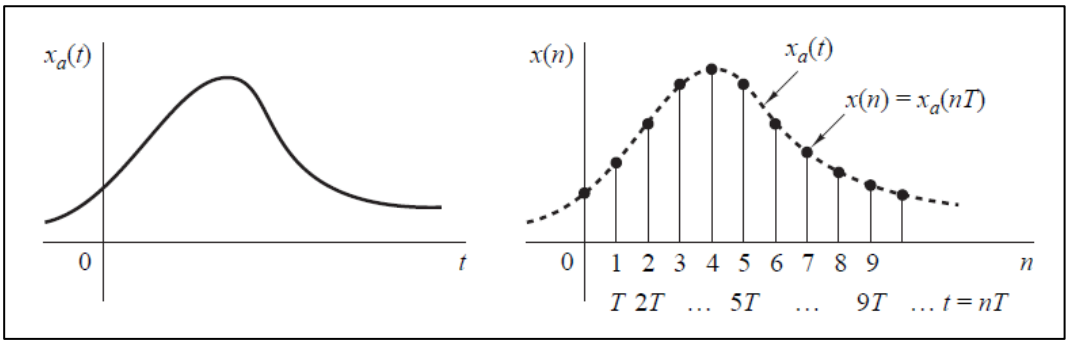


Figura 3. Muestreo periódico de una señal analógica.
Fuente: (John G. Proakis y Dimitris G. Manolakis, 2007)

Es importante tomar en cuenta el teorema del muestreo el cual implica que, si la frecuencia más alta contenida en una señal analógica $x_a(t)$ es $F_{máx} = B$ y la señal se muestrea a una frecuencia $F_s \geq 2F_{máx} \equiv 2B$, entonces $x_a(t)$ puede recuperarse de forma exacta a partir de los valores de sus muestras utilizando la siguiente función de interpolación indicada en la ecuación 1:

$$g(t) = \frac{sen\ 2\pi Bt}{2\pi Bt}$$

Ecuación 1. Función de interpolación

2.3. Cuantificación

Este proceso realiza la conversión de una señal de valores continuos tomados en instantes discretos de tiempo, en una señal de valores discretos en instantes de tiempo discretos (es decir, es una señal digital). Como se muestra en la Figura 4, el valor de cada muestra de la señal se representa mediante un valor seleccionado dentro de un conjunto finito de posibles valores. La diferencia entre la muestra no cuantificada $x(n)$ y la salida cuantificada $x_q(n)$ es el error de cuantificación. (John G. Proakis y Dimitris G. Manolakis, 2007)

2.4. Codificación

En el proceso de codificación, cada valor discreto $x_q(n)$ se representa mediante una secuencia binaria de b-bits, en la Figura 4 se puede observar cómo se codifica cada valor de la cuantificación.

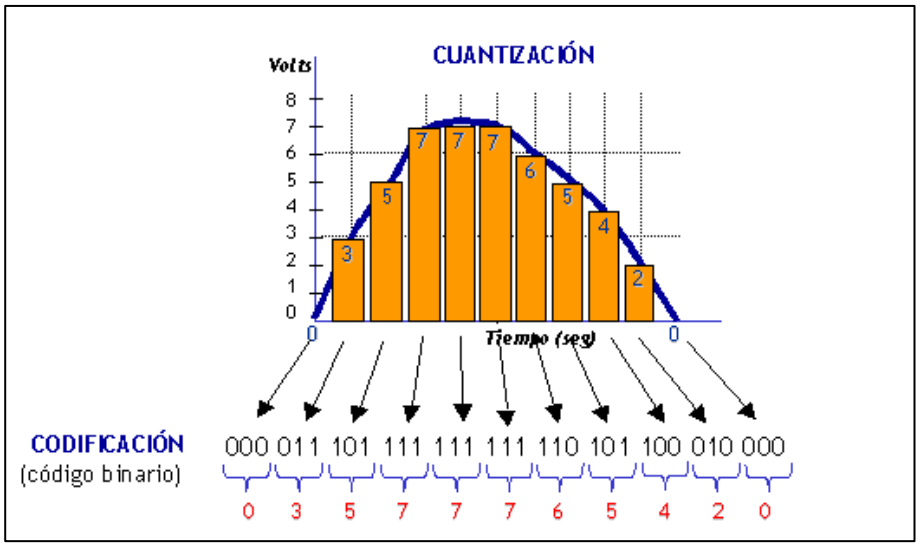


Figura 4. Cuantificación y codificación de una señal
Fuente: (Martinez, 2017)

2.5. Información

La información se puede definir como un conjunto organizado de datos, los cuales han sido seleccionados, organizados, ordenados e interpretados para generar un conocimiento especifico. Por lo que la información cambia el estado de conocimiento de la persona o máquina a la que fue entregada.

Su etimología se origina en el sustantivo latino informationis que viene del verbo informare, que significa: dar forma a la mente, instruir, enseñar. La palabra informationis en latín, era usada para indicar un concepto o una idea. Por lo tanto, se podría decir que la palabra información es dar forma a determinados datos hacia adentro de la persona o máquina.

Es importante tomar en cuenta que la información al estar compuesta por datos tienen ciertas características que los definen. En la Figura 5 se muestra cómo se clasifican los datos en base al tipo de contenido que expresan.

Los datos son representaciones simbólicas de alguna entidad, pueden ser letras alfabéticas, puntos, números, dibujos, etc. Los datos unitariamente no tienen sentido ni valor semántico, es decir, no tienen impacto. Pero al ser procesados adecuadamente, se convierten en información significativa que ayuda a tomar decisiones. En la Figura 6 se muestra el proceso para convertir los datos en conocimiento. (SEO, 2019)

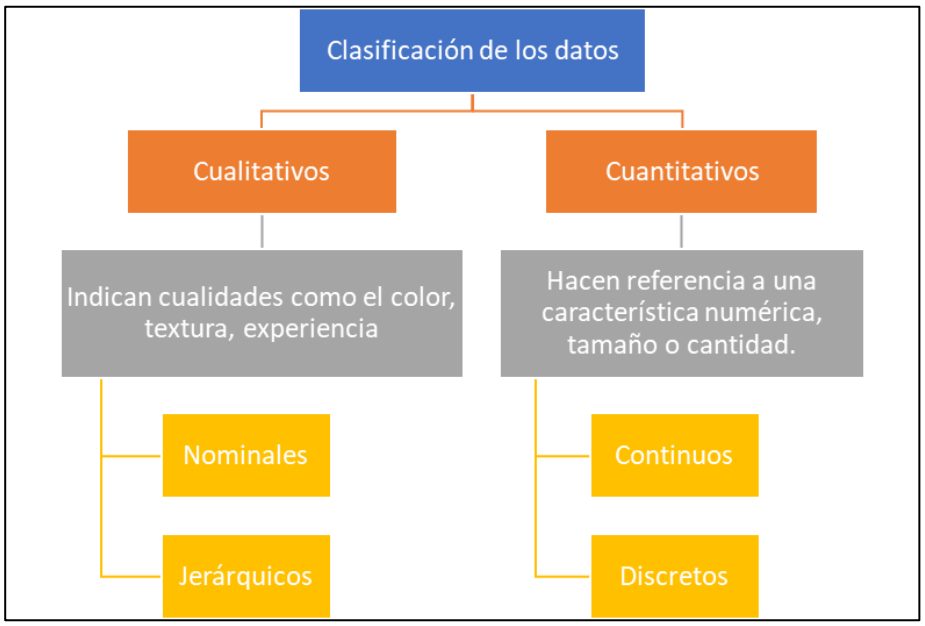


Figura 5. Clasificación de los datos por su tipo de contenido

La información tiene 4 características principales las cuales son:

1. Los datos: Son los detalles, hechos, números y parámetros que pueden ser consolidados para hacer un análisis más profundo.
2. El orden: Permite que la información se pueda comprender y tenga sentido.
3. La veracidad: Implica que las fuentes donde se han generado los datos sean confiables y no genere dudas de su contenido.
4. El valor: Es una característica subjetiva en donde el receptor de la información reconoce si los datos trasmitidos han sido útiles.

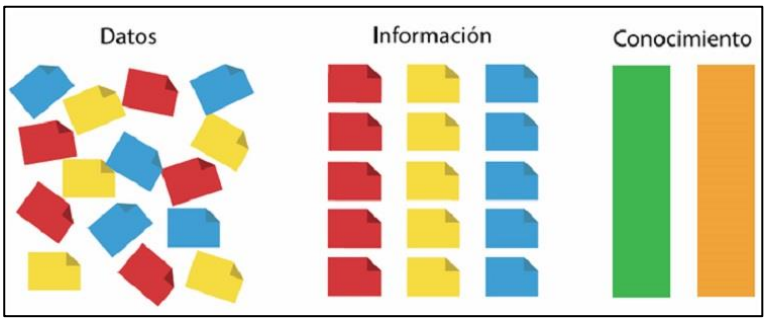


Figura 6. Proceso para adquirir conocimiento
Fuente: (SEO, 2019)

2.6. Transmisión de la información

Antes de analizar los medios y diferentes métodos a través de los cuales las personas transmiten la información, es importante comprender que hay una diferencia entre el proceso de comunicación y transmitir información. La comunicación es el acto de relación entre dos o más sujetos, mediante el cual se evoca en común un significado. Mientras que, la información es un conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y estructurarlos de una manera determinada, de modo que le sirvan como guía de su acción. (Antonio).

En la Figura 7 se muestran algunos ejemplos de las actuales herramientas y métodos utilizados para transmitir información. En la actualidad, en un mundo globalizado y en la denominada era digital, la principal forma de comunicarse es haciendo uso de las redes sociales como: Facebook, Instagram y Twitter. El uso de la televisión ha evolucionado a las plataformas virtuales que entregan contenido bajo demanda, la mayoría de las personas visualiza contenidos que se transmiten mediante streaming.

Figura 7. Transmisión de información en la actualidad
Fuente: (Salgero, 2018)

La información se debe caracterizar por ser siempre: útil, confiable y oportuna.

2.7. Seguridad de la información

Al hablar ya sea de una empresa, institución u organismo es importante tomar en cuenta que la información relacionada a estas debe ser resguardada bajo buenas medidas de seguridad, en entornos financieros, bancarios e investigativos las fugas de información son puntos críticos para el desarrollo de los distintos proyectos que se puedan manejar.

La seguridad de la información engloba un conjunto de técnicas, y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido. La seguridad de la información tiene como objetivo principal proteger los datos de las empresas. Pero, este concepto es en términos generales, puesto que el sistema lo que va a hacer es asegurar tres aspectos fundamentales: la confidencialidad, la disponibilidad y la integridad. (School, 2019)

2.8. Ocultación de la información

Sabiendo que, en nuestra condición de seres sociales, las personas necesitamos comunicarnos. Y la comunicación permite transmitir información e intercambiar o compartir ideas, lo que enriquece la experiencia humana. Por lo tanto, es de vital importancia para el ser humano tener una correcta comunicación y al ser un tema de alto impacto social, la falta de comunicación tiene grandes consecuencias, las cuales expertos han analizado y concluyen que afecta desde relaciones de pareja hasta el desempeño de empresas, organizaciones o países.

De esta manera, nace la idea de ocultar información, lo cual no implica la falta de esta, sino más bien se refiere a que exista una forma de comunicarse que solo sea percibida y utilizada por determinadas personas, a pesar de que se utilicen medios que son accesibles para otros usuarios. Un ejemplo de esto ocurrió en 2010 donde el FBI (*Federal Bureau of Investigation*) destapó una red de espías rusos, los cuales utilizaban métodos propios de la guerra fría para enviar mensajes ocultos en imágenes cargadas a sitios web públicos, este es un claro ejemplo de las aplicaciones del método conocido como esteganografía.

“El antiguo método utilizado para ocultar mensajes es conocido como esteganografía, ya descrito por el historiador Heródoto, consiste en ocultar mensajes dentro de otros mensajes u objetos, como por ejemplo la tinta invisible o la inclusión de texto dentro de imágenes.” (press, 2010)

2.9. Métodos para ocultar información

Para comprender de mejor manera cuales son los métodos o formas a través de las cuales las personas pueden ocultar información, debemos analizar el desarrollo histórico de esta práctica.

El primer registro histórico que se tiene está en los papiros escritos por Heródoto, en los cuales relata la historia del mundo conocido de su época, este escritor griego vivó hace unos 2400 años probablemente en 430 a.C. en estos papiros tenemos un par de ejemplos:

1. Relata como una persona habría usado un cuadernillo con dos hojas, rayó presionando bien la cera que las cubría y posterior a esto la volvió a cubrir con cera normal.
2. Relata como un rey había rasurado la cabeza de un esclavo en quien confiaba, le tatuó un mensaje en su cuero cabelludo, espero el tiempo necesario para que le volviera a crecer el cabello y lo envió a otro reino dándole instrucciones de que le rasuraran la cabeza.

En el siglo XV Giovanni Battista della Porta quien era un científico italiano descubrió cómo esconder un mensaje dentro de un huevo cocido. Para lograrlo, debía preparar una tinta y luego se escribía en la cáscara, esta penetraba en la cáscara porosa y dejaba el mensaje en la superficie de la albúmina del huevo, y se podía leer al pelar el huevo. Benedictino Johannes Trithemius en 1499 escribió el libro “Steganographia” el libro trataba sobre la ocultación de mensajes, y métodos para conjurar a espíritus. Hoy en día el libro es considerado como maldito y es muy apreciado por los esoteristas del mundo entero. (EcuRed, 2019)

De manera general, se podría decir que existen dos formas para ocultar información: la criptografía y la esteganografía. Estos dos métodos suelen confundirse entre sí por ser ambos procesos para proteger información, pero sus fundamentos son distintos los cuales se explican en la Figura 8.

Figura 8. Comparación entre la esteganografía y criptografía

2.10. La criptografía y la esteganografía

"La criptografía y la esteganografía pueden complementarse, dando un nivel de seguridad extra a la información." (EcuRed, 2019)

Se puede cifrar el mensaje que se desea ocultar, si existiera un intruso primero deberá advertir la presencia del mensaje oculto, y posterior descifrarlo. (EcuRed, 2019)

La manera más fácil de entender la diferencia de criptografía y esteganografía es analizando el problema del prisionero (Gustavus J. Simmons, 1983), el cual se ilustra en la Figura 9:

¿Cómo podrían comunicarse dos prisioneros y planear un plan de escape, si están en celdas separadas y solo pueden enviar mensajes a través del guardia?

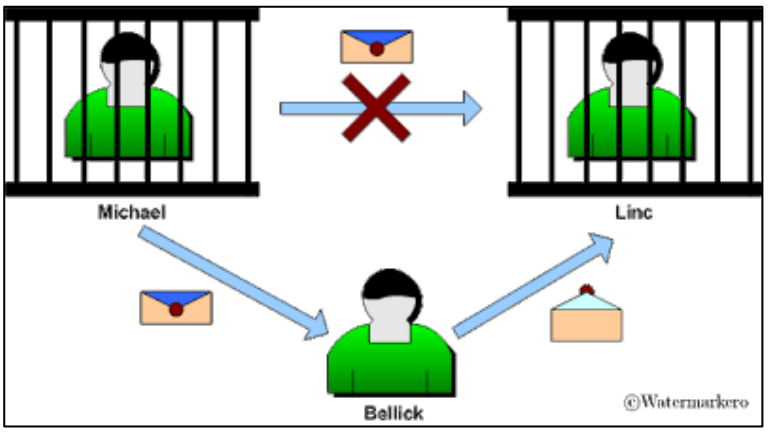


Figura 9. Esquema del problema del prisionero
Fuente: (EcuRed, 2019)

Como se observa en la Figura 9, todos los mensajes deben pasar por el guardia, por lo cual el mensaje debe estar oculto de alguna manera. En la Figura 10 se muestra el envío del mensaje original.

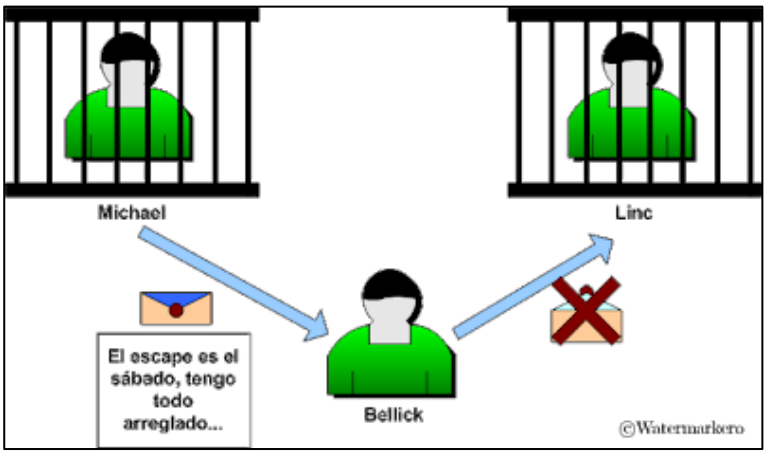


Figura 10. Ejemplo de envío del mensaje sin ser ocultado
Fuente: (EcuRed, 2019)

Si el mensaje que Michael desea que Linc reciba es leído por el guardia (Bellick), ambos prisioneros serán duramente castigados. Por lo tanto, en la Figura 11 se muestra el uso de la criptografía para enviar el mensaje.

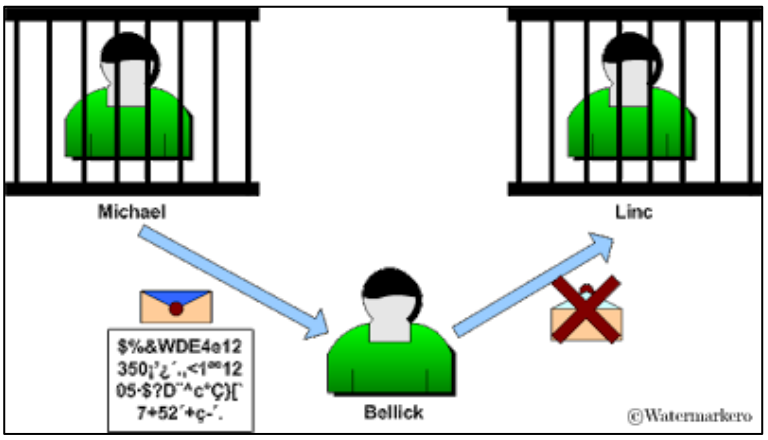


Figura 11. Ejemplo de mensaje cifrado enviado
Fuente: (EcuRed, 2019)

Debido a que Michael conoce de criptografía entonces lo que hace es cifrar el mensaje que le envía a Linc (Linc conoce como descifrar el mensaje), para que Bellick no lo entienda. Pero Bellick al ver el mensaje cifrado, sospecha y lo destruye, evita la planificación del escape y los castiga severamente. Pero, en la Figura 12 se muestra como Michael usa la esteganografía con el mensaje original, lo cual no genera sospechas en Bellick y permite el paso del mensaje.

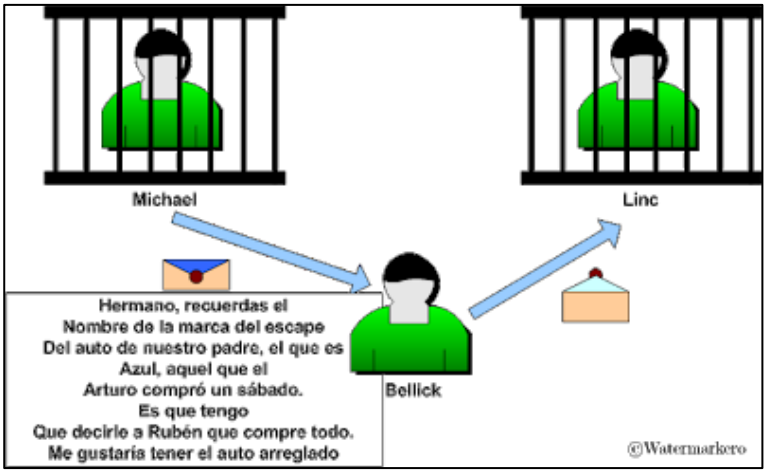


Figura 12. Ejemplo de mensaje enviado con información oculta dentro
Fuente: (EcuRed, 2019)

La mejor opción en este caso sería la esteganografía, Michael al utilizarla puede esconder el mensaje, pero ahora lo haría de una manera tal que dicho mensaje se escondería dentro de otro mensaje menos importante, es decir un medio portador inocuo. Como se muestra en la Figura 13, el mensaje oculto dice: “el escape es el sábado tengo todo arreglado”.

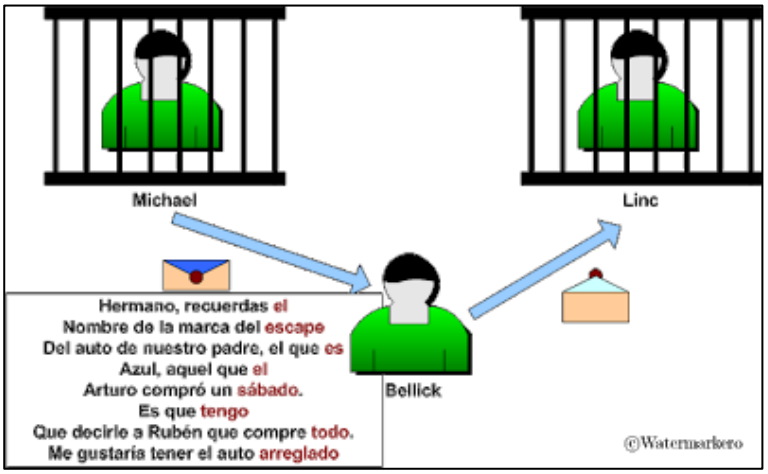


Figura 13. Ejemplo de información oculta encontrada por el receptor
Fuente: (EcuRed, 2019)

El guardia (Bellick) lee el mensaje, pero al parecer no tiene nada extraño, por lo cual no advierte del plan de los prisioneros, y deja pasar el mensaje de Michael a Linc.

Al tomar en cuenta este ejemplo, pero ahora en nuestros días. Bellick podría ser un hacker y está analizando todos los mensajes que envían Michael y Linc, como se muestra en la Figura 14. Si se utiliza la criptografía Bellick trataría de romper dicha codificación para obtener la información oculta, en cambio sí se utiliza la esteganografía Bellick no sabría que existen mensajes encubiertos en dicha comunicación, manteniendo el secreto a salvo.

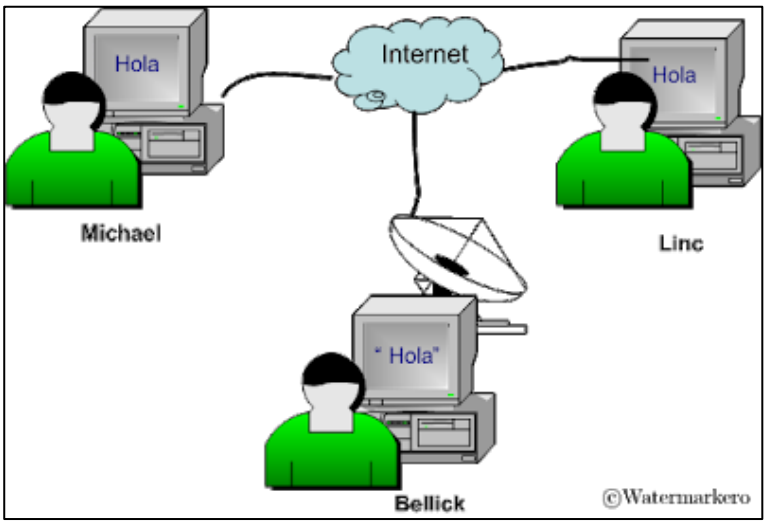


Figura 14. Ejemplo de uso de esteganografía en la actual red internet
Fuente: (EcuRed, 2019)

En un sistema esteganográfico o de marcas de agua se utiliza la criptografía (cifrando el mensaje que se oculta) para obtener una mayor seguridad, por si logran romper el esquema de ocultamiento.

Con este ejemplo, se puede notar la diferencia sutil de como ocultan la información estás dos disciplinas. Podemos concluir, que el objetivo de la esteganografía es pasar desapercibida y el de la criptografía es evitar ser decodificada (o descifrada).

2.11. Diferencia entre encriptar y cifrar

Cripta viene del latín crypta, que significa ocultar. Así encriptar significa, poner en oculto, es decir, ocultar. Y la criptología, sería la ciencia de la ocultación. El origen de la palabra “cifrar” se encuentra en el latín, que a su vez proviene del árabe sifr que hace referencia a cualquier dígito.

Es decir que encriptar es ocultar, mientras que cifrar es hacer referencia a cualquier digito. El cifrado es solo una de las tecnologías que se pueden usar para la encriptación. Los datos se pueden

ocultar mimetizándolos, o simplemente sin cifrarlos, pero poniéndolos en un lugar oculto. Por mencionar solo dos maneras de encriptación que no serían cifrado de datos. (Fernandez, 2018)

2.12. Imágenes digitales

Debido a que en la actualidad toda la información está pasando por un proceso de digitalización, y las imágenes no son ajenas a este procedimiento, es necesario comprender como están compuestas las imágenes digitales, que es un megapíxel, puntos por pulgada, profundidad de color, etcétera.

Cuando generamos imágenes, tomando fotos o escaneamos un documento, se tiene que tomar algunas decisiones para alcanzar un compromiso entre la calidad de la imagen y el tamaño del archivo. Para tomar dichas decisiones hay que tener claros algunos conceptos básicos, comenzando por los tipos de imágenes que se pueden generar.

2.13. Tipos de imágenes digitales

Existen dos tipos de imágenes digitales, cada una de estas imágenes se produce y edita con programas diferentes y tiene aplicaciones diferentes. Se debe comprender en qué se diferencian y cuáles son las ventajas e inconvenientes de cada una.

2.13.1. Imágenes vectoriales

Las imágenes vectoriales están compuestas por entidades geométricas simples: segmentos y polígonos básicamente (de hecho, una curva se reduce a una sucesión de segmentos). Cada una de estas entidades está definida matemáticamente por un grupo de parámetros (coordenadas inicial y final, grosor y color del contorno, color del relleno, etc.) Por compleja que pueda parecer una imagen, puede reducirse a una colección de entidades geométricas simples. (CAD, s.f.)

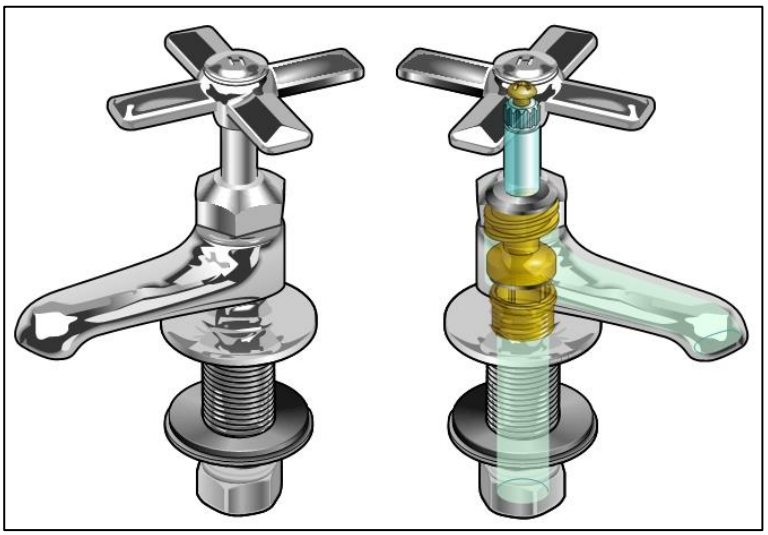


Figura 15. Ejemplo de imagen vectorial
Fuente: (CAD, s.f.)

En la Figura 15 se muestra un ejemplo de imagen vectorial. Al estar compuestas por entidades geométricas simples se pueden cambiar de escala, para ampliarlas o reducirlas, sin que la imagen pierda calidad. La Figura 16 obtenida haciendo zoom sobre la Figura 15 sin perder calidad en los bordes de la imagen tenemos mucho más detalle sobre el sistema de fijación de la cruceta al eje del grifo.

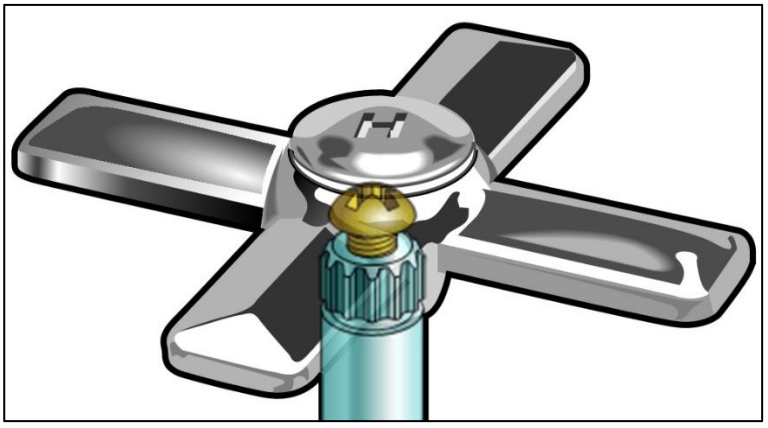


Figura 16. Zoom de la imagen vectorial sin afectar su calidad
Fuente: (CAD, s.f.)

Los programas utilizados para realizar esta clase de imágenes son: Corel Draw, Illustrator, que forma parte del producto Creative Suite de la empresa Adobe, el preferido por los profesionales del diseño gráfico. Una prometedora alternativa, en el mundo del software libre, se llama Sodipodi y, de momento, sólo está disponible para plataformas Linux. (CAD, s.f.)

2.13.2. Imagen bitmap

Las imágenes de mapa de bits están construidas mediante una gran cantidad de pixeles, cada uno de estos está relleno de un color uniforme, pero la sensación obtenida es el resultado de integrar visualmente, en la retina, las variaciones de color y luminosidad entre píxeles vecinos.

La unidad básica que compone una imagen es el denominado píxel que proviene de "PICture ELement" (*elemento de imagen*) los cuales están perfectamente alineados en columnas y filas. (Rodríguez). En la Figura 17 se muestra un ejemplo de imagen bitmap.

Figura 17. Ejemplo de imagen tipo mapa de bits (bitmap)
Fuente: (CAD, s.f.)

Las imágenes de mapa de bits son llamadas también bitmap, son una alternativa ideal para reproducir objetos sutilmente iluminados y con gran variación tonal. Es el tipo de imagen utilizado

para la fotografía y el cine. La calidad de la imagen dependerá de la cantidad de píxeles utilizados para representarla.

Las imágenes bitmap no permiten el cambio de escala. Al hacer zoom sobre las flores de la Figura 17: los píxeles son evidentes y la representación es totalmente irreal. El efecto se conoce como pixelado, se hace más evidente en las líneas curvas y en las zonas en las que hay cambios bruscos de luminosidad. En la Figura 18 se muestra el resultado del zoom sobre la Figura 17.

Figura 18. Imagen bitmap pixelada debido al cambio de escala
Fuente: (CAD, s.f.)

Los programas más utilizados para generar, o editar, este tipo de imágenes bitmap son Photoshop, Photopaint. Existe una alternativa de software libre llamada The Gimp, un programa excelente, potente y profesional. Las imágenes vectoriales son ideales para cartelería, diseño de envases, imagen corporativa, logotipos etc., es decir en todas aquellas situaciones en las que una misma imagen, hecha con una gama reducida de tintas planas, debe ser reproducida en distintos soportes y a distintos tamaños. (CAD, s.f.)

Las imágenes en mapa de bits, son perfectas cuando la gama de colores cambia sutilmente. En este caso, la imagen debe generarse teniendo muy en cuenta dónde y cómo va a mostrarse, con una cantidad de píxeles y una gama de colores adaptados al soporte en el que va a reproducirse. Una vez hechas las modificaciones se tendrá pérdida de calidad. (CAD, s.f.)

2.14. Parámetros de la imagen

Sabiendo que una imagen digital es el archivo informático resultante de una discretización de una imagen, natural o sintética, en elementos de imagen, llamados píxeles. Para lograr escanear o digitalizar una fotografía, puede describirse como una función continua $F(x, y)$, denominada imagen, donde las coordenadas x, y son variables espaciales y la función valor (amplitud) es la densidad. Esta función es además el producto de dos funciones separadas: Una función es la de iluminación I, mientras que la otra función describe las propiedades del objeto que está siendo iluminado, conocida como reflexión R. En realidad, para poder obtener la imagen digital la función continua debe estar discretizada, tanto en las variables espaciales como en la amplitud. La función discreta resultante $f(x, y)$ se denomina imagen digital. El proceso de discretizar las variables espaciales $\Delta x, \Delta y$ se conoce como muestreo y la discretización de la amplitud g como cuantificación. (Aguilera, 2010). El elemento discreto $\Delta x, \Delta y$ es el píxel y Δg es un nivel de gris, denominado informalmente brillo. Así pues, una imagen digital puede expresarse por lo expuesto en la ecuación 2:

$$f\ (\Delta x \cdot i, \Delta y \cdot j, i = 0, \dots, N-1; j = 0, \dots., M-1)$$

Ecuación 2. Modelo para expresar una imagen digital

Siendo i, j la dirección del píxel, N el número de filas y M el número de columnas. La función imagen se escribe normalmente como $f(x, y)$. Hay que tener en cuenta que las variables espaciales son valores discretos, usualmente valores enteros. La cuantización de la imagen asignará a cada localización discreta (x, y) un valor entero 2^b, con b siendo valores de: 2, 4, 8, 12, 16 o 32 bits por píxel. De esta forma la resolución radiométrica describirá el número de bits por píxeles en una imagen.

Existen varios parámetros estadísticos útiles para describir la distribución de los valores de pixeles; sirven para su análisis, modificación y manipulación, tales parámetros como la desviación estándar, media, histograma, son de gran importancia al momento de hacer un análisis a las imágenes digitales.

2.14.1. Media

"Es el nivel de gris medio en el caso de imágenes en escala de grises y nivel medio de color en imágenes RGB, indica la luminosidad o brillo de una imagen." (Aguilera, 2010)

2.14.2. Desviación estándar

"Medida del contraste o variación de la información dentro de la imagen. Si la imagen tiene poco contraste o poca información, el valor de la desviación será pequeño, caso contrario el valor será alto." (Aguilera, 2010)

2.14.3. Histograma

Es una representación gráfica de una imagen, permite observar la distribución de valores de pixeles o niveles de color y la variación o contraste en la imagen. Según (Aguilera, 2010), "es la curva que a lo largo de uno de sus ejes representa cada uno de los posibles niveles de gris o de

color si es el caso, mientras que en el otro eje muestra su frecuencia relativa de aparición en la imagen analizada.” Para generar el histograma es necesario contar con el valor de cada pixel que presenta la imagen. Una imagen con tonos oscuros genera un histograma que tiende a la izquierda, y tonos claros tiende a la derecha. (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016). Un histograma de imágenes a color tiene tres curvas, y tiene un rango de niveles de intensidad de 0 a 255 (8 bits) si se hace referencia al modelo RGB24.

2.15. Mediciones de la calidad de la imagen

Las imágenes digitales al estar expuestas a modificaciones e inserción de distorsiones, provocadas por el procesamiento, manipulación (transformación) y transmisión. Dan a lugar a posible ataques estegoanalíticos visuales, ya que su calidad se verá afectada, es por esto que surge la necesidad de evaluar (cuantificar) la calidad visual de las imágenes utilizando una métrica estandarizada. Este tipo de mediciones se las realiza al comparar la imagen original con la modificada.

2.15.1. RMSE (Root Mean Square Error)

Es una medida objetiva de la calidad de la imagen, la cual se obtiene mediante el cálculo de la raíz cuadrada de la diferencia cuadrática media entre los valores de los píxeles de la imagen a evaluar y la imagen referencia, este valor representa un error, por lo que un menor valor demuestra mayor similitud de las imágenes y por ende mejor calidad.

2.16. Capacidad de incrustación

Para ocultar información el principal problema es la capacidad de incrustación, debido a que, al ocultar una imagen dentro de otra imagen portadora, es necesario que ambas tengan las mismas

características, si tienen diferente tamaño se debe comprimir una de las imágenes antes del proceso de incrustación. Pero, al comprimir las imágenes se ocasionan distorsiones y pérdidas, esto perjudica los resultados finales. (Cristian Marcelo Vasco Estupiñan, Freddy Roberto Acosta Buenaño., 2018)

2.17. Esteganografía

Viene de un vocablo griego que significa “escritura oculta”, por lo que se la conoce como “la ciencia de ocultar mensajes en un objeto portador”. (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

El objeto portador puede ser imágenes, videos, audio, etcétera. El objetivo principal de la esteganografía es lograr una comunicación confidencial y segura, permitiendo que la información oculta solo pueda visualizarse por el receptor al que va dirigido el mensaje. (Ya-Lin Lee, Wen-Hsiang Tsai, 2014)

2.17.1. Tipos de técnicas esteganográficas en imágenes

En la Figura 19 se muestran algunas de las técnicas esteganográficas que se pueden utilizar en imágenes.

Figura 19. Tipos de técnicas esteganográficas en imágenes
Fuente: (C.P.Sumathi, T.Santanam, G.Umamaheswari, 2013)

2.17.2. Esteganografía en el dominio espacial

Son técnicas de baja complejidad, las cuales ocultan en los valores de los pixeles de la imagen la información secreta, es decir que se modifican ligeramente los pixeles de la imagen para ocultar un mensaje. Algunas de estas técnicas son:

A. Sustitución del Bit Menos Significativo

"Consiste en sustituir el bit menos significativo de cada píxel por el bit del mensaje oculto, se lo realiza transformando el mensaje a ocultar en un flujo de bits y la imagen portadora en matrices de bits, 8 bits para cada píxel de imágenes en escala de grises y 24 bits para imágenes RGB. Tiene gran cantidad de incrustación, pero es susceptible a pérdidas de información por modificaciones en la imagen portadora ya sea debido a compresión o recorte." (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

B. Diferencia de valores de píxel

"Consiste en dividir a la imagen portadora en bloques de dos pixeles consecutivos y evaluar la diferencia entre ellos lo cual determina el número de bits que se pueden incrustar en el par de pixeles. Utiliza los bordes, debido a que la vista de los seres humanos es más sensible a variaciones de la imagen en zonas lisas mientras que es más difícil que se detecte alteraciones en bordes." (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

C. Modificación de niveles de grises

"Consiste en realizar un mapa de la imagen portadora modificando el valor de niveles de grises en los pixeles. Se usan los números pares e impares y se selecciona mediante funciones matemáticas ciertos bits dentro de la imagen, los cuales se comparan posteriormente con el flujo

de bits mapeado en la imagen. Tiene una gran capacidad de incrustación y baja complejidad de procesamiento.” (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

D. Uso de textura

“Consiste en sustituir bloques de pixeles, el primer paso divide la imagen portadora y la imagen secreta en pequeños bloques del mismo tamaño. En cada bloque de la imagen secreta se determina un patrón de textura y se compara con los bloques de la imagen portadora, se busca el más similar para reemplazarlo, finalmente crea una nueva imagen con la menor distorsión posible.” (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

E. Esteganografía basada en bordes

“Consiste en utilizar la técnica LSB, pero no se oculta información en todos los pixeles, únicamente se utilizan aquellos que corresponden a bordes. Tiene baja capacidad de incrustación, utiliza los 3 bits menos significativos de cada píxel.” (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

En la Tabla 1 se muestra un resumen acerca de las ventajas y desventajas de las técnicas esteganográficas en el dominio espacial.

Tabla 1

Tabla resumen de las técnicas esteganográficas en el dominio espacial

Ventajas	Desventajas
Gran capacidad de incrustación	Susceptibilidad a pérdidas de información por manipulación de la imagen
Menor degradación de la calidad en la imagen original	Mas vulnerabilidad a ataques sencillos
Bajo procesamiento matemático	

Fuente: (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

2.18. Imágenes como medio portador dentro de la esteganografía

Al considerar a las imágenes digitales como un medio portador de información, a través del uso de la esteganografía, es importante conocer el modelo RGB (Red, Green, Blue) el cual se ilustra en la Figura 20. El modelo RGB sirve para definir un color de 16’777.216 posibles, esto mediante la combinación de 3 valores en el rango de 0 hasta 255 asignados a cada tono (rojo, azul y verde).

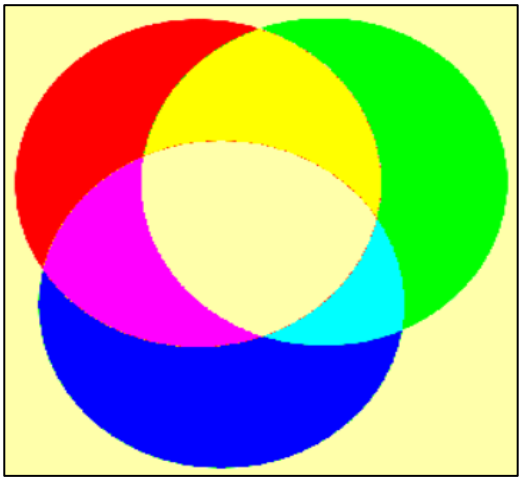


Figura 20. Estructura del modelo RGB
Fuente: (CAD, s.f.)

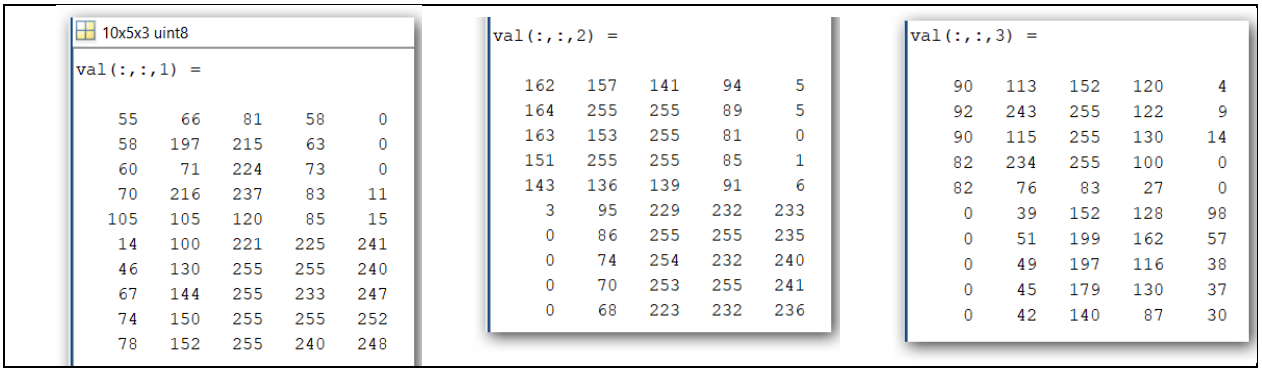
En la Tabla 2, se encuentra detallado como se calculan algunos colores en base al modelo RGB.

Tabla 2
Valores del modelo RGB para generar colores básicos

Color	R	G	B
Blanco	255	255	255
Rojo	255	0	0
Verde	0	255	0
Azul	0	0	255
Amarillo	255	255	0
Negro	0	0	0

Al utilizar el modelo RGB, se puede analizar una imagen digital como una matriz de 3 dimensiones por n filas y m columnas, en el caso de imágenes a color y de una dimensión por n filas y m columnas en el caso de imágenes a blanco y negro. Las columnas representan la numeración de los pixeles en el eje x (ancho de la imagen), y las filas la numeración de los pixeles ubicados en el eje y (alto de la imagen), la otra dimensión corresponderá al color del modelo, los valores que tendrá cada elemento de la matriz van a variar desde 0 hasta 255. Para comprender de mejor manera el procedimiento para analizar una imagen digital, en la Figura 21, se puede ver una imagen que tiene 5 pixeles de ancho y 10 de largo, en la cual se observan diferentes colores y al "leer" la imagen con Matlab® nos entrega la información mostrada en la Figura 22.

Figura 21. Imagen (5 pixeles de ancho x10 pixeles de alto) con modelo RGB



10x5x3 uint8

val(:,:,1) =

55	66	81	58	0
58	197	215	63	0
60	71	224	73	0
70	216	237	83	11
105	105	120	85	15
14	100	221	225	241
46	130	255	255	240
67	144	255	233	247
74	150	255	255	252
78	152	255	240	248

val(:,:,2) =

162	157	141	94	5
164	255	255	89	5
163	153	255	81	0
151	255	255	85	1
143	136	139	91	6
3	95	229	232	233
0	86	255	255	235
0	74	254	232	240
0	70	253	255	241
0	68	223	232	236

val(:,:,3) =

90	113	152	120	4
92	243	255	122	9
90	115	255	130	14
82	234	255	100	0
82	76	83	27	0
0	39	152	128	98
0	51	199	162	57
0	49	197	116	38
0	45	179	130	37
0	42	140	87	30

Figura 22. Valores generados al leer la imagen mostrada en la Figura 21.

Al ver que la imagen a ser analizada no se comporta de una manera ideal, a pesar de haberla editado píxel a pixel, surge la necesidad de comprender cuales son los formatos de compresión de las imágenes, sus características, ventajas y desventajas.

2.19. Compresión de imágenes digitales

El archivo creado después de la generación de una imagen digital contiene la información de cada píxel, además de una cabecera para información destinada al programa encargado de abrir la imagen y mostrarla en el monitor. Todos los archivos gráficos, suelen tener tamaños muy grandes. Este gran consumo de espacio en disco hizo necesario el desarrollo de tecnologías capaces de comprimir archivos gráficos.

"Cada sistema de compresión utiliza un algoritmo matemático propio para reducir la cantidad de bits necesarios para describir la imagen, y marca el archivo resultante con una extensión característica: bmp, wmf, jpg, gif, png, etcétera." (CAD, s.f.) Estos sistemas se distinguen entre sí por las pérdidas producidas en la información de la imagen durante el proceso de compresión. Así pues, hay algoritmos con pérdidas y sin pérdidas.

2.19.1. Formato JPG (Joint Photographic Experts Group)

Este es un formato de compresión con pérdidas, en el proceso de compresión desecha en primer lugar la información no visible, por lo que las pérdidas apenas son perceptibles. Su algoritmo está basado en el hecho de que el ojo humano percibe peor los cambios de color que las variaciones de luminosidad por lo cual divide la información de la imagen en dos partes: color y luminosidad; y las comprime por separado. Admite modos en escala de grises con una profundidad de 8 bits y en

color hasta 24 bits. Permite la carga progresiva en un navegador, lo que lo ha convertido en el formato estándar en la web. No es adecuado para imágenes con alto contraste de color.

Se debe tomar en cuenta que la compresión se produce automáticamente cada vez que se guarda el archivo, por lo que es aconsejable guardar en este formato una única vez.

2.19.2. Formato GIF (Graphics Interchange Format)

Este formato devuelve imágenes de tamaño muy reducido. Esa reducción se consigue indexando los colores, es decir, asimilándolos a uno de los 256 colores de su tabla. Su profundidad de color máxima, por tanto, es de 8 bits. Este formato permite hacer transparente uno de los colores indexados en la tabla, lo que permite suprimir fondos. También permite enlazar varias imágenes gif en una secuencia, lo que se conoce con el nombre gif animado.

Al tener un pequeño tamaño hizo que fuera el formato más extendido en los primeros tiempos de Internet. Pero su principal defecto es que es un formato propietario (CompuServe Inc.), lo que ha provocado la aparición del formato libre png que, además, comprime mejor que gif.

2.19.3. Formato PNG (Portable Network Graphics)

Es el formato de más rápido crecimiento en la web, porque reúne lo mejor de jpg y gif. Es un formato de compresión sin pérdidas, con una profundidad de color de 24 bits. Soporta hasta 256 niveles de transparencia, lo que permite fundir la imagen perfectamente con el fondo. Uno de sus inconvenientes es que no soporta animaciones y que el tamaño de los archivos png, debido a la capa de transparencia, siempre es mayor que el de los archivos jpg.

2.20. Audio como medio portador dentro de la esteganografía

De la misma manera en que las imágenes están sufriendo un proceso de digitalización en la era actual, el audio que es una señal analógica de origen, puede digitalizarse y no escapa del hecho de que se podría incrustar información en estos archivos.

El sonido es una variación de la presión ambiental la cual se propaga en forma de onda a través del aire. Tiene cuatro características que lo definen: amplitud, longitud de onda, período y frecuencia, como se muestra en la Tabla 3.

Tabla 3
Definición de características del sonido

Característica	Definición
Amplitud	Distancia máxima que pude alcanzar una onda con respecto a su posición de equilibrio.
Longitud de onda	Distancia que existe entre dos puntos que se encuentran en el mismo estado de vibración (crestas o valles)
Cresta	Es el punto en donde la amplitud de la señal es máxima y por encima de su eje de equilibrio
Valle	Representa el lugar donde la amplitud es máxima pero que se encuentra por debajo del eje de equilibrio
Periodo	Es el tiempo que requiere la onda en viajar una longitud de onda
Frecuencia	Representa la cantidad de variaciones u oscilaciones que presenta una onda en un período de tiempo

Fuente: (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018)

Para implementar esteganografía en audio es necesario utilizar el archivo de audio como portador de la información secreta, el cual puede ser cualquier tipo de archivo, se debe manejar correctamente de la información considerando la existencia de bits redundantes, estos bits duplican una porción de información y modificarlos no afecta la calidad del archivo portador ni compromete la técnica esteganográfica. (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018)

2.21. Técnicas de esteganografía en audio

De la misma forma que en las imágenes digitales, en los archivos de audio se puede aplicar técnicas esteganográficas, y estas tienen diferentes características.

2.21.1. Codificación del bit menos significativo

Esta es la técnica más sencilla que existe, a pesar de esto tiene resultados que demuestran su eficiencia al reducir la degradación de la información oculta. Su fundamentación es la misma que la expresada en la Sección 2.17.2 del capítulo 2 del presente trabajo de investigación.

2.22. Formatos de Audio

Es importante analizar cuáles son los formatos en los cuales la información de audio digitalizada se almacena, sus características, ventajas y desventajas. A continuación, algunos de ellos:

2.22.1. Formato WAV (Waveform Audio File)

Es un formato desarrollado por Microsoft e IBM, el cual no comprime los datos, esto permite tener alta calidad, es uno de los formatos más utilizados a nivel profesional. Permite generar audio mono canal y estéreo. Su frecuencia de muestreo puede ser 22050 Hz hasta 44100 Hz que es la más utilizada.

2.22.2. Formato WMA (Windows Media Audio)

Es un formato desarrollado por Microsoft pero que, si maneja compresión de datos, por lo que su principal ventaja es ocupar menor espacio de almacenamiento, su desventaja es la calidad, ya que disminuye a causa de la compresión. Maneja mono canales y canales estéreo, cuenta con una frecuencia de muestreo entre los 44100 Hz a los 48100 Hz. (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018)

2.22.3. Formato MP3 (MPEG Audio Layer III)

Surge de la necesidad de almacenar mayor cantidad de archivos de audio y en el mismo espacio de almacenamiento. “El formato se encargó de eliminar las porciones de información que eran irrelevantes para el oído humano, como por ejemplo los rangos de frecuencia mayores a 20 kHz y menores a 20 Hz, con esto logra archivos con tamaño menor.” (Carlos Eduardo Rodríguez Guayaquil, Freddy Acosta B., 2016)

2.23. Video como medio portador dentro de la esteganografía

En las Secciones 2.16 y 2.20 del capítulo 2 del presente trabajo de investigación, se analiza la capacidad de las imágenes y el audio para convertirse en un medio portador de mensajes secretos, es decir la aplicabilidad de técnicas esteganográficas en imágenes y audio. Y debido a que un video está compuesto por una secuencia de imágenes y un audio se puede concluir que puede ser utilizado como medio portador de alguna técnica esteganográfica. Para lograr este cometido es importante analizar los formatos de manejan los archivos multimedia de video, su compresión, características y métodos de análisis.

2.23.1. Componentes del Video

Fundamentalmente los videos están compuestos por una parte visual y otra auditiva, esto viene a ser las imágenes y el audio.

Un aspecto para tomar en cuenta es el sincronismo de la secuencia de imágenes con la reproducción del audio, el desarrollo tecnológico permite un procesamiento, sincronismo, creación y edición de videos sencillo.

Algo importante a definir es el frame o conocido como fotograma o cuadro, es un componente de la secuencia de imágenes obtenidas del video, la frecuencia de muestreo de dichas imágenes es la que genera la sensación de movimiento. Es decir, es una imagen particular dentro de una sucesión de imágenes que componen una animación. Del mismo concepto surge el *frame rate* que vendría a ser la tasa de cuadros que se transmiten/capturan en un segundo, por lo cual se mide en fps (*frames per second).* En la Figura 23 se observa un ejemplo de cómo se visualiza una animación con diferente fps.

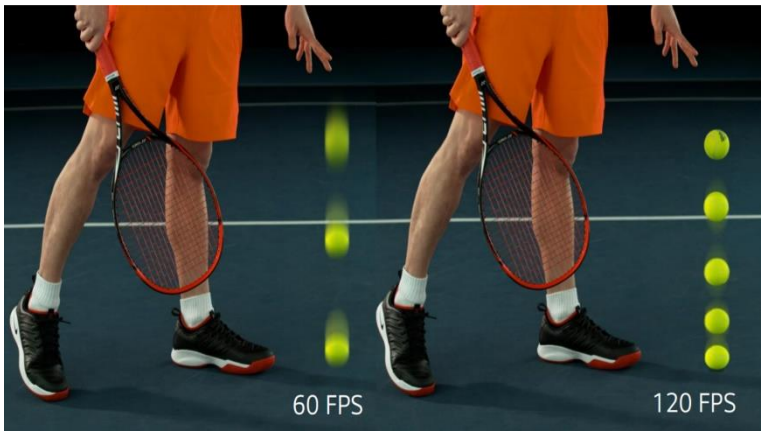


Figura 23. Ejemplo de una imagen capturada a una tasa de 60 y 120 fps
Fuente: (London, 2018)

2.24. Formatos de Video

De la misma manera que las imágenes digitales y el audio, los video tienen algunos formatos que pueden ser utilizados, estos se detallan a continuación:

2.24.1. Formato AVI (*Audio Video Interleaved)*

Sus siglas en español significan audio y video intercalado, es un formato contenedor de audio y video. El formato concreto de estos flujos no es objeto del formato AVI y es interpretado por un

programa externo denominado códec. Es decir, el audio y el video contenidos en el AVI pueden estar en cualquier formato (AC3/DivX, u MP3/Xvid, entre otros). Por eso se le considera un formato contenedor. Este formato tiene alta calidad de imagen y sonido, pero el tamaño de los archivos es bastante grande por lo que ocupa gran capacidad de almacenamiento. (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018)

2.24.2. Formato MPEG (*Moving Pictures Expert Group*)

"Es el formato estándar para la compresión de archivos en video digital, admite diversos tipos de códec's de video como: MPEG-1 (Calidad CD), MPEG-2 (Calidad DVD), MPEG-3 (Calidad orientada para audio MP3) y MPEG-4 (Utilizado para videos en la web)." (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018)

2.24.3. Formato MOV

"Es un formato desarrollado por la empresa Apple, tiene un códec de video propio, el cual maneja una serie de actualizaciones en tiempos cortos, estas actualizaciones permiten que el manejo de videos en internet sea efectivo por motivo de su calidad y peso. Este formato fue diseñado para admitir streaming." (Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy., 2018)

2.24.4. Formato WMV (*Windows Media Video*)

Es un formato desarrollado por Microsoft, tiene alta calidad de imagen y poco espacio de almacenamiento, este formato es capaz de manejar streaming.

Es importante tomar en cuenta que, los archivos de video están compuestos por un contenedor y un contenido. El contenedor guarda distintos tipos de datos, entre ellos el video, el audio,

subtítulos y metadatos que sirven para sincronizar el video y el audio, activar unas pistas de audio o texto y desactivar otras. El códec es el encargado de descifrar y descomprimir la información que hay en esa corriente de unos y ceros. Un buen códec comprime la información lo máximo posible sin que el video final pierda calidad.

El contenedor o formato del archivo de video como por ejemplo: .mp4, .avi, .mkv, .mov: pueden contener información codificada con diferentes códecs.

Se debe tomar en cuenta que no todos los códecs son compatibles o pueden formar parte de un formato o tipo de contenedor.

CAPITULO 3

3. DISEÑO DEL PROGRAMA

3.1. Descripción general

El algoritmo consiste en combinar un método de transformación de imágenes que modifica sus características de color con un método para ocultar información en el audio. Esto implementado en un video.

Para cumplir con el propósito del trabajo de investigación, de manera resumida se podría decir que se han ejecutado las siguientes acciones:

1. Definir el video portador de la información.
2. Definir las imágenes secretas.
3. Convertir el video portador a formato AVI.
4. Descomponer el video portador.
5. Detectar cambios de escena en la secuencia de fotogramas.
6. Identificar las imágenes portadoras.
7. Definir el par imagen portadora / imagen secreta más apto.
8. Transformar la imagen secreta en la imagen objetivo/portadora.
9. Organizar los datos para la recuperación de la imagen secreta.
10. Incrustar los datos en el audio del video portador.
11. Construir el estego-video.
12. Recuperar la información oculta.

3.2. Definición del video portador de la información

Para elegir el video portador de la información es importante tomar en cuenta las siguientes características:

a. Resolución de 1920 x 1080 pixeles
b. Duración mayor o igual a 30 segundos
c. Contenido de interés y que llame la atención

Tomando en consideración estos criterios se ha decidido elegir el video "Himno a la Universidad de las Fuerzas Armadas ESPE" el cual está cargado en la plataforma YouTube. Es importante indicar que de ser necesario modificar la duración del video se puede utilizar la herramienta disponible en la web: https://online-video-cutter.com/es/ o https://www.onlinevideoconverter.com/es/mp3-converter. En el presente trabajo se recortó al video original un total de 2 segundos, debido a que al final del video se tenían 2 segundos de pantalla negra para indicar el fin del video, estos dos segundos de exceso de información implicarían el análisis de 48 fotogramas más, por lo que se ha tomado la decisión de retirarlos.

3.3. Definición de las imágenes secretas a ser ocultas

Las imágenes a ser ocultas deben tener un propósito, razón por la cual se han definido imágenes con temas sobre:

a. Rutas de movilización desde el palacio de Carondelet
b. Rutas de transporte desde cuarteles
c. Fotos de personas buscadas por la policía nacional
d. Retratos hablados

e. Fotos de operaciones contra el narcotráfico

f. Fotos de grupos paramilitares

g. Imágenes de uso comercial exclusivo

Por ejemplo, en las Figuras 24 y 25 se tiene rutas de movilización desde el palacio de Carondelet y de los cuarteles cercanos.

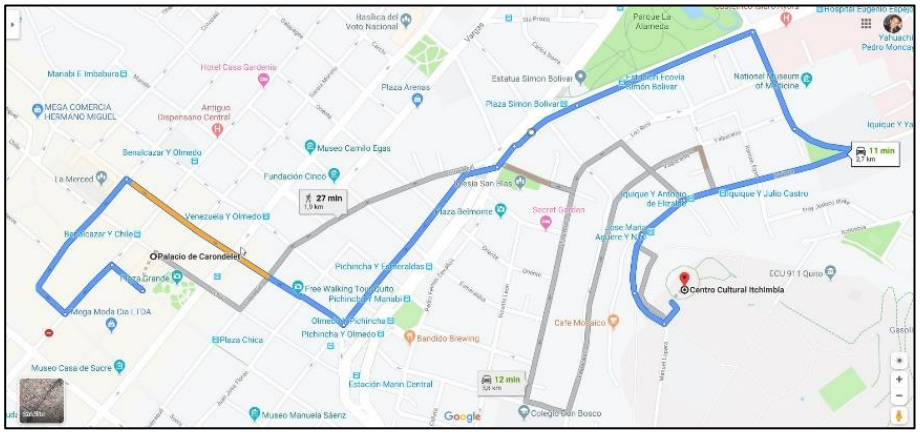


Figura 24. Imagen secreta sobre movilización desde Carondelet

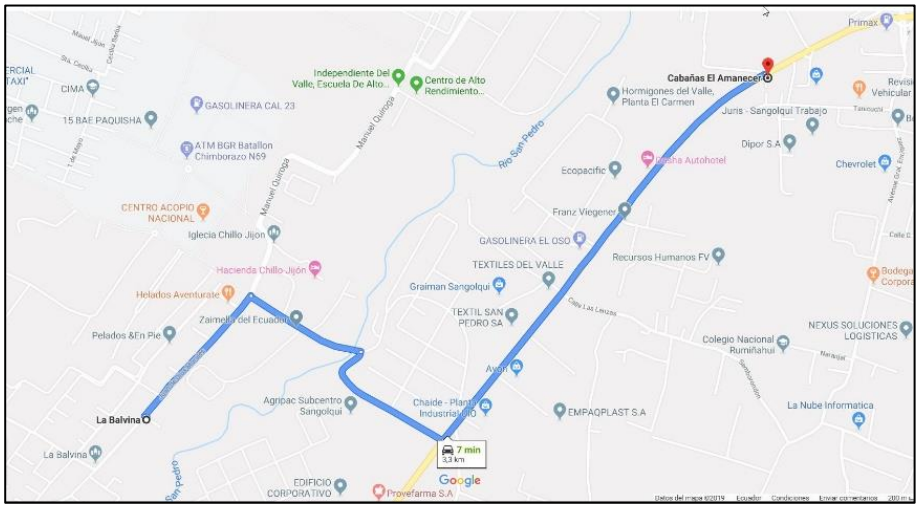


Figura 25. Imagen secreta sobre ruta de transporte desde cuarteles

En las Figuras 26 y 27 se tienen fotos sobre personas buscadas por las autoridades y retratos hablados de las mismas.

Figura 26. Imagen secreta sobre personas buscados por las autoridades

Figura 27. Imagen secreta sobre retratos hablados

3.4. Conversión del video portador, desde su formato original a formato AVI

Para la conversión del video portador, se lograron definir tres métodos:

a. Método usando el programa VLC media player

Con el programa en su versión 3.0.7.1 se puede convertir un video de formato MP4 a formato AVI, fácilmente.

b. Método desarrollado en la herramienta Matlab®

Con el código presentado en la Figura 28, la herramienta Matlab® a través de un script puede convertir un video en formato MP4 a un video en formato AVI. Para poder convertir el archivo multimedia en Matlab®, es necesario ejecutar el script tomando en cuenta que deben estar dentro de la misma carpeta el archivo original y el script desarrollado.

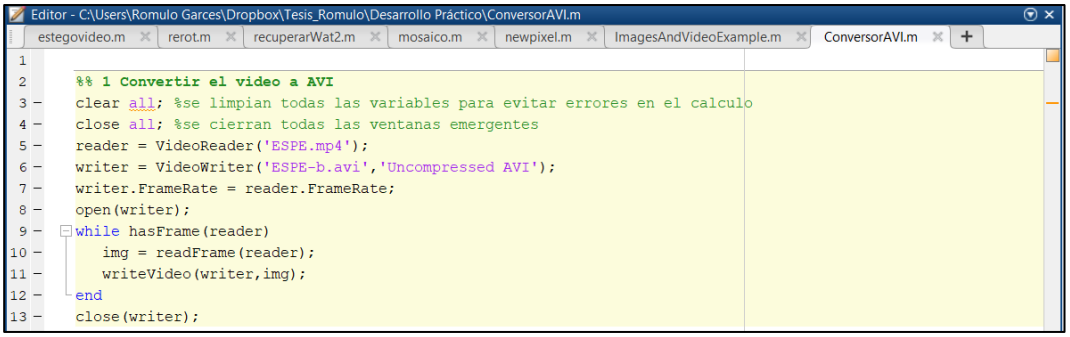


Figura 28. Programa de conversión de formato desarrollado en Matlab®

c. Método usando una herramienta web

En el siguiente link: https://video.online-convert.com/es/convertir-a-avi se dispone de una herramienta en línea que permite convertir archivos de vídeo a AVI de alta calidad útil para convertir videos de formato MP4. Además, con la siguiente página web: https://www.clipconverter.cc/, se han realizado las respectivas pruebas de conversión y se han logrado los mejores resultado de entre todos los métodos.

3.5. Descomposición del video portador de la información

La descomposición del video portador se la realiza con la herramienta Matlab® la cual permite manipular de una manera correcta la información, por su capacidad de procesamiento y además ayuda con el manejo de señales que, en este caso, vendrían a ser señales de audio e imágenes.

Para la descomposición del video portador se ha desarrollado un programa que utiliza la función *audioread* con la cual se extrae el audio del video portador, después se utiliza la función *audiowrite* con la cual se genera el archivo de audio en formato WAV como se muestra en la Figura 29.

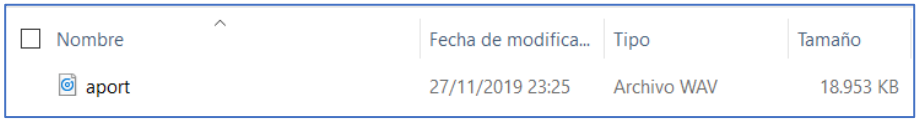


Figura 29. Archivo generado por la descomposición del video

El archivo de audio con formato WAV contiene el fondo musical del video portador. Una vez se ha separado el audio del video portador, es necesario obtener la base de datos de los fotogramas que componen el video. Para obtener los fotogramas que componen el video se debe utilizar la función *VideoReader*. En el Anexo 1, se puede observar como se ha ido desarrollando el programa.

Una vez creado el objeto con la función *VideoReader* el cual tiene las propiedades de un objeto de video, se han extraído del archivo multimedia de video los fotogramas que componen la secuencia visual y se ha creado una base de datos (una serie de imágenes) en la carpeta seleccionada, como lo indica la Figura 30.

El número de fotogramas que se han de generar depende directamente de la duración del video y de tasa de fotogramas por segundo (fps). Para este caso en particular Matlab®, con ayuda del método “NumberOfFrames” correspondiente al objeto tipo video permite identificar cuantos

fotogramas se han de generar, que son 2639. Esta cantidad coincide con los esperado, ya que por definición se debería tener tantos fotogramas como sea el resultado de multiplicar la tasa de fotogramas por segundo, y la duración del video en segundos, como se indica en la ecuación 3.

$$fotogramas = \text{fps x duración} = 23.976 \left(\frac{\text{frames}}{\text{segundo}}\right) \text{x } 110.0683 \text{ (segundos)} \cong 2639$$

Ecuación 3. Cálculo de fotogramas que componen el video

Una vez ejecutado esta sección del programa el resultado será una carpeta con los fotogramas originales del video portador, con un ancho y alto correspondiente a la resolución del video portador (1920 x 1080). En la Figura 30 se muestra cómo se han generado un total de 2639 imágenes en formato jpg, las cuales corresponden a todos los fotogramas que componen la secuencia de video.

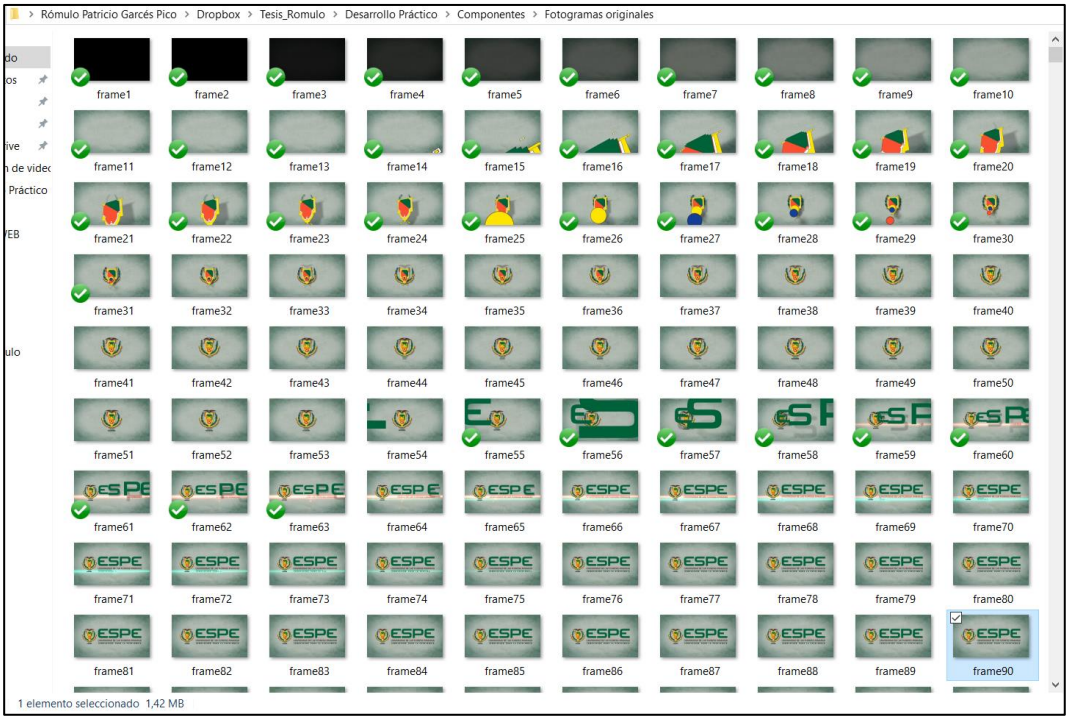


Figura 30 Carpeta donde se almacenan los 2639 fotogramas del video portador

3.6. Detección de cambios de escena en la secuencia de fotogramas

Para detectar automáticamente los cambios de escena del video portador, se ha desarrollado un algoritmo en base al SSIM que sirve para medir la similitud de una imagen en comparación a una imagen de referencia. Para lograr detectar los cambios de escena, se ha calculado el valor del "Índice de similitud estructural" (SSIM) de los fotogramas consecutivos.

Primeramente, se establece un laso que va a ejecutar la comparación desde el fotograma 1 hasta el penúltimo fotograma del video portador, compara cada fotograma con el siguiente correspondiente de la secuencia. El SSIM al ser una métrica de calidad de imagen que evalúa el impacto visual de tres características: luminancia, contraste y estructura, es una evaluación exhaustiva, que implica el uso de gran cantidad de recursos del computador, por lo tanto, es considerable el tiempo que demora en ejecutarse, se han realizado algunas pruebas para determinar cuál es la mejor manera de implementar esta comparación.

Para reducir el tiempo de procesamiento del programa se toma una muestra de cada fotograma, esto se lo realiza considerando la proporción aurea, la cual indica lo siguiente: "Lo pequeño es a lo grande como lo grande es al todo", este concepto realza la armonía de los objetos, del diseño o la arquitectura. En la Figura 31 se observa donde está ubicado uno de los puntos áureos de la imagen.

Figura 31 Ejemplo de proporción aurea en una imagen
Fuente: (Vidal, s.f.)

La proporción aurea también se la conoce como la divina proporción, la cual tiene una estrecha relación con la sucesión de Fibonacci, descubierta gracias a Leonardo Pisano, también conocido como Fibonacci. En la Figura 32 se muestra un ejemplo del punto áureo de la imagen mostrada.

En la Sucesión de Fibonacci (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, etc.) la suma de dos números consecutivos siempre da como resultado el siguiente número (1+1=2; 13+21=34). La división entre cada pareja de números consecutivos se aproxima al número áureo (1,618034).

Para poder encontrar esta muestra, se detectan los puntos áureos o puntos de interés, después de esto se dibuja una cuadrícula para identificar cual es la mejor muestra del fotograma, con la cual se podrá comparar la mayor cantidad de información. En el arte se utilizan estos cuatro puntos áureos para ubicar en ellos el centro de atención de la composición, logrando crear una imagen equilibrada. Comúnmente el objeto principal es colocado en alguno de los puntos áureos, y si hubiese otro, se coloca en el punto opuesto diagonal. En la Figura 32 se ha encontrado uno de los 4 puntos áureos para proceder a dibujar la cuadricula.

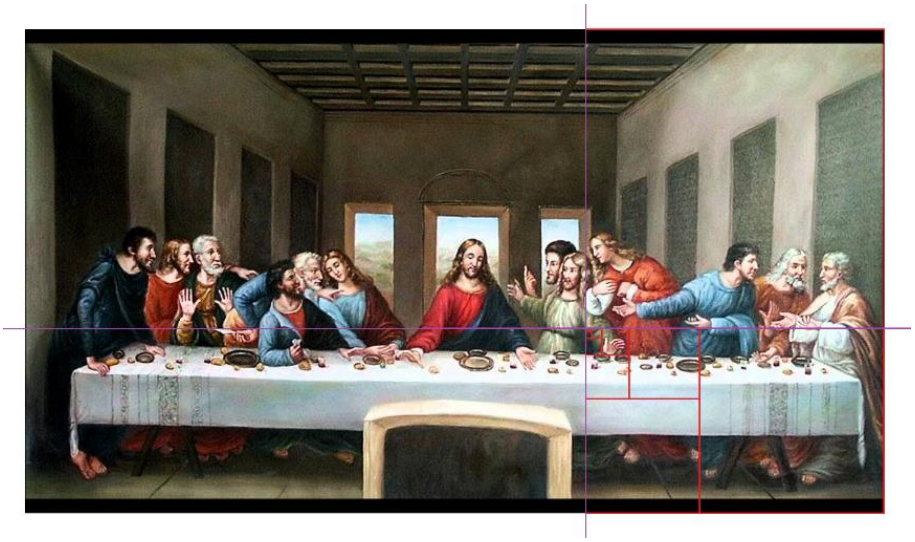


Figura 32 Ejemplo de detección del punto áureo en una imagen

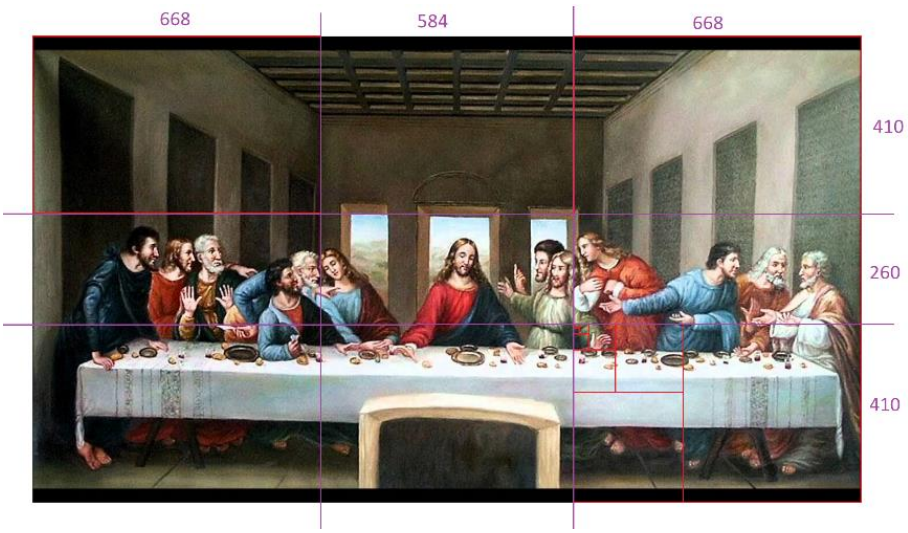


Figura 33 Cuadrícula con puntos áureos de una imagen

Una vez identificados los puntos áureos y dibujada la cuadrícula como se muestra en la Figura 33, se define que la mejor muestra de cada fotograma será de 584x260 pixeles, se considera que esta muestra es un 7,32% del fotograma, por lo que se decide también probar con la relación de tercios que tiene una novena parte de la imagen es decir un 11,11% del fotograma, esto es lo que muestra la Figura 34.

Figura 34 Ejemplo del uso de la regla de los tercios

Se realizaron pruebas con estas muestras, los resultados han sido tabulados en el Anexo 3 y se determinó que la muestra con mejores resultados es la que aplica la regla de los tercios la cual se muestra en la Figura 34, ya que reduce en un 88,53% el tiempo necesario para analizar los fotogramas a comparación de usar el 100% de cada uno, además tiene un error relativo del 18% en referencia a las comparaciones realizadas con el 100%, es importante considerar que se tuvo una prueba en donde el resultado tuvo una gran variación justamente al evaluar un cambio de escena. En la Tabla 4 se detallan los valores del tamaño de la muestra y el porcentaje que corresponde al original.

Tabla 4
Tabla de las muestras tomadas de cada fotograma para realizar las pruebas

Toma de muestras				
Tamaño en pixeles	Cantidad de pixeles	Porcentaje de la muestra	Rango horizontal	Rango vertical
1920x1080	2073600	100%	1-1920	1-1080
640x360	230400	11,11%	641 - 1280	361 - 720
584x260	151840	7,32%	669 - 1252	411 - 670

Finalmente, para mejorar el tiempo de procesamiento, se ha modificado el algoritmo tomando en cuenta que la comparación SSIM se está realizando con las 3 capas de cada imagen en un solo cálculo. Se dividió el procedimiento, ahora el cálculo se realizará de cada capa de la imagen RGB y el resultado de cada capa se multiplica con los otros dos para obtener un valor de SSIM.

3.7. Identificación de las imágenes portadoras de la información

Después de determinar cuál es la muestra de cada fotograma con la cual se hará la comparación en el algoritmo para su detección automática, y haber separado el cálculo para reducir el tiempo de ejecución. Se debe definir cuál es el valor del SSIM que se obtiene en un cambio de escena, es

importante considerar esto, ya que los cambios de escena pueden ser de tipo desvanecimiento o corte (cambio de escena directo). Para esto, se identifican manualmente todos los cambios de escena y se realizan pruebas con cada uno de ellos para determinar un valor de SSIM promedio, el cual detecte la mayoría de los cambios de escena. En la Tabla 5 se resumen los valores que se encontraron en las pruebas realizadas.

Tabla 5
Valor promedio del SSIM según el tipo de cambio de escena

Nro.	Tipo de cambio de escena	SSIM promedio
1	Cambio de escena por desvanecimiento	0,91
2	Cambio de escena por corte	0,25

Una vez definido el valor del SSIM que se considera para identificar un cambio de escena, se implementa el algoritmo para que el programa los detecte automáticamente, realizando comparaciones sucesivas entre el enésimo fotograma y el siguiente de la secuencia, se obtienen los fotogramas que servirán como portadores de la información, tras descartar los que tengan un SSIM mayor a 0,25.

3.8. Descartar fotogramas compuestos uniformemente

Una vez se han detectado los cambios de escena automáticamente, es necesario descartar los fotogramas que están compuestos uniformemente como los mostrados en la Figura 35. Estos, por tener una estructura uniforme, permiten que el ojo humano detecte cambios más fácilmente por su gran cantidad de zonas lisas, por lo que se debe evitar usar estos fotogramas.

En la Figura 35 se observan los 12 primeros fotogramas del video portador, si solo se considera el valor SSIM de la comparación tendríamos que el fotograma 3 es un cambio de escena, pero sería

incorrecto usarlo para ocultar información ya que es perceptible al ojo humano, por lo tanto se deben descartar este tipo de fotogramas.

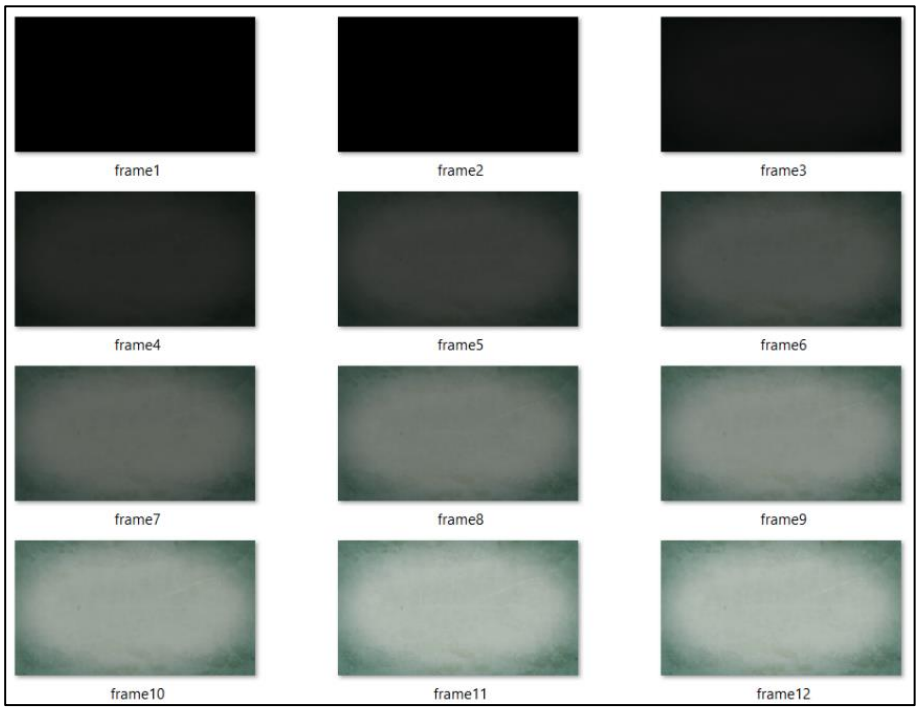


Figura 35 Fotogramas compuestos uniformemente extraídos del video portador

Para lograr este objetivo se ha desarrollado un algoritmo que descarta los fotogramas que tienen las características mencionadas anteriormente, se utiliza la función *std2* de Matlab®, ya que por definición esta calcula la desviación estándar de todos los valores de un arreglo. Se calcula este valor para cada fotograma. Y se descartan los que no tengan una desviación mayor a 50.

3.9. Definición del par imagen secreta / imagen portadora más apto para procesar

Gracias al algoritmo desarrollado se han definido cierta cantidad de fotogramas que servirán como portadores de la información, de la misma manera tenemos cierta cantidad de imágenes secretas para ser ocultas. Ahora, es necesario determinar que imagen portadora es la mejor para

ocultar cierta imagen secreta, esto se realiza mediante la comparación de todas las imágenes secretas con todos los fotogramas portadores y con ayuda del valor SSIM se determinan los pares a procesar más aptos, en base a la mayor similitud que haya tenido cada uno.

Se determina el valor del SSIM de cada fotograma portador con cada imagen secreta, y almacena estos valores en un vector, con cada vector de la comparación del SSIM de los fotogramas portadores, se construye una matriz, esta se ordena de mayor a menor valor del SSIM por filas y cada vez que se avanza en las filas se va descartando los valores que ya han sido ordenados en la fila anterior.

De esta forma, se logra determinar que fotograma portador debe ser transformado con que imagen secreta. El programa desarrollado nos muestra en la ventana de comandos cual es el resultado de esta comparación de bases de datos, como se muestra en la Figura 36.

```
fotograma portador 1(fotograma 1095) con imagen secreta 5
fotograma portador 2(fotograma 271) con imagen secreta 8
fotograma portador 3(fotograma 2073) con imagen secreta 16
fotograma portador 4(fotograma 1596) con imagen secreta 13
fotograma portador 5(fotograma 1281) con imagen secreta 4
fotograma portador 6(fotograma 2272) con imagen secreta 12
fotograma portador 7(fotograma 188) con imagen secreta 1
fotograma portador 8(fotograma 238) con imagen secreta 6
fotograma portador 9(fotograma 766) con imagen secreta 7
fotograma portador 10(fotograma 2028) con imagen secreta 9
fotograma portador 11(fotograma 1062) con imagen secreta 11
fotograma portador 12(fotograma 1129) con imagen secreta 15
fotograma portador 13(fotograma 734) con imagen secreta 14
fotograma portador 14(fotograma 2307) con imagen secreta 6
fotograma portador 15(fotograma 901) con imagen secreta 2
fotograma portador 16(fotograma 2134) con imagen secreta 3
>>
```

Figura 36 Resultado de la comparación entre fotogramas portadores e imágenes secretas

Como se muestra en la Figura 36, cada fotograma portador (imagen objetivo) tiene su correspondiente imagen secreta con la cual se realizará la transformación de color reversible. Esta imagen secreta asignada, tiene la mayor similitud de entre todas las demás.

3.10. Transformación de la imagen secreta en la imagen portadora

Para la transformación de la imagen secreta en el fotograma portador, se utiliza la metodología desarrollada en (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016).

Primero se igualan las dimensiones de la imagen secreta y la imagen objetivo/portadora, luego se dividen cada una en bloques de 8x8 pixeles, esto genera imágenes tipo mosaico como se observa en la Figura 37. El proceso de transformación se indica en el diagrama de flujo de la Figura 38.

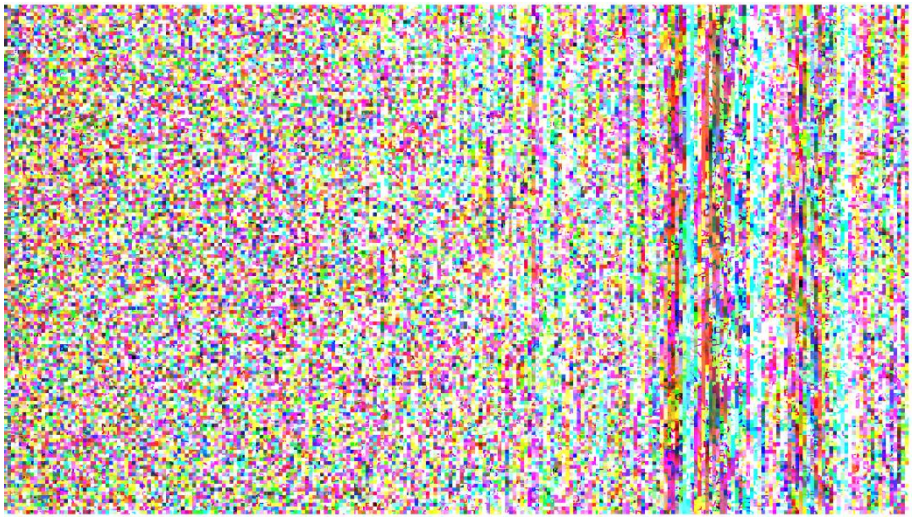


Figura 37. Imagen tipo mosaico generada para la transformación

Posteriormente, cada bloque de la imagen secreta pasa por una transformación de color para igualarlo al bloque correspondiente en el fotograma portador. Y se rota cada bloque para que se asemeje más a la imagen objetivo/portadora.

Esta transformación genera un vector con información acerca de las características del color de la imagen secreta (medias y desviaciones estándar), además de los índices y ángulos originales, esta información es de suma importancia ya que sirve para la reconstrucción de la imagen secreta.

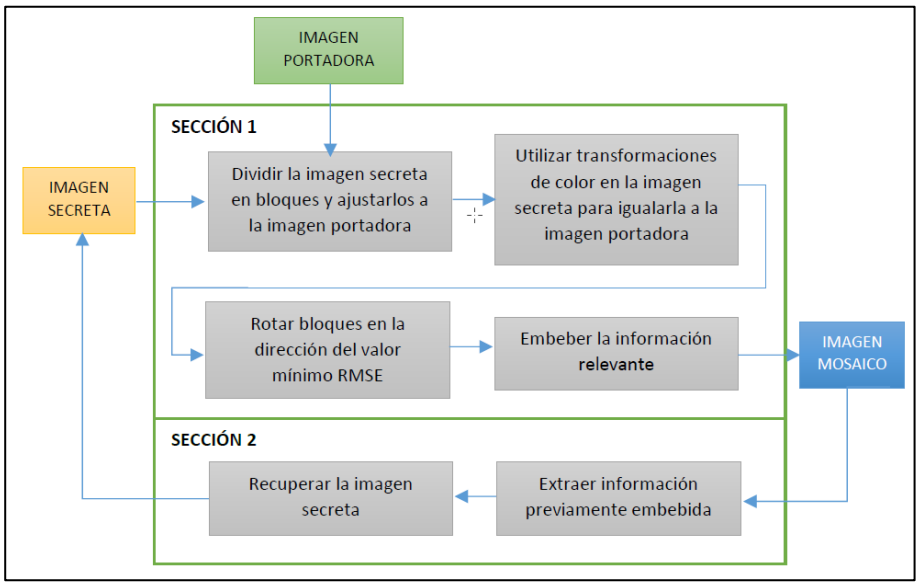


Figura 38 Diagrama de bloques de algoritmo Ya-Lin – Wen-Hsiang
Fuente: (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

Una vez realizado todo este proceso se obtiene finalmente la imagen tipo mosaico que se asemeja a la imagen objetivo/portadora, a la cual llamaremos estego-fotograma o estego-imagen. Esta debe ser insertada en el video, reemplazando el fotograma original (imagen objetivo) por este estego-fotograma.

Es importante recordar que toda la información relevante para reconstruir la imagen secreta se encuentra almacenada en un vector y este debe ser trasmitido de alguna forma al receptor para que pueda recuperar la imagen secreta. El vector está compuesto por 4 partes: los índices de los cuadros que componen el mosaico, sus ángulos originales, la media de cada uno y la conversión de los residuos.

Para comprender el proceso, en las Figuras 39 y 40 se muestran las imágenes tipo mosaico generadas a partir de dividir en bloques de 8x8 pixeles la imagen secreta que se desea ocultar, se tiene una denominada “Imagen Ordenada” la cual es la imagen tipo mosaico que se genera con la

imagen secreta pero sus bloques están ordenados en base las características de la imagen objetivo (fotograma portador), además, se tiene una imagen tipo mosaico denominada “Imagen desviación” la cual es el resultado de ordenar en base a la desviación estándar de cada bloque de la imagen secreta.

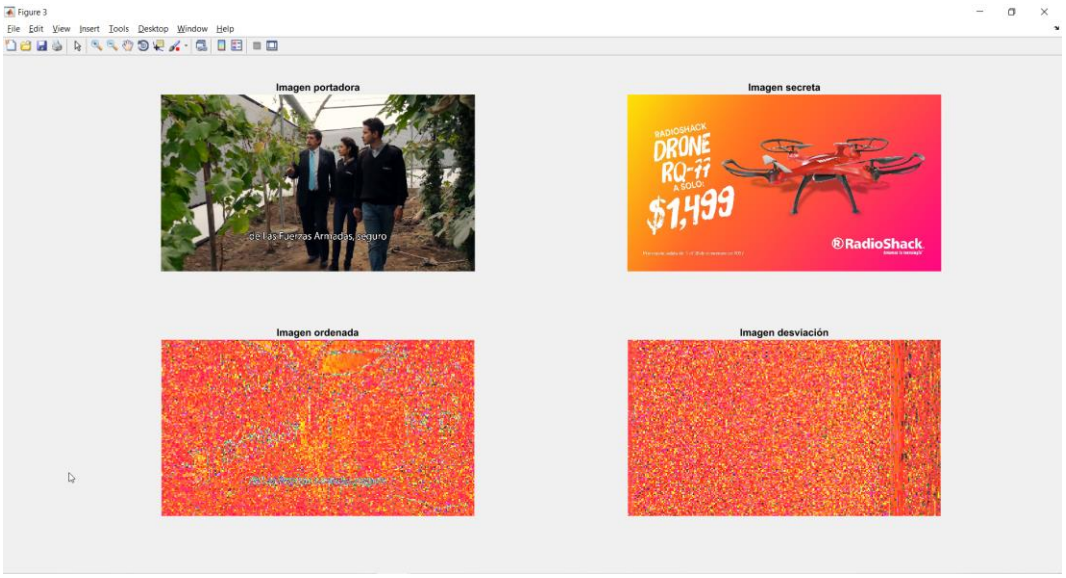


Figura 39 Ejemplo de imagen generada por la división en bloques

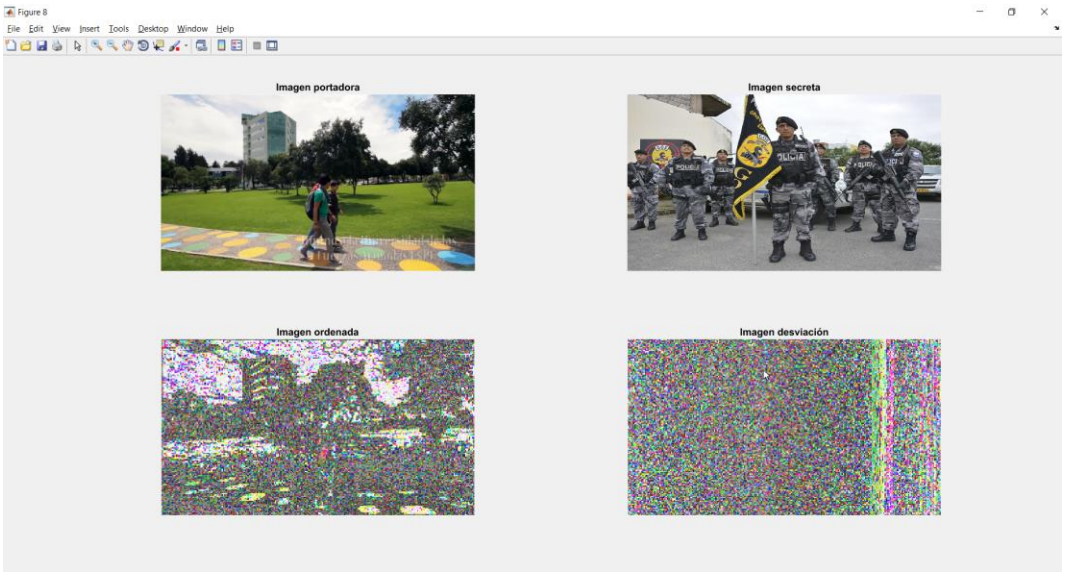


Figura 40 Ejemplo de imagen generada por la división en bloques

En la Figura 41 se puede ver todas las conversiones de cada imagen secreta en imágenes tipo mosaico, y como se han ordenado estas, en base a las características de su correspondiente imagen objetivo (fotograma portador).

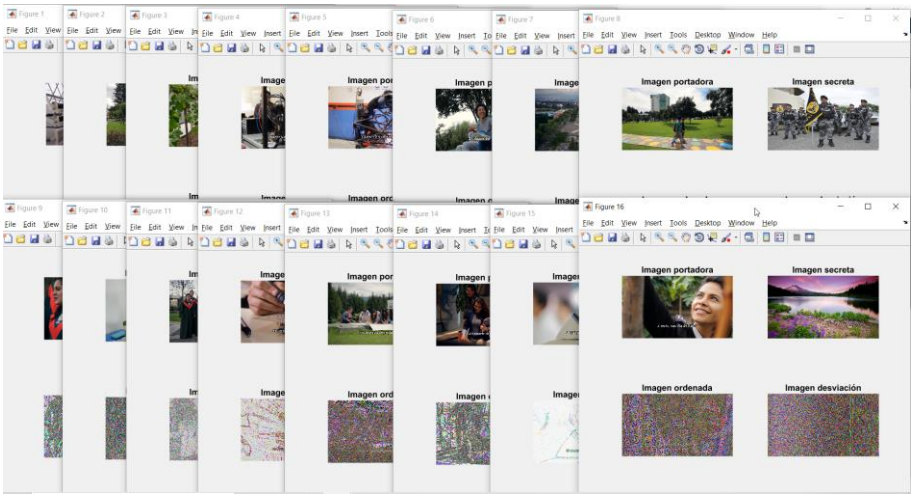


Figura 41 Todas las 16 imágenes generadas por la división en bloques

Una vez generadas las imágenes secretas tipo mosaico, con ayuda de la ventana de comandos se muestra información relevante para la inserción de bits en el audio, en la Figura 42 se observan las cantidades de bits que ha generado el proceso de división en bloques y nos da una primera idea de toda la información que se debe incrustar en el audio.

```
Command Window
  Cantidad de bloques = Bloques = 1080/8 * 1920/8 = 135 * 240 = 32400
  Bits para cada indice de bloque = Bits_ind = 15
  Cantidad total de bits para vector de indices = Bloques * Bits_ind = 486000
  Bits para cada angulo = Bits_ang = 2
  Cantidad de bits para vector de angulos = Bits_ang * Bloques = 64800
  Cantidad de bits para vector de media del bloque = Bloques * 23 = 745200
```

Figura 42 Información relevante respecto a la inserción de bits en el audio

Se utilizan las imágenes secretas tipo mosaico ordenadas en base a la desviación de los bloques de la imagen objetivo y se aplica la transformación de color descrita en la Figura 38. Se han

convertido los bloques de las imágenes secretas tipo mosaico en los bloques correspondientes de las imágenes objetivo/portadoras tipo mosaico, y se han generado las denominadas estego-imágenes, las cuales reemplazarán a las imágenes objetivo/portadoras y se obtendrá la secuencia de cuadros para crear el estego-video.

3.11. Organización de la información de recuperación

Para incrustar la información que se utiliza para recuperar la imagen secreta, es necesario estructurarla de una manera eficiente y organizada, para poder reconstruir la matriz o el vector que tiene la información relevante de cada imagen secreta. Primeramente, es necesario calcular la longitud del vector que se desea incrustar, para lo cual hay que considerar que el vector está compuesto por 4 partes: los índices originales de cada bloque, los ángulos que se han rotado, la media de cada bloque y los residuos del cálculo. Al tomar en cuenta la capacidad de incrustación, se determina que se pueden recuperar solo dos imágenes, puesto que se pueden insertar en el audio 2 vectores de aproximadamente 4,5 millones de bits en el bit menos significativo de cada muestra tomada.

3.12. Encriptación de la información

Para mejorar la seguridad del sistema, y evitar que una tercera persona pueda reconstruir la información que se desea ocultar en el video. Se ha desarrollado un algoritmo de encriptación, basado en el cifrado de César. Básicamente lo que hace este algoritmo es tomar un byte (8 bits) del vector que se va a ocultar, convertir este byte a decimal e incrementar en 3 su valor. La Figura 43 muestra el funcionamiento del algoritmo.

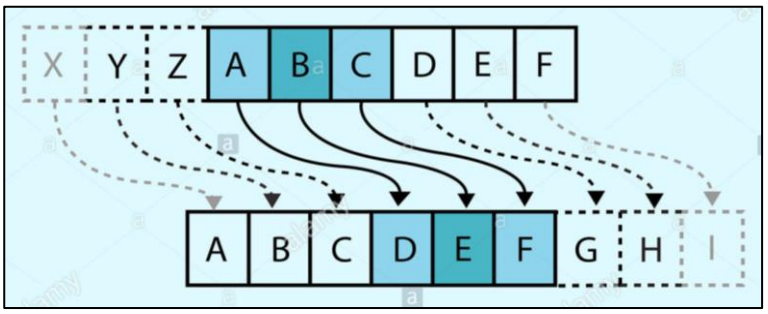


Figura 43 Referencia del modelo de Cifrado de César
Fuente: (Images, 2018)

En este caso, los 8 bits van a generar un número decimal desde el 0 hasta el 255 (256 posibles valores), por lo cual si el número incrementado en 3 sobrepasa el valor de 255 continuará con el número 1.

3.13. Incrustación de datos en el audio

Se utiliza la función *fopen* de Matlab®, con lo cual al ingresar el parámetro "r" nos permite leer el archivo con nombre "aport.wav" que contiene la señal de audio extraída del video portador, señal que fue descompuesta del mismo al inicio del programa.

Con el archivo "abierto" podemos acceder a su información, y con la función *fread*, se extraen en variables los bits que componen al archivo. Ya con los datos almacenados en una variable, se procede a utilizar la función *fclose* para cerrar la información del archivo de audio.

Una vez listo el vector a ser incrustado en el audio del video portador, se utiliza la función *bitset* de Matlab® para cambiar un bit de la variable "datos", la cual contiene la información de los datos del archivo de audio. La función *bitset* de Matlab® permite ingresar el parámetro "bit" que es la posición del bit que se desea establecer o cambiar, este pará metro en este caso debe ser 1 ya que es el LSB.

Se establecieron rangos de la variable “datos” en los cuales se tiene diferente información, el primero rango son 8 bits para la clave que debe ser establecida en el emisor y debe coincidir con la del receptor para que el programa autorice extraer los datos, caso contrario no se podrá recuperar la información incrustada. Luego, están dos rangos que corresponden a la longitud de los vectores de cada imagen secreta a ser recuperada, y finalmente en el último rango está el vector que reconstruye a las imágenes secretas ocultadas en el video portador.

3.14. Creación del estego audio

Se utiliza la función *fopen* para poder crear un archivo de audio e insertar las variables originales y la variable “datos” la cual contiene los vectores de reconstrucción de las imágenes, al utilizar el parámetro “w”, se crea un archivo de audio y se le inserta la información.

3.15. Construcción del estego-video

Una vez que se dispone del estego-audio (audio con información oculta) y de los fotogramas finales (fotogramas que componen el video, entre ellos están los estego-fotogramas) se puede crear el archivo de video. Para lo cual se utiliza la función *VideoWriter* con su configuración predeterminada la cual nos genera un archivo de video en formato AVI.

3.16. Recuperación de la información oculta

Para la recuperación de la información y la correspondiente reconstrucción de las imágenes ocultas, se ha utilizado gran parte del código que se creó para ocultar la información. Básicamente, lo que se ha hecho es un proceso inverso al que se implementó y ejecutó al momento de crear el estego-video.

Para generar los fotogramas recuperados se ha utilizado la función *VideoReader* y la función *imwrite.*

Para crear el archivo de audio recuperado se ha utilizado las funciones *fread, fopen y fclose.*

Para poder evaluar la calidad del algoritmo de recuperación de información se crearon unas líneas de código las cuales nos muestran el porcentaje de igualdad entre el vector insertado originalmente y el vector recuperado.

Ahora para construir los vectores que servirán para la reconstrucción de las imágenes se ha utilizado la función *bitget.*

3.17. Desencriptación de la información recuperada

Para poder utilizar la información recuperada se debe desencriptar, se realiza el proceso inverso del cifrado de César, es decir toman un byte, lo convierten a decimal y le resta a su valor 3. Con lo cual el byte vuelve a su valor original.

3.18. Reconstrucción de vectores e imágenes secretas

Con el vector recuperado se utilizan los rangos definidos por la cantidad de bloques de cada imagen, con los que se va extrayendo la información oculta, de esta manera se reconstruye el vector para recuperar las dos imágenes que se eligieron. Una vez se dispone de cada vector de las imágenes, se utilizan los rangos determinados por el tamaño de las imágenes y la dimensión de los bloques, por ejemplo:

a. Para los índices de cada bloque, al tener fotogramas de 1920x1080 pixeles se los divide en bloques de 8x8, a lo ancho se tienen 240 (1920/8) bloques y a lo alto se tiene 135 (1080/8)

bloques. Por lo tanto, en total se tienen 32400 (240x135) bloques. Para poder enumerar y organizar todos estos bloques se utilizan 15 bits (2^15 = 32768 posibles combinaciones), de esta manera la parte del vector que especifica los índices de cada bloque tiene una longitud total de 486000 (32400x15) bits.

b. Para los ángulos rotados, se pueden tener 4 posibles valores (0°, 90°, 180°, 270°) por lo tanto se requieren 2 bits para especificar cada uno de estos, al tener un total de 32400 bloques se requieren 64800 (32400x2) bits.
c. Para obtener la media de cada bloque, se tienen 24 bits y por tener los 32400 bloques se tienen un total de 777600 (32400x24) bits.
d. Finalmente, el resto de los bits corresponden a los residuos que deja el proceso de transformación de cada imagen.

Ya organizada la información recuperada, se procede a ejecutar el proceso inverso a la transformación de imágenes, primero se rota cada bloque a su ángulo original, se hace la transformación inversa con ayuda de los residuos recuperados, y las imágenes recuperadas se convierten en una imagen tipo mosaico que se ordena con ayuda de los índices originales que se recuperaron y se asemeja a la imagen secreta original.

3.19. Procesamiento posterior a la recuperación de la imagen

Para lograr obtener una imagen recuperada lo más semejante a la imagen secreta original, se debe tomar en cuenta su tamaño, por lo cual se utiliza la función *imresize* para establecer el tamaño de la imagen secreta recuperada en base a la imagen secreta original.

Además, para evitar el efecto del pixelado, provocado por la división de la imagen en bloques se aplican 3 tipos de filtros a la imagen resultante de la recuperación, con lo cual se pueden analizar diferentes resultados y así determinar cuál filtro genera el mayor valor de similitud con la imagen secreta original.

CAPITULO 4

4. ANÁLISIS DE RESULTADOS

4.1. Métodos de conversión de videos

De los 3 métodos que se mencionan en la Sección 3.4 del presente trabajo de investigación el mejor es el que utiliza una herramienta web para convertir el video. Este método no genera cambios en las características originales del video portador, entrega un archivo con tamaño en disco razonable y el códec que utiliza es compatible con la mayoría de los reproductores multimedia.

Se realizaron pruebas con cada uno de los métodos, se tabularon los resultados y están detallados en la Tabla del Anexo 2.

Se ha concluido que el mejor método para convertir un video de formato MP4 a formato AVI es, el uso de una herramienta WEB disponible en https://www.clipconverter.cc/. Puesto que utiliza el códec de video H264. Generando un video con nitidez, calidad en el audio y que es compatible con todos los reproductores. La desventaja es que modifica la velocidad de fotograma, entrega un video con una velocidad de fotograma mayor a la original, pero con Matlab® es posible manipular esta tasa de fotogramas, además su tamaño en disco es manejable al ser 50 MB aproximadamente, que es mucho menor a los otros métodos de conversión evaluados.

4.2. Algoritmo para detección de cambios de escena

Para realizar las pruebas y determinar el tiempo de procesamiento necesario para determinar los cambios de escena, se tomó una muestra de los fotogramas originales del video portador.

Se tienen un total de 2639 fotogramas del video portador, de los cuales se eligieron 13 fotogramas. Es decir, se tomó aproximadamente un 0,5% de los fotogramas del video portador, que vendrían a ser menos de un segundo (0,55 segundos) de su duración.

Se puede observar en la Tabla del Anexo 3, que en promedio para comparar dos fotogramas con un tamaño de 1920 x 1080 pixeles es necesario un tiempo de procesamiento de 54,09 segundos, esto considerando que se utiliza una computadora con sistema operativo Windows 10, con un procesador Intel® Core i5-4210U que funciona entre 1.7 y 2.4 GHz y una memoria RAM de 8 GB.

Las pruebas indican que, para detectar cambios de escena en el video portador, utilizando dos fotogramas RGB de 1920x1080 pixeles y haciendo uso de la función *ssim* de Matlab® se requiere aproximadamente un minuto por cada comparación. Es decir que, teniendo 2639 fotogramas, se necesitaría esperar 2638 minutos que vendrían a ser aproximadamente 44 horas, para detectar los cambios de escena, por tener este recurso computacional limitado se descarta esta opción.

Tomar una muestra de cada fotograma para realizar una comparación es la mejor opción y según la Tabla 6, la mejor muestra es tomar una novena parte de la imagen (11,11%), la muestra que se toma del centro como indica la Figura 34 en la Sección 3.6 del presente trabajo de investigación. Esto da como resultado una reducción del 88,53% en el tiempo de ejecución del programa, ahora en lugar de esperar cerca de un minuto por cada comparación se deberá esperar 7 segundos aproximadamente. Además, el error relativo promedio es aproximadamente un 9% el cual es menor al calculado con el uso de la muestra número 3 de la Tabla 6 el cual usa un 7.32% del fotograma original.

El detalle de las pruebas ejecutadas las cuales sustentan la información presentada a manera de resumen en la Tabla 6, se muestran en el Anexo 4 y Anexo 5.

Tabla 6
Resultados de la comparación con varias muestras de cada fotograma

T	Porcentaje de la muestra	Tamaño en pixeles	Tiempo promedio para comparar 2 fotogramas (segundos)	Tiempo total para analizar video de prueba (segundos)	Tiempo total para analizar video de prueba (horas)	Porcentaje comparado con T1	Reducción del tiempo T1	Error relativo promedio
1	100,00%	1920x1080	60,79	160370,62	44,55	100,00%	0,00%	0%
2	11,11%	640x360	6,975	18400,05	5,11	11,47%	88,53%	9%
3	7,32%	584x260	5,25	13856,10	3,85	8,64%	91,36%	15%

Para poder reducir este tiempo de ejecución, se ha mejorado el algoritmo de detección de cambios de escena, al reemplazar la estructura de comparación compuesta por las 3 capas y ejecutada en una sola comparación, por 3 comparaciones, una por cada capa, con lo cual se reduce el tiempo de ejecución de esta Sección del programa en un 75% aproximadamente.

Tabla 7
Porcentaje de mejora del algoritmo original

Descripción	Valor medido	Observación
Tiempo que demora con algoritmo original (segundos)	6,53	Porcentaje de mejora en tiempo: 74,64%
Tiempo que demora con algoritmo mejorado (segundos)	1,66	
Porcentaje de error relativo promedio del algoritmo original	19,68%	Porcentaje de diferencia de error relativo promedio: 2,82%
Porcentaje de error relativo promedio del algoritmo mejorado	22,50%	

Como se muestra en la Tabla 7, se logra reducir el tiempo de ejecución, pero el error relativo promedio aumenta en un 3% aproximadamente.

Es importante analizar que la relación costo beneficio, entre el incremento del error relativo promedio y la mejora en el tiempo de ejecución del algoritmo, es alta, es decir se tiene un bajo

costo y el beneficio es alto. Esta relación se puede decir que se calcula dividiendo el beneficio para el costo, y se analiza cómo se indica a continuación:

- B/C > 1 indica que los beneficios superan los costos, por consiguiente, el proyecto debe ser considerado.
- B/C=1 Aquí no hay ganancias, pues los beneficios son iguales a los costos.
- B/C < 1, muestra que los costes son mayores que los beneficios, no se debe considerar.

Para el presente proyecto de investigación, la ecuación 4 muestra el resultado del cálculo:

$$\frac{B}{C} = \frac{74{,}64\%}{2{,}82\%} = 26{,}48 \quad \text{por lo tanto,} \quad \frac{B}{C} > 1$$

Ecuación 4. Cálculo de la relación costo beneficio del algoritmo mejorado

Al tener aproximadamente un 20% de error en cuanto a la detección de cambios de escena, este valor debe considerarse al momento de evaluar el SSIM y determinar los fotogramas que son cambios de escena. Para lograr esto, en el código que condiciona el valor del SSIM se reduce del 0,25 que se habría establecido con las primera pruebas detalladas en la Tabla 5 al 0,05 tras restarle el 20% (0,2).

4.3. Pruebas del algoritmo de detección de cambios de escena

Al delimitar el valor del SSIM resultante de la comparación de fotogramas, se garantiza que los fotogramas elegidos como portadores cumplen con la característica de baja similitud con el fotograma siguiente, esto permite que la imagen mosaico a ser oculta en el video sea menos detectable. Ahora es necesario evitar los fotogramas que componen un cambio de escena por

desvanecimiento, es decir los cuadros negros que inician y finalizan los videos o los fotogramas que están compuestos uniformemente.

Para descartar los fotogramas que están estructurados uniformemente, es decir que tienen gran parte de sus pixeles de un solo color, o que están compuestos por gran cantidad de pixeles con las mismas características, se ha realizado una prueba con 9 cambios de escena (imágenes objetivo) que se detectaron al evaluar el SSIM, se calculó la desviación estándar de cada uno de ellos y se tuvieron los resultados mostrados en la Tabla 8.

Tabla 8
Resultados del cálculo de la desviación estándar de varios fotogramas

Nro.	Cambio de escena detectado	DStd promedio
1	Fotograma uniforme	23,83
2	Fotograma con contenido	37,97

Las pruebas realizadas se detallan en el Anexo 6. Una vez analizados estos valores su puede concluir que se debe limitar los fotogramas portadores (imágenes objetivo) con la característica de tener una desviación estándar mayor a 23,83 y que por lo menos se acerque al valor de un fotograma con contenido que sería 37,97. Por lo tanto es correcto establecer en el algoritmo que solo los fotogramas con una desviación estándar mayor a 30 se definan como fotogramas portadores (imágenes objtivo). Pero es necesario considerar el porcentaje de error relativo promedio, por lo cual en la línea del código del programa, que condiciona el valor de la desviación estándar promedio se incrementa este valor, pasando de 30 a 50, con el objetivo de elegir fotogramas que tienen gran cantidad de información.

Se realizó una prueba y los primeros 25 fotogramas mostrados en la Figura 44 tienen los valores de desviación estándar mostrados en la Tabla 9. Por otro lado, en la Figura 45 se tienen los

fotogramas cargados de información. Por lo cual, se verifica que los fotogramas con una desviación estándar menor a 50 son fotogramas que tienen poca información y están estructurados uniformemente.

Figura 44 Primeros 25 fotogramas del video portador estructurados uniformemente

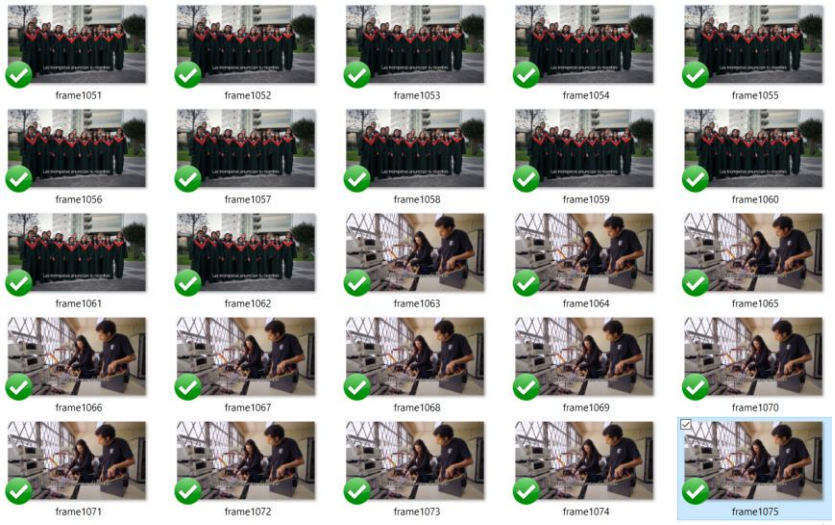


Figura 45 Fotogramas con información relevante al video

Tabla 9

Desviaciones estándar medidas en los fotogramas uniformes iniciales del video

Fotograma	DStd
1	0
2	0
3	2,639339416
4	5,872043455
5	8,533633335
6	10,97814698
7	13,37739215
8	16,09975264
9	18,82268478
10	21,63880738
11	24,16595195
12	24,17552054
13	24,24092356
14	25,37827125
15	35,15876081
16	46,9373732
17	50,7366249
18	50,10774487
19	48,09842308
20	45,95667491
21	43,68880718
22	41,66981659
23	39,73029767
24	38,0309246
25	48,46034856

4.4. Pares a procesar definidos por el algoritmo

El algoritmo define que imagen secreta debe ocultarse con que imagen objetivo (fotograma portador). Donde cada imagen objetivo (fotograma portador) tiene con su correspondiente imagen secreta el mayor SSIM posible.

4.5. Encriptación de datos

El algoritmo de encriptación de información es de baja complejidad, por lo cual nos permite tener un tiempo de ejecución relativamente corto, aproximadamente 2 minutos toma encriptar los

9’511.625 bits que sirven para reconstruir 2 imágenes ocultas. Esto permite mejorar la seguridad del sistema.

4.6. Incrustación de información en el audio

Para cuantificar la diferencia entre el archivo de audio original, el archivo de audio con información oculta (estego-audio) y el archivo de audio recuperado, se utilizan medidas estadísticas, el error cuadrático medio (MSE) y el PSNR, además se ha calculado la similitud entre las señales con ayuda del SSIM. Como se muestra en la Tabla 10, se han realizado mediciones en cuanto a parámetros estadísticos entre en audio original, el estego-audio y el audio recuperado. Como se puede ver, el error cuadrático medio es despreciable, la relación señal a ruido es adecuada ya que supera el 90%, y la comparación de similitud con el SSIM es prácticamente ideal.

Tabla 10
Medición de parámetros estadísticos al estego-audio y el audio recuperado

Audio de referencia	Audio evaluado	MSE
Audio original	Estego-audio	7,579673E+04
Audio original	Audio recuperado	7,713328E+04

Audio de referencia	Audio evaluado	PSNR
Audio original	Estego-audio	91,203495
Audio original	Audio recuperado	91,127582

Audio de referencia	Audio evaluado	SSIM
Audio original	Estego-audio	0,999999
Audio original	Audio recuperado	0,999999

Como se puede ver en la Figura 46, la señal del audio original y la señal del estego-audio se sobreponen en el dominio del tiempo, es prácticamente imperceptible el cambio del ultimo bit menos significativo, por lo cual se validan los resultados mostrados en la Tabla 10. En la Figura

47, se muestra la gráfica únicamente del audio original en el dominio de la frecuencia para observar como en la Figura 48, la señal del estego-audio en el dominio de la frecuencia lo sobrepone.

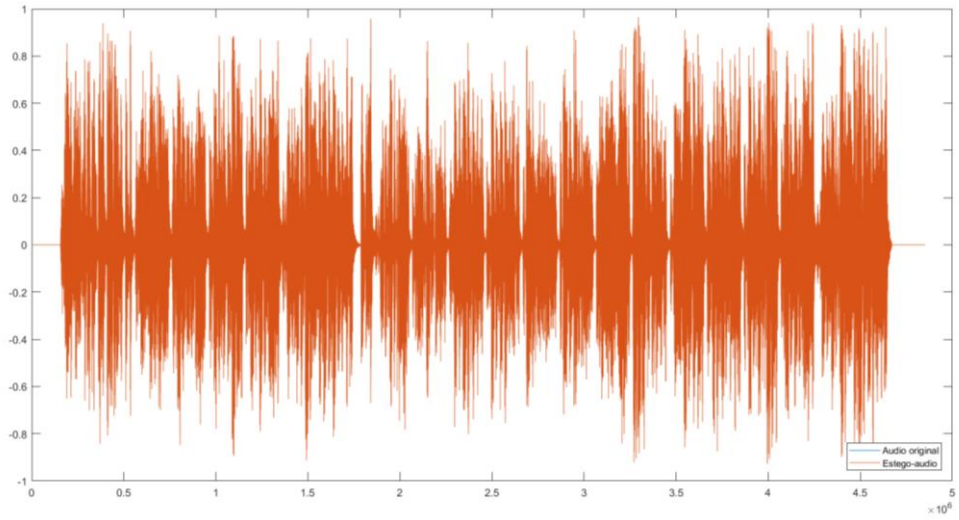


Figura 46. Señal del audio original y estego-audio en el dominio del tiempo

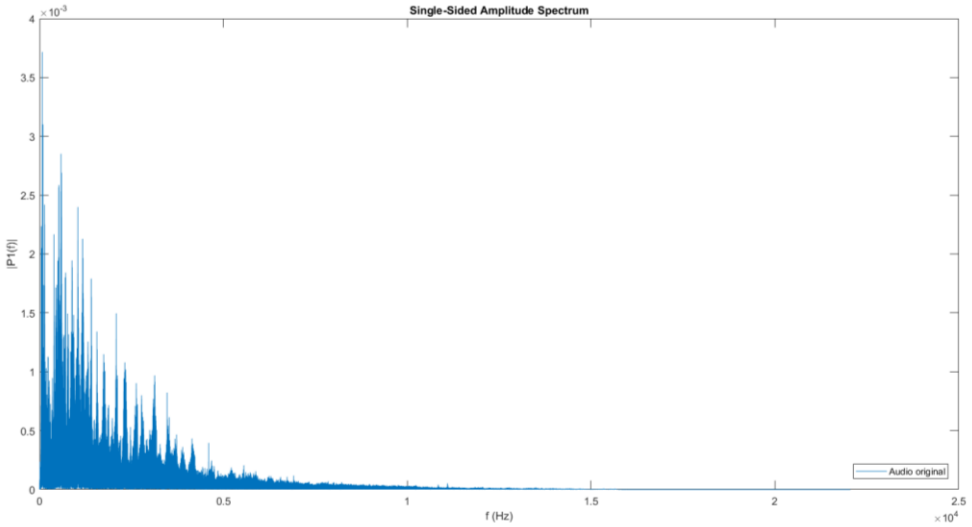


Figura 47. Señal del audio original en el dominio de la frecuencia

En la Figura 48 se observa como la señal del estego-audio se sobrepone a la señal del audio original en el dominio de la frecuencia, por lo que no se percibe ningún cambio a causa de la modificación del ultimo bit menos significativo.

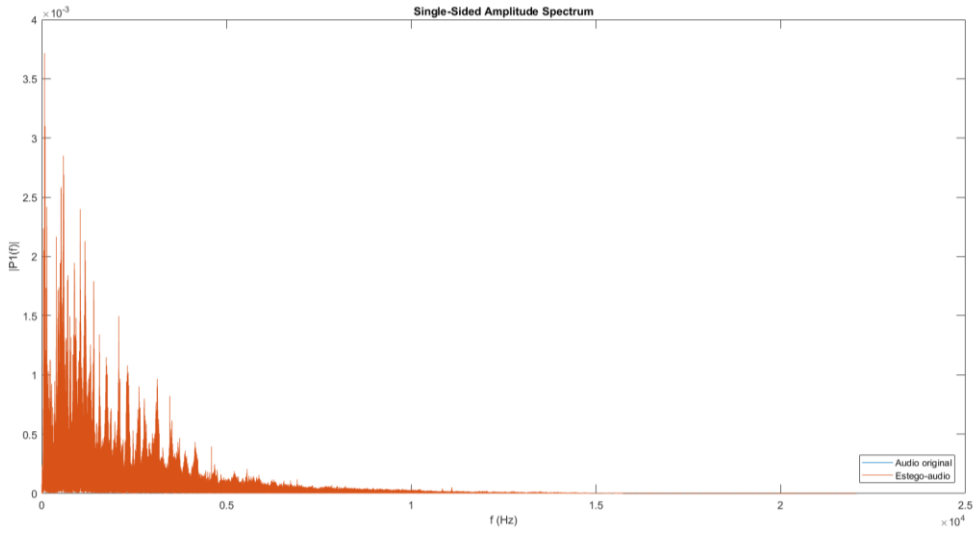


Figura 48. Comparación del audio original y el estego-audio en el dominio de la frecuencia

De igual manera, en la Figura 49 se comprueba que los valores de los parámetros estadísticos están correctos ya que es imperceptible el cambio en la señal.

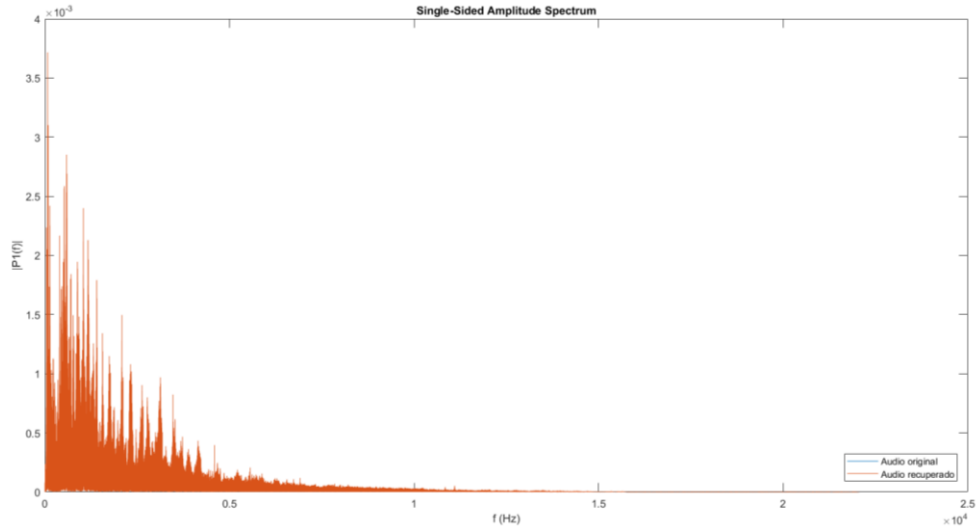


Figura 49. Comparación del audio original y el audio recuperado en el dominio de la frecuencia

4.7. Construcción del estego video

El uso de las funciones *fopen, fwrite, fclose, bitset, VideoWriter, open, writeVideo* ha resultado efectivo para el presente trabajo de investigación ya que nos ha facilitado el poder manipular los archivos de la manera correcta, modificando solo los bits que deseamos y generar archivos con los parámetros deseados, como es el caso de la tasa de fotogramas por segundo o fps.

4.8. Capacidad de incrustación

La capacidad de incrustación está definida por las características del audio del video portador, y los parámetros con los que este se ha digitalizado.

Los parámetros más importantes para considerar son: la frecuencia de muestreo y la cantidad de bits por muestra. Al descomponer el audio del video portador elegido se puede determinar cuál es la frecuencia de muestreo, y al saber que este se maneja con formato WAV la frecuencia de muestreo es 44100 Hz por ser su estándar. Esta misma frecuencia de muestreo es la que se debe mantener al momento de generar el estego-audio, con el fin de no modificar las propiedades del audio en el video portador.

La frecuencia de muestreo nos permitirá calcular cuantas veces se ha medido la señal de audio en un segundo, ahora es importante conocer con cuantos bits se ha medido esta señal en cada muestra. Para definir la cantidad de bits por muestra es necesario comprender que mientras más bits se tenga por cada muestra, mayor tamaño tendrá el archivo, y la tasa de bits incrementará.

Para este caso con ayuda de la función *audioinfo* se pueden obtener las características, como se indica en la Figura 50, donde se obtiene la tasa de muestreo (SampleRate), la duración exacta (Duration), los bits por muestra (BitsPerSample) y el número de canales (NumChannels).

Para determinar la cantidad de muestras tomadas se debe multiplicar la tasa de muestreo por la duración del audio. Como se indica en la ecuación 5 y posteriormente se evalúa en la ecuación 6.

$$Total\ muestras = Tasa\ de\ muestreo\ \left[\frac{muestras}{segundo}\right]\ x\ Duración\ [segundos]$$

Ecuación 5. Cálculo de la cantidad de muestras tomadas

$$Total\ muestras = 44100\ \left[\frac{muestras}{segundo}\right]\ x\ 110.0161\ [segundos] = 4851712\ [muestras]$$

Ecuación 6. Cálculo de la cantidad de muestras tomadas

Ahora para determinar el número de bits que utiliza cada muestra es necesario multiplicar la cantidad de canales por la cantidad de bits que utiliza para cuantificar cada uno, como en la ecuación 7.

$$Bits\ por\ muestra = 2\ x\ 16\ [bits\ por\ muestra] = 32\ [bits\ por\ muestra]$$

Ecuación 7. Cálculo de la cantidad de bits utilizados para cuantificar

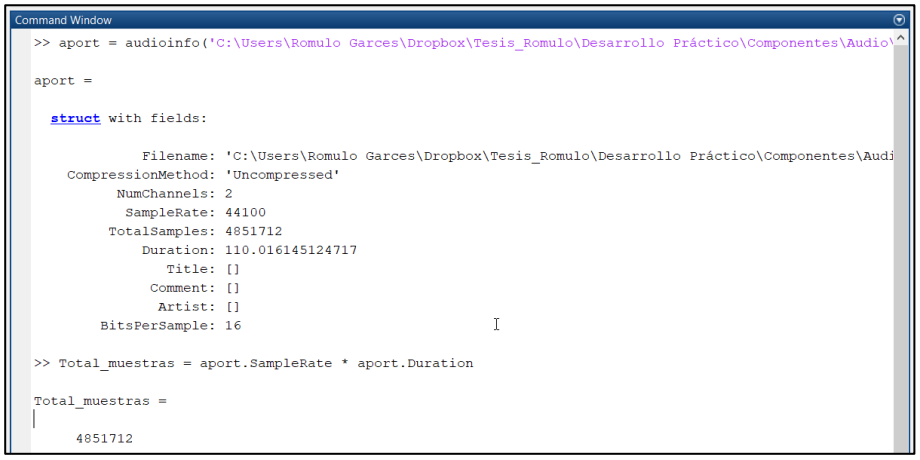


Figura 50 Características del audio del video portador

En la Figura 51, se observa como calcular el tamaño en disco del audio generado con las características expuestas anteriormente.

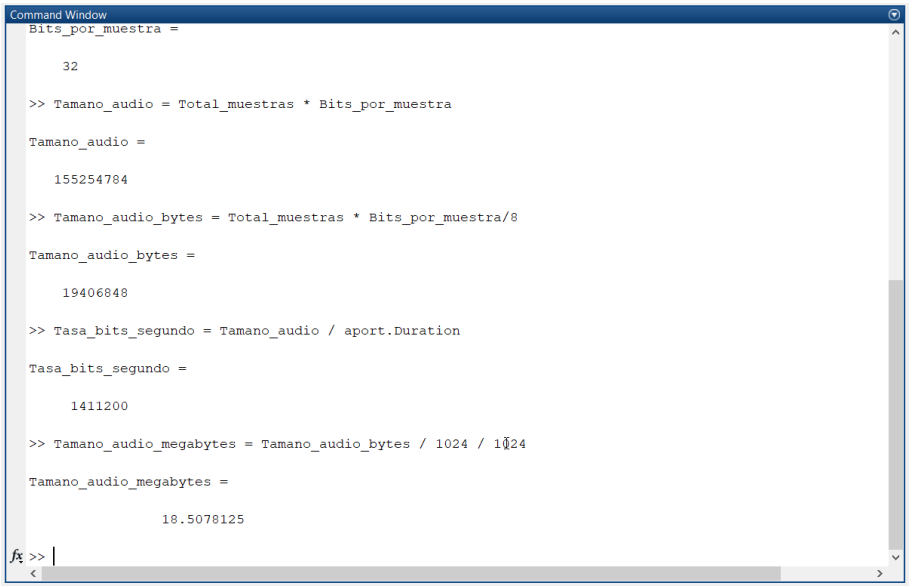


Figura 51 Cálculo del tamaño en disco del audio

Como se puede observar en la Figura 51, el tamaño en disco del archivo de audio descompuesto del video portador tiene un tamaño aproximado de 18,5 MB, lo cual concuerda con lo mostrado en la pantalla del explorador de Windows, mostrada en la Figura 52.

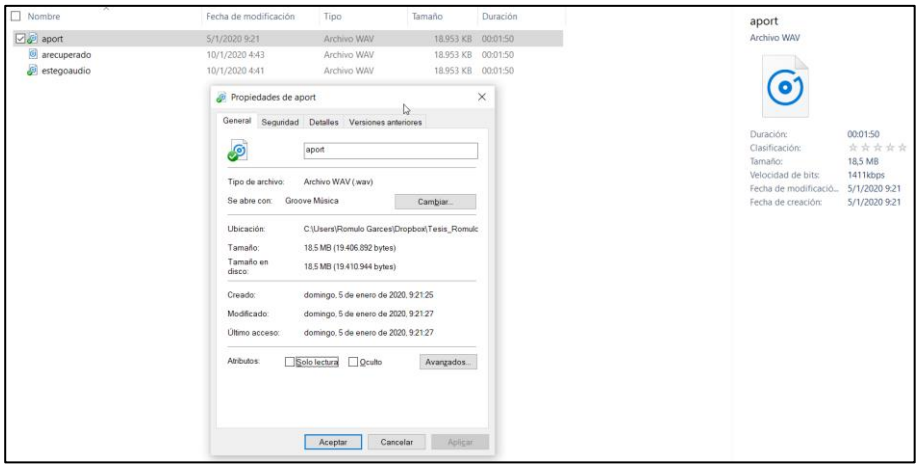


Figura 52. Propiedades del archivo de audio generado

Como se ha indicado en esta sección, en resumen, la capacidad de incrustación está determinada por 3 factores:

a. Es directamente proporcional a la frecuencia de muestreo y a la duración del video. Al utilizar el bit menos significativo de cada muestra, se tiene tantos bits como sea la multiplicación de la frecuencia de muestre por la duración en segundos del video/audio.
b. La cantidad de bits por muestra que se utilizan para cuantificar la señal de audio. Se debe tomar en cuenta que se podrían utilizar más bits comenzando desde el LSB en orden ascendente en base a la significancia del bit, pero se deben realizar pruebas para poder determinar hasta que bit se podría utilizar.
c. El tamaño del archivo generado. En el presente trabajo de investigación, se ha utilizado un archivo de 18,5 MB. Al compararlo con un archivo en formato MP3 con la misma duración, se puede observar como el tamaño es varias veces más grande, por lo que se lo debe considerar para no generar un archivo de audio demasiado pesado.

La capacidad de incrustación del método desarrollado en el presente trabajo de investigación es de 9’703.424 (4’851.712 x 2) bits.

En la Tabla 11, se puede observar que en promedio los vectores que se generaron para poder recuperar las imágenes ocultas tienen una longitud de 4’391.310, es decir que aproximadamente en el bit LSB de cada canal es posible incrustar la información de recuperación de una imagen.

Tabla 11
Tamaño de los vectores generados por la transformación de cada imagen secreta

Imagen secreta	Tamaño del vector
1	4568497
2	4375441
3	4538363
4	4256222
5	4262450
6	4943128
7	4403228
8	4170586
9	4483263
10	4442989
11	4375795
12	4201224
13	4254824
14	4572673
15	4133467
16	4278797

4.9. Imágenes recuperadas

Las imágenes que se muestran a continuación corresponden al desarrollo práctico del presente trabajo de investigación, se han ocultado un total de 16 imágenes, pero por la capacidad de incrustación solo se han podido recuperar 2. En las Figura 53 y 58 se muestran las dos imágenes objetivo (fotogramas portadores).

Figura 53. Imagen objetivo (fotograma portador) nro.1

En las Figuras 54 y 59 se muestran las imágenes secretas a ser ocultas. En las Figuras 55 y 60 se muestra el proceso de transformación de cada imagen secreta en el correspondiente fotograma portador. En las Figuras 56 y 61 se muestran los estego-fotogramas generados, y finalmente en las Figuras 57 y 62 se observan las imágenes secretas recuperadas.

Posterior a su observación, se van a medir los parámetros que sirven para determinar la calidad de las imágenes recuperadas.

Al tener solo dos imágenes recuperadas, se las denominará imagen procesada nro. 1 e imagen procesada nro. 2.

Figura 54. Imagen secreta par de la imagen objetivo (fotograma portador) nro. 1

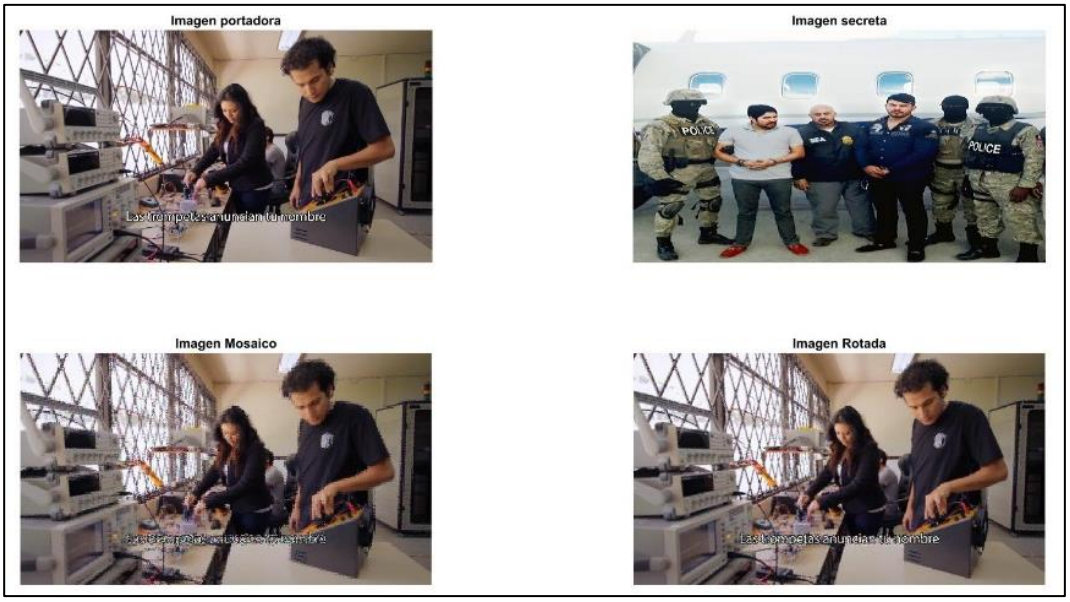


Figura 55. Proceso de transformación de la imagen secreta con imagen objetivo nro. 1

Figura 56. Estego-imagen generada nro. 1

Figura 57. Imagen secreta recuperada nro. 1

Figura 58. Imagen objetivo (fotograma portador) nro. 2

Figura 59. Imagen secreta par del fotograma portador nro. 2

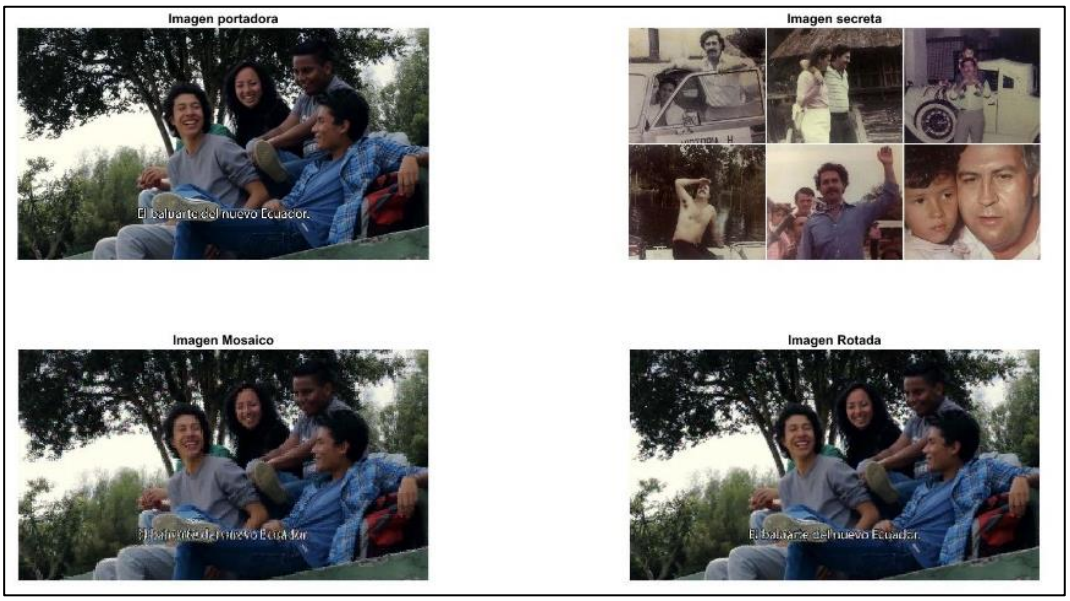


Figura 60. Proceso de transformación de la imagen secreta con la imagen objetivo nro. 2

Figura 61. Estego-imagen generada nro. 2

Figura 62. Imagen secreta recuperada nro. 2

A continuación, se realiza la medición de criterios objetivos para determinar cuáles son los resultados de la técnica esteganográfica desarrollada.

4.10. PSNR (Peak Signal to Noise Ratio)

Para cuantificar la cantidad de ruido que contiene cada imagen recuperada se ha utilizado la funcion *psnr* de Matlab®, la cual mide el ruido de la estego-imagen usando como referencia el fotograma portador y la imagen secreta.

Como se muestra en la Tabla 12, se tiene un PSNR superior al que se obtuvo en (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016) por lo que se podría decir que la técnica esteganográfica si mejora la recuperación de la imagen secreta. Además, se puede observar que al usar el filtro de Mediana se han obtenido los mejores resultados con la imagen procesada nro. 1 y con la imagen procesada nro. 2 el filtro compuesto es la mejor opción.

Tabla 12
PSNR entre las imagen objetivo, estego-imagen e imagen recuperada

Nro. de imagen procesada	Imagen de referencia	Imagen a medir	Valor resultante PSNR
1	Imagen objetivo (fotograma portador) nro. 1	Estego-imagen generada nro. 1	23,9163
1	Imagen recuperada nro. 1	Imagen secreta nro. 1	23,9778
1	Imagen recuperada nro. 1 con filtro de Mediana	Imagen secreta nro. 1	24,4673
1	Imagen recuperada nro. 1 con filtro Wiener	Imagen secreta nro. 1	23,2736
1	Imagen recuperada nro. 1 con filtro Compuesto	Imagen secreta nro. 1	23,7117
2	Imagen objetivo (fotograma portador) nro. 2	Estego-imagen generada nro. 2	23,1238
2	Imagen recuperada nro. 2	Imagen secreta nro. 2	22,7447
2	Imagen recuperada nro. 2 con filtro de Mediana	Imagen secreta nro. 2	23,0899
2	Imagen recuperada nro. 2 con filtro Wiener	Imagen secreta nro. 2	22,8783
2	Imagen recuperada nro. 2 con filtro Compuesto	Imagen secreta nro. 2	23,1241

En la Figura 63 se puede observar que el mayor valor de la medición del PSNR para la imagen procesada nro. 1, se encuentra al procesarla posterior a su recuperación con el filtro de mediana.

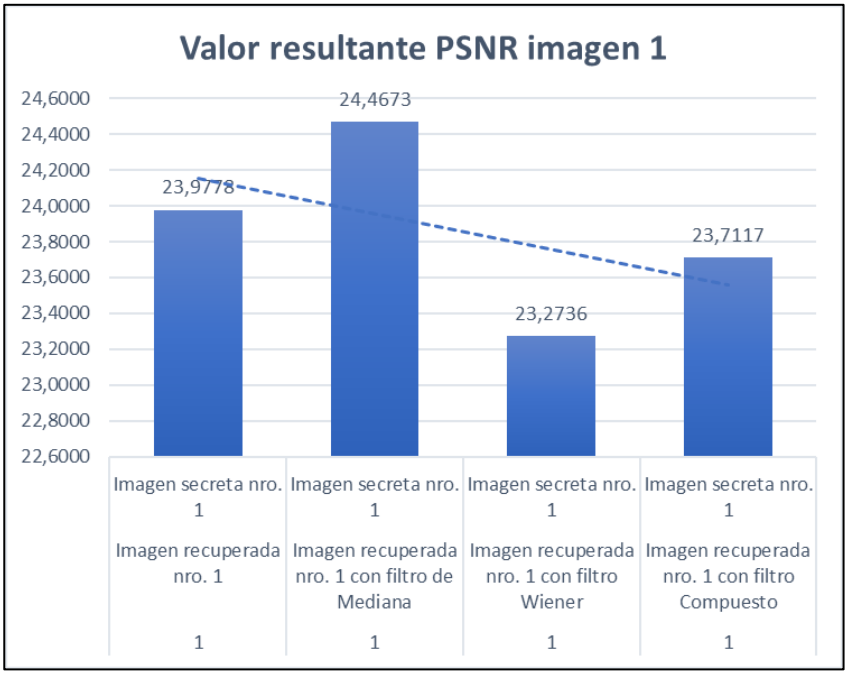


Figura 63 Resultado del cálculo PSNR con la imagen procesada nro. 1

Por otro lado, con la imagen procesada nro. 2 en la Figura 64 se observan los resultados del PSNR, estos indican que tanto el filtro de mediana como el filtro compuesto tienen valores aproximados, pero el filtro compuesto es el de mayor valor.

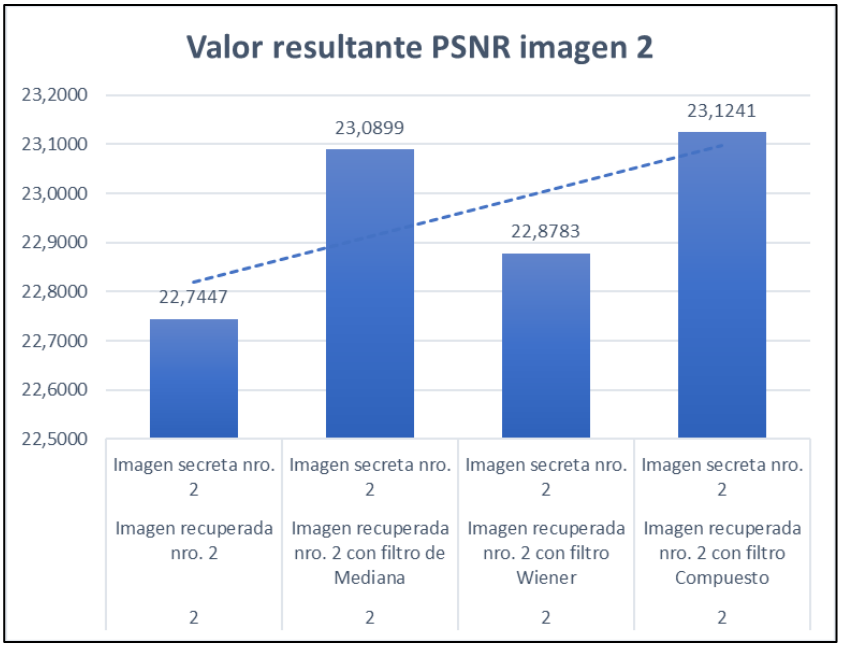


Figura 64 Resultado del cálculo PSNR con la imagen procesada nro. 2

4.11. RMSE (Root Mean Square Error)

Se realizaron las mediciones del RMSE a la estego-imagen usando como referencia la imagen portadora y la imagen secreta con referencia a la imagen recuperada. Una vez realizadas estas pruebas se han obtenido los resultados mostrados en la Tabla 13, el valor obtenido es menor al que se reflejó en (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016) por lo que se puede concluir que la técnica esteganográfica mejora la reconstrucción de las imágenes, como se observa en este caso el valor optimo es el más bajo, por lo tanto para determinar cuál es el filtro

que mejores resultados entrega, se debe considerar que para la imagen procesada nro. 1 el filtro de mediana es el que mejor resultado entrega al tener un RMSE de 15,2467, para la imagen procesada nro. 2 el filtro compuesto entrega el mejor resultado seguido muy de cerca del filtro de mediana.

Tabla 13

RMSE entre la imagen objetivo, la estego-imagen y la imagen recuperada

Nro. de imagen procesada	Imagen de referencia	Imagen a medir	Valor resultante RMSE
1	Imagen objetivo (fotograma portador) nro. 1	Estego-imagen generada nro. 1	16,2452
1	Imagen recuperada nro. 1	Imagen secreta nro. 1	16,1306
1	Imagen recuperada nro. 1 con filtro de Mediana	Imagen secreta nro. 1	15,2467
1	Imagen recuperada nro. 1 con filtro Wiener	Imagen secreta nro. 1	17,4929
1	Imagen recuperada nro. 1 con filtro Compuesto	Imagen secreta nro. 1	16,6325
2	Imagen objetivo (fotograma portador) nro. 2	Estego-imagen generada nro. 2	17,7972
2	Imagen recuperada nro. 2	Imagen secreta nro. 2	18,5911
2	Imagen recuperada nro. 2 con filtro de Mediana	Imagen secreta nro. 2	17,8666
2	Imagen recuperada nro. 2 con filtro Wiener	Imagen secreta nro. 2	18,3073
2	Imagen recuperada nro. 2 con filtro Compuesto	Imagen secreta nro. 2	17,7964

En la Figura 65 se observa que el filtro de mediana es el que menor valor genera, por lo que se concluye que este es el mejor de las 3 opciones.

Para la imagen procesada nro. 2 en la Figura 66 se observa que el filtro compuesto tiene el menor valor de RMSE por lo que este es el de mejores resultados, pero el filtro de mediana está a 0,6 décimas de igualar su valor, por lo que se concluye que el filtro de mediana es el óptimo.

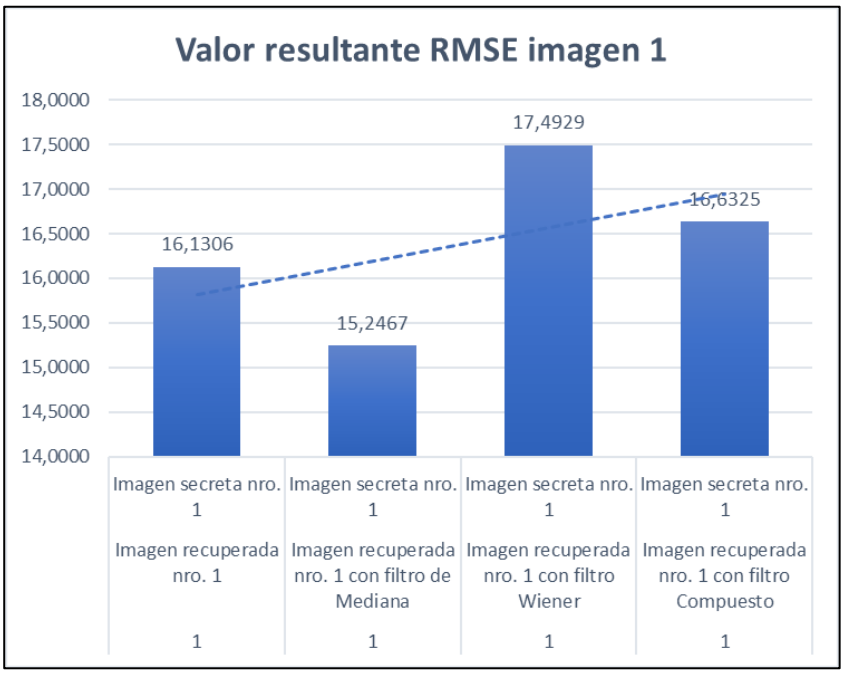


Figura 65 Resultado del cálculo RMSE con la imagen recuperada 1

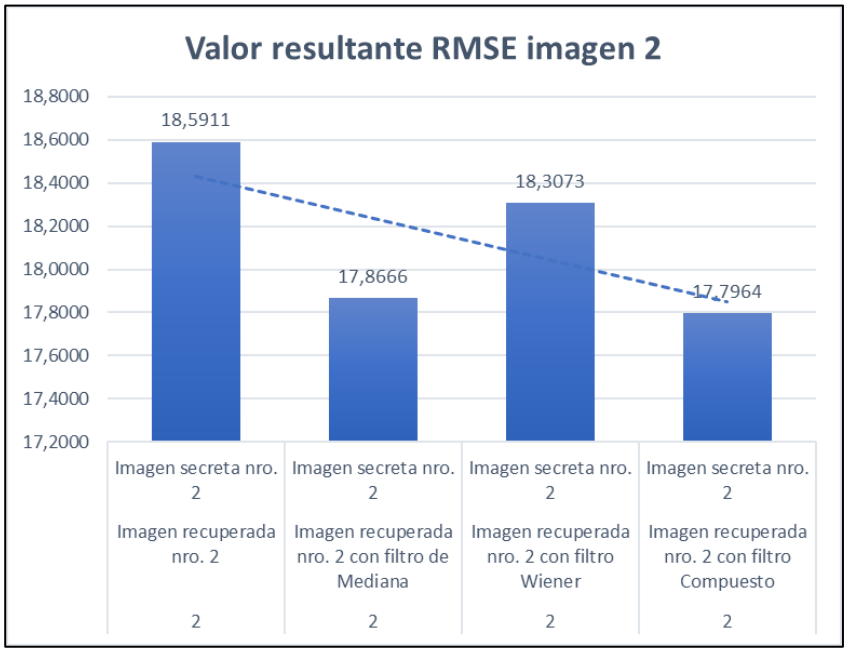


Figura 66 Resultado del cálculo PSNR con la imagen recuperada 2

4.12. SSIM (Structural Similarity Index)

Las mediciones del PSNR y RMSE evalúan errores en la imagen de una manera objetiva, la evaluación SSIM mide la similitud entre imágenes considerando 3 aspectos: luminancia, contraste y estructura. Esta métrica es de tipo índice es decir que tiene valores de 0 hasta 1, 0 representa la pérdida total de la similitud y 1 una copia exacta entre las imágenes comparadas. Con los mismos escenarios que en los casos anteriores, se han obtenido los resultados mostrados en la Tabla 14.

Tabla 14
SSIM medido

Nro. de imagen procesada	Imagen de referencia	Imagen a medir	Valor resultante SSIM
1	Imagen objetivo (fotograma portador) nro. 1	Estego-imagen generada nro. 1	0,8418
1	Imagen recuperada nro. 1	Imagen secreta nro. 1	0,8240
1	Imagen recuperada nro. 1 con filtro de Mediana	Imagen secreta nro. 1	0,8392
1	Imagen recuperada nro. 1 con filtro Wiener	Imagen secreta nro. 1	0,7280
1	Imagen recuperada nro. 1 con filtro Compuesto	Imagen secreta nro. 1	0,7571
2	Imagen objetivo (fotograma portador) nro. 2	Estego-imagen generada nro. 2	0,8020
2	Imagen recuperada nro. 2	Imagen secreta nro. 2	0,7806
2	Imagen recuperada nro. 2 con filtro de Mediana	Imagen secreta nro. 2	0,7955
2	Imagen recuperada nro. 2 con filtro Wiener	Imagen secreta nro. 2	0,7566
2	Imagen recuperada nro. 2 con filtro Compuesto	Imagen secreta nro. 2	0,7720

En la Figura 67 se observa que la mayor similitud entre la imagen secreta original y la imagen recuperada (aplicada filtros) es al utilizar el filtro de mediana.

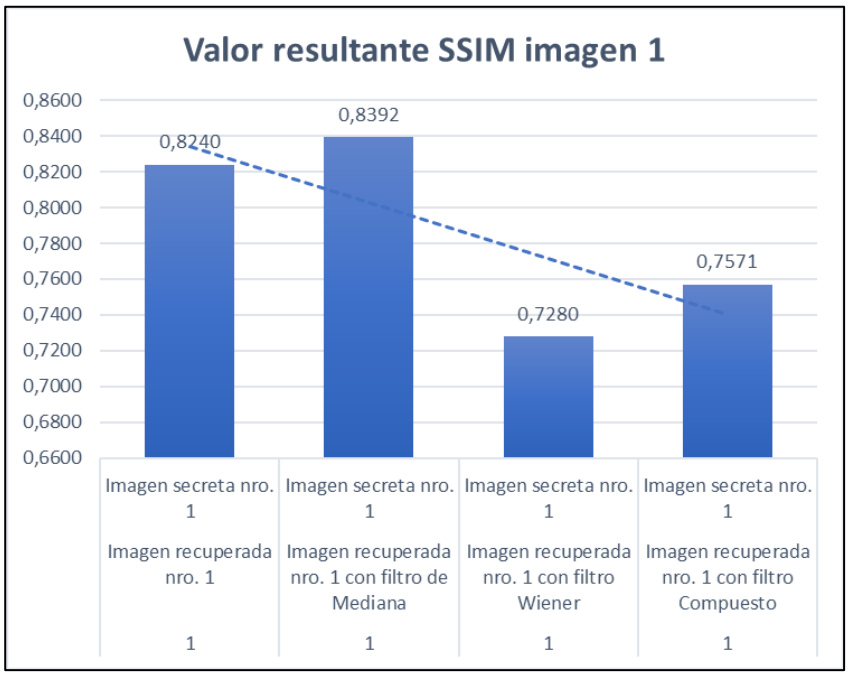


Figura 67 Resultado del cálculo SSIM con la imagen procesada nro. 1

Como se puede observar en la Tabla 14, el mejor resultado se dio al utilizar el filtro de mediana, lo que concuerda con los resultados del RMSE y PSNR. Los resultados de la recuperación de la imagen secreta son buenos, y nos permiten verificar que lo mostrado en (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016) se cumple y además se mejora con la técnica esteganográfica desarrollada en el presente trabajo de investigación. Se concluye que el filtro de mediana mejora la recuperación al reducir el efecto de pixelado provocado por la división en bloques.

En la Figura 68 los resultados muestran que el filtro de mediana es el que genera mayor similitud entre la imagen secreta correspondiente al procesamiento nro. 2 y la imagen recuperada.

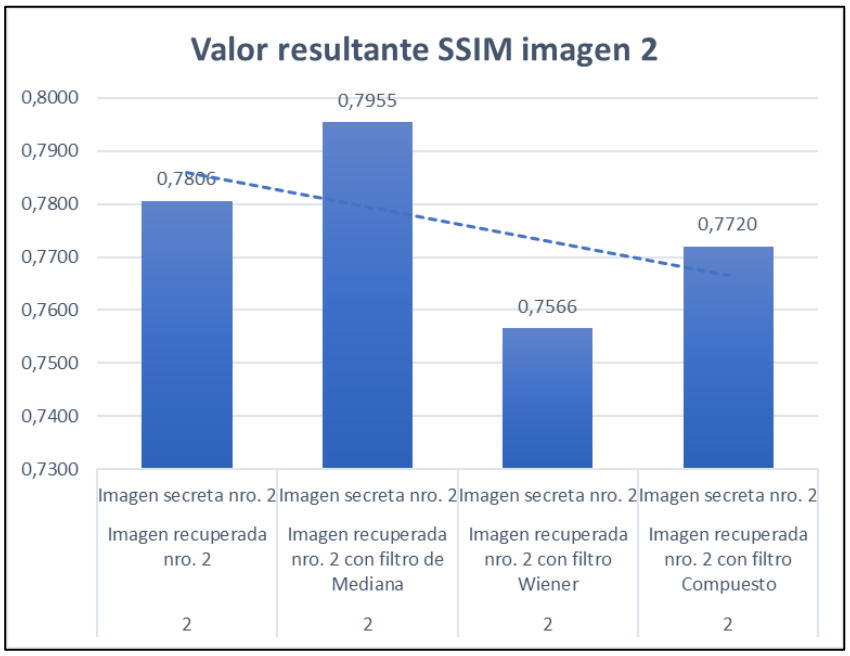


Figura 68 Resultado del cálculo SSIM con la imagen recuperada 2

Por lo tanto, con los resultados mostrados al calcular el PSNR, RMSE y el SSIM se concluye que la técnica esteganográfica ha mejorado la reconstrucción de las imágenes y el uso del filtro de mediana reduce el ruido, menora el error e incrementa la similitud entre las imágenes.

4.13. Análisis de histogramas

El mostrar los histogramas de la estego-imagen, la imagen portadora, la imagen secreta y la imagen recuperada. Nos permite visualizar como cada uno de los canales de su estructura RGB, se comportan, considerando que en el eje x está el valor de los pixeles, en este caso por usar 8 bits está en el rango de 0 a 255, en el eje y se disponen las frecuencias de cada valor de píxel.

Se puede observar en la Figura 69 el histograma del canal R de la imagen objetivo del procesamiento nro. 1 y el canal R de la estego-imagen generada en el procesamiento nro. 1. Se

observa claramente que el comportamiento de ambas imágenes es muy similar, con lo que se verifican los resultados obtenidos anteriormente.

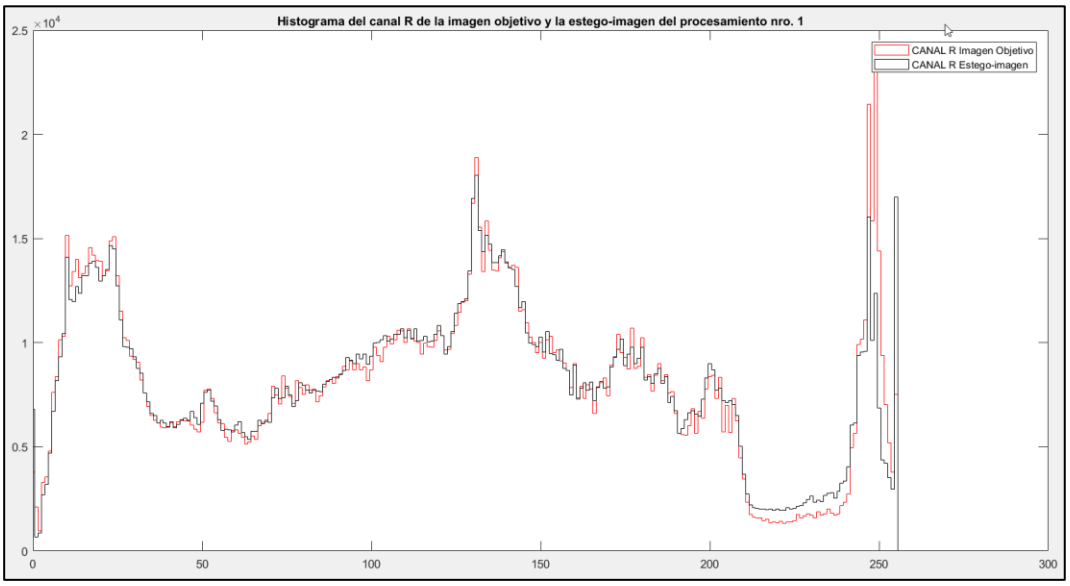


Figura 69 Histograma del canal R de la imagen objetivo y la estego-imagen nro.1

En la Figura 70 se observa el comportamiento del canal G de la imagen objetivo del procesamiento nro. 1 y el canal G de la estego-imagen generada en el procesamiento nro. 1. Lo cual demuestra que ambas imágenes tienen alta similitud.

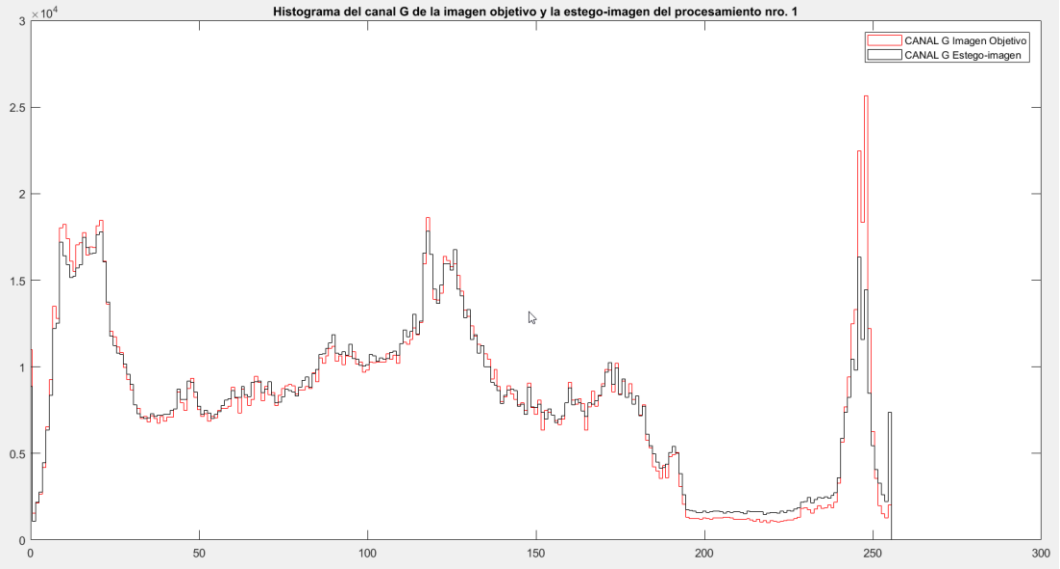


Figura 70. Histograma del canal G de la imagen objetivo y la estego-imagen nro.1

De la misma manera en la Figura 71 se observa la similitud en el comportamiento del canal B entre la imagen objetivo del procesamiento nro. 1 y la estego-imagen generada.

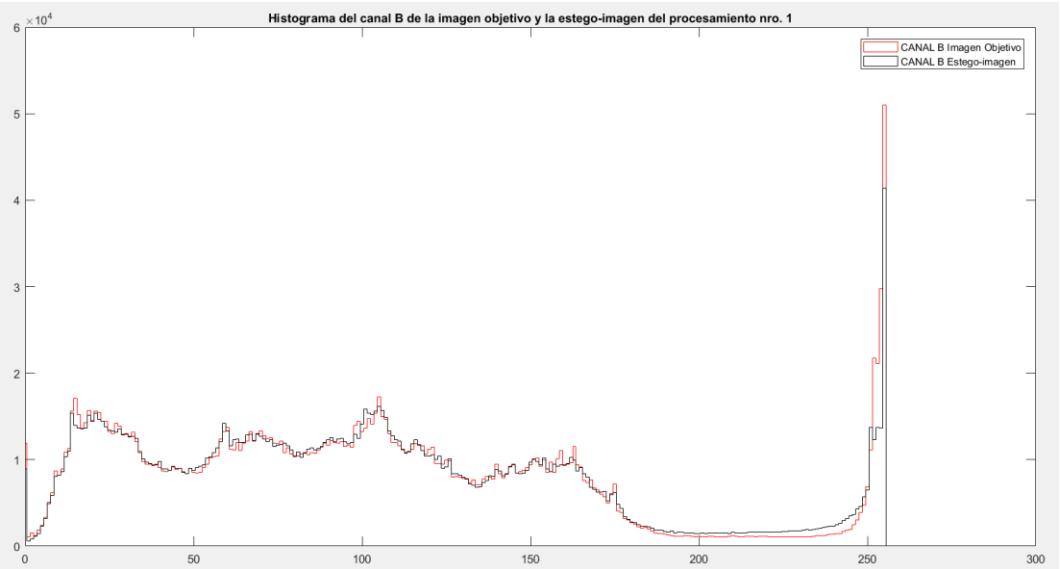


Figura 71. Histograma del canal B de la imagen objetivo y la estego-imagen nro.1

En la Figura 72 se muestra el histograma del canal R de la imagen secreta original para el procesamiento nro.1 y el canal R de la imagen recuperada procesada con el filtro de mediana.

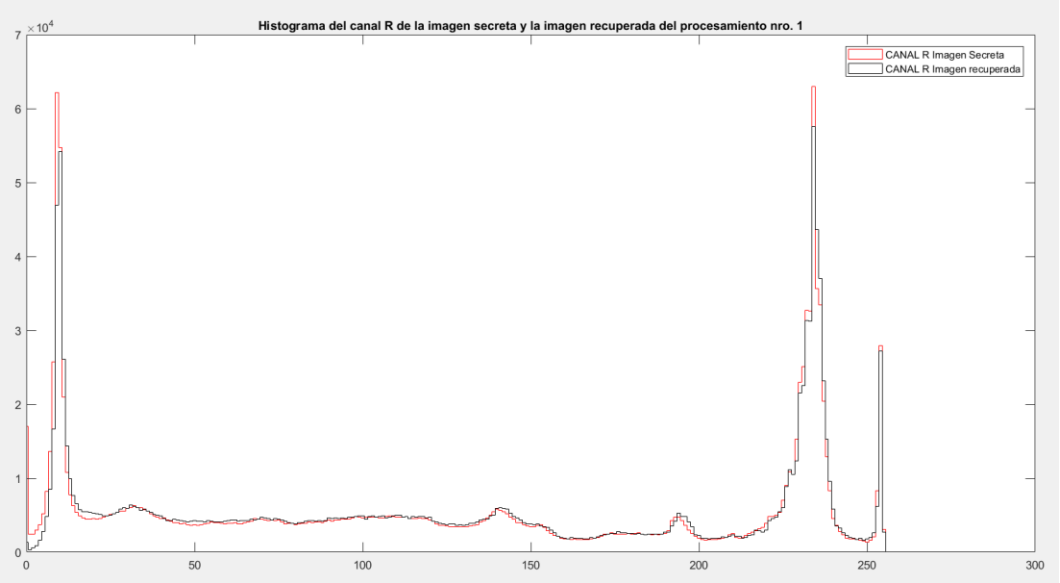


Figura 72. Histograma del canal R de la imagen secreta y la imagen recuperada nro.1

En la Figura 73 se observa la similitud que existe entre el canal G de la imagen secreta y la imagen recuperada para el procesamiento nro. 1. Y en la Figura 74 se observa la similitud del canal B existente entre la imagen secreta y la imagen recuperada.

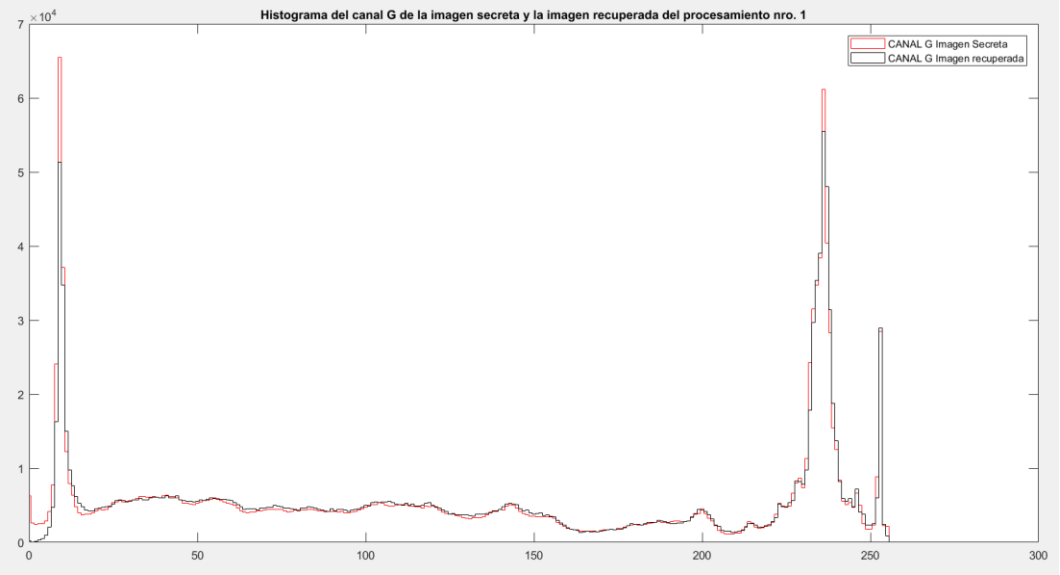


Figura 73. Histograma del canal G de la imagen secreta y la imagen recuperada nro.1

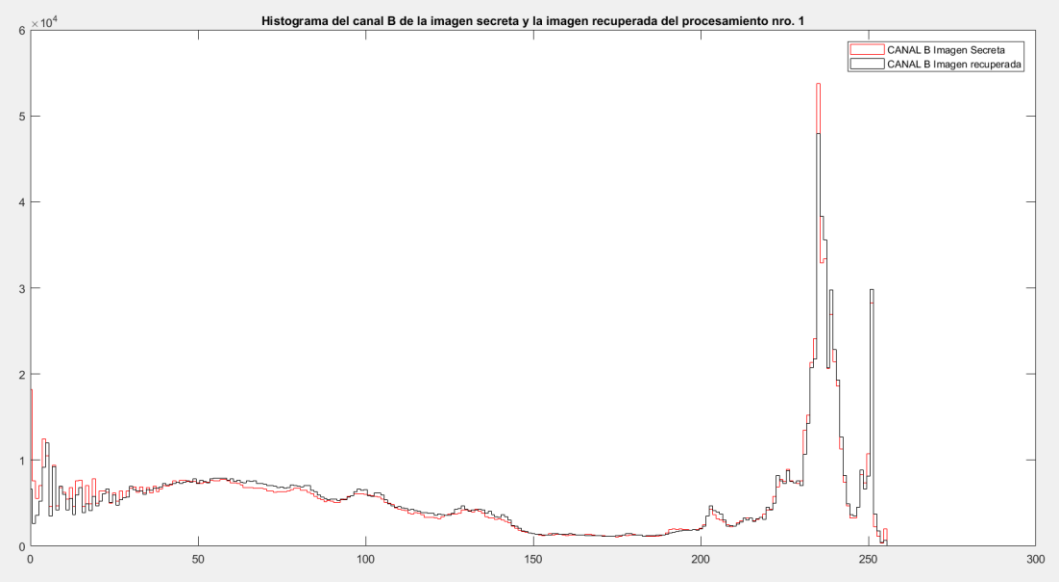


Figura 74. Histograma del canal B de la imagen secreta y la imagen recuperada nro.1

Por lo tanto, se verifica el valor de similitud entre la imagen objetivo (fotograma portador) y la estego-imagen generada, así como la similitud entre la imagen secreta original y la imagen recuperada.

4.14. Resultados del MOS (Mean Opinion Score)

Esta es una medida subjetiva de la calidad del video, por su parte visual y auditiva ya que el estego-video ha sido modificado tanto en sus fotogramas como en el audio. La encuesta fue enviada alrededor de 60 personas de las cuales respondieron 43, se utilizó la herramienta de Formularios de Google para desarrollar la encuesta. En la Tabla 15 se observa el resumen de las respuestas a las preguntas 1 y 2 de los 43 encuestados.

Tabla 15
Resumen de respuestas de las preguntas 1 y 2

Pregunta/Respuestas	1	2	3	4	5
Pregunta 1: ¿Como calificaría la calidad del video mostrado?	0	0	0	4	39
Pregunta 2: ¿Como calificaría la calidad del audio del video mostrado?	0	0	0	8	35

a. Pregunta 1: ¿Como calificaría la calidad del video mostrado?

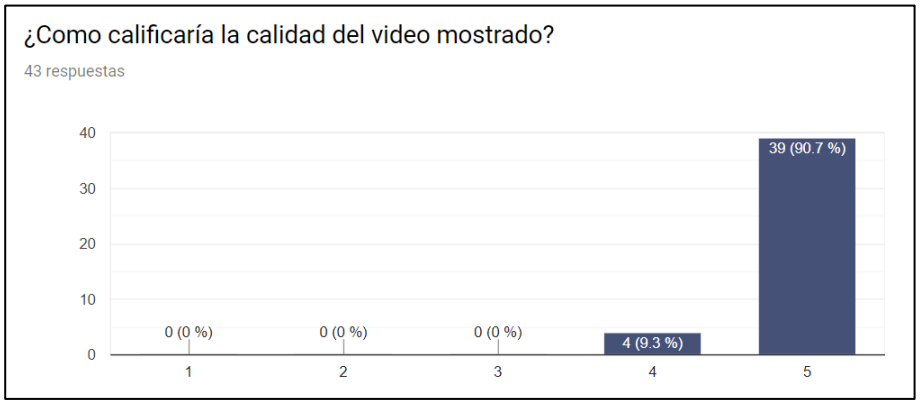


Figura 75 Resultados de la primera pregunta del MOS
Fuente: Formularios de Google

De los 43 encuestados, **39** (**90,7%**) han indicado que el video tiene una “Excelente calidad” y **4** personas es decir el **9,3%** restante, ha calificado la calidad del video como “Buena”, como se

observa en la Figura 75. Por lo tanto, se concluye que la técnica esteganográfica aplicada en el presente trabajo de investigación no afecta la calidad del video portador.

b. Pregunta 2: ¿Como calificaría la calidad del audio del video mostrado?

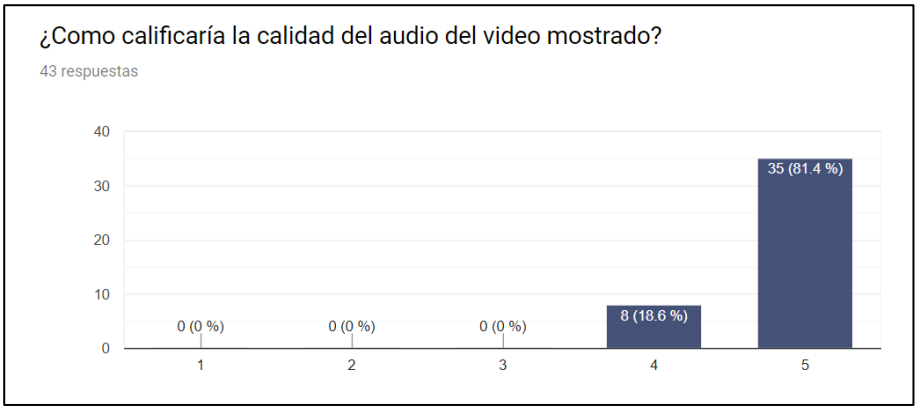


Figura 76 Resultados de la segunda pregunta del MOS
Fuente: Formularios de Google

En la Figura 76, se puede observar que **35** personas un **81,4%** de los encuestados han calificado la calidad del audio como “Excelente” y **8** personas un **18,6%** de los encuestados indican que la calidad del audio es “Buena”.

Por lo tanto, la incrustación de información en el audio del video portador se ha realizado con resultados positivos, la incrustación de información en el bit menos significativo de cada muestra no afecta la calidad del audio que se utiliza en el video portador.

c. Pregunta 3: ¿Ha notado algún cambio perceptible en el transcurso del video mostrado?

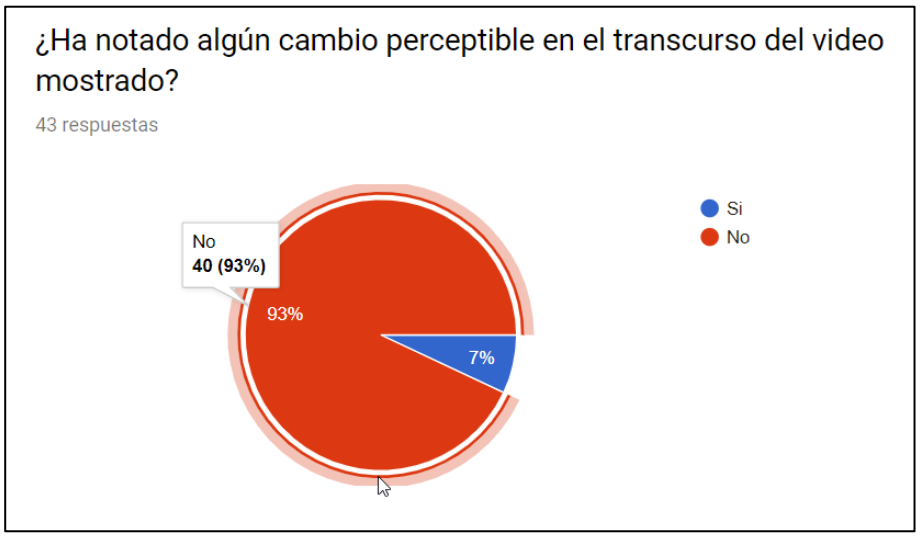


Figura 77 Resultados de la tercera pregunta del MOS
Fuente: Formularios de Google

Como se observa en la Figura 77, el **93%** de los encuestados (**40 personas**), indican que no han percibido ningún cambio en el estego-video, y el **7%** de los encuestados (**3 personas**) indican que sí.

Es importante considerar que el video portador contiene subtítulos, texto en la parte inferior que viene a ser un punto débil ya que visualmente es donde se podría detectar un pixelamiento.

d. Pregunta 4: ¿Creería usted que dentro del video se encuentra algún tipo de información oculta?

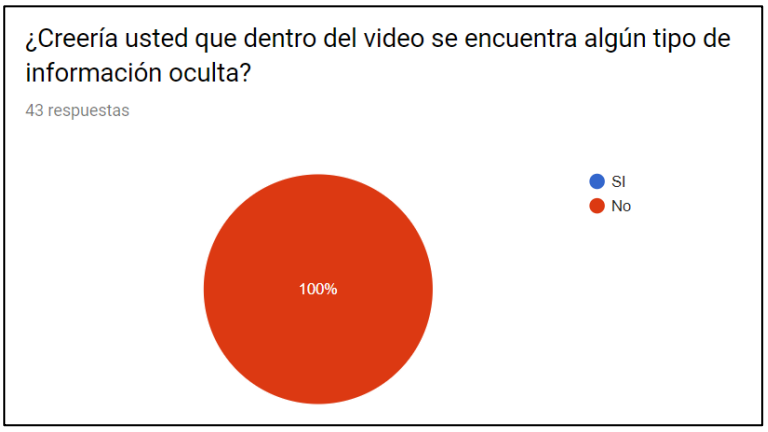


Figura 78 Resultados de la cuarta pregunta del MOS
Fuente: Formularios de Google

En la Figura 78 se observa que todos los encuestados (**100%**), es decir las 43 personas indican que no creerían que en el video mostrado exista alguna información oculta, por lo que se concluye que la técnica esteganográfica en realidad pasa desapercibida, los resultados son los esperados.

e. ¿Creería usted que dentro del audio del video mostrado se encuentra algún tipo de información oculta?

Figura 79 Resultados de la cuarta pregunta del MOS
Fuente: Formularios de Google

Como se muestra en la Figura 79, el **100%** de los encuestados indican que no creerían que en el audio del estego-video se tenga algún tipo de información oculta, por lo que se puede decir que el resultado de la técnica esteganográfica desarrollada ha sido el esperado.

CAPITULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se ha desarrollado una técnica esteganográfica basada en una transformación de color reversible y el uso del bit menos significativo del audio en un video portador, para ocultar imágenes y recuperarlas con la información oculta en el audio.
- Usar el audio como señal portadora de la información para recuperar las imágenes secretas ocultas por transformación de color reversible, es una técnica de baja complejidad pero su capacidad de incrustación se limita por el tiempo de duración y la frecuencia de muestreo.
- Se ha logrado ocultar 16 imágenes secretas, en un video de aproximadamente 2 minutos de duración con una resolución de 1920 x 1080 pixeles, de las 16 imágenes ocultas debido a la capacidad de incrustación de información en el audio, se han logrado recuperar 2. Las dos imágenes recuperadas tienen un promedio del 85% de similitud con la original, esto considerando el valor del índice evaluado con el SSIM.
- El valor PSNR correspondiente a la evaluación de las imágenes recuperadas, nos permite indicar que el ruido presente es bajo ya que con el filtro de mediana se obtiene el valor más alto que es 24,4673 para la imagen recuperada 1 y 23,0899 para la imagen recuperada 2, lo cual es una mejora a los resultados mostrados en (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)
- El valor del RMSE de la evaluación realizada a las imágenes recuperadas nos permite indicar que se tiene el error relativamente bajo, ya que con el uso del filtro de mediana en

la imagen recuperada 1 se tiene un valor de 15,2467 y para la imagen 2 con el filtro de mediana se tiene un valor de 17,8666, lo cual mejora los resultados mostrados en (Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy., 2016)

- La cantidad de imágenes secretas que se pueden ocultar en el video portador depende de la detección de cambios de escena, en la técnica esteganográfica que se ha desarrollado en el presente trabajo de investigación, se ha evidenciado que se podrían insertar hasta 23 imágenes secretas, con el video portador utilizado.
- Al evaluar con el MSE, PSNR y el SSIM a la señal del estego-audio y el audio recuperado en comparación al audio original, se comprueba que la incrustación de datos es imperceptible.
- Los resultados de la encuesta tipo MOS nos indican que la técnica esteganográfica desarrollada para ocultar información en un video es imperceptible a simple vista.

5.2. Recomendaciones

- Se recomienda utilizar la técnica esteganográfica desarrollada en el presente trabajo de investigación en videos que no contenga subtítulos o letras ya que esto se vuelve un punto débil al momento de visualizar el contenido, puesto que es difícil evitar el pixelamiento en estas zonas de la imagen.
- Utilizar los parámetros de evaluación como indicadores para mejorar procesos, como en este caso se utilizó el SSIM para detectar cambios de escena automáticamente y de la misma manera sirve para evaluar la similitud entre la imagen recuperada y la original.

- Elegir imágenes secretas de la misma o menor resolución que el video portador, ya que al momento de recuperarlas y se las vuelva a su tamaño original, el pixelamiento provocado por la división de imágenes en bloques será menos evidente.
- Generar histogramas y analizarlos permite visualizar como es el comportamiento de cada uno de los canales RGB que componen las imágenes, y cuales con los cambios evidentes.

5.3. Trabajos futuros

- Enfocarse en desarrollar un método que permita generar un estego-video con el mismo tamaño en disco que el video original, además implementar el programa desarrollado en el presente trabajo de investigación con una interfaz gráfica la cual permita al usuario comprender de mejor manera como es que se va construyendo el estego-video. Investigar y evaluar los resultados de utilizar más del bit menos significativo del audio para incrustar información, tomando en cuenta que con el LSB es imperceptible la información insertada. Además, se podría modificar el tamaño del bloque en el que se divide la imagen secreta y portadora para realizar la transformación con el fin de medir cuales son los resultados objetivos de las evaluaciones de RMSE, PSNR y SSIM.

Referencias

(S.f.). Obtenido de http://electronicadigitaltu.blogspot.com/

Aarón, p. (21 de enero de 2009). *Crónicas de un watermarkero*. Obtenido de crónicas de un watermarkero: http://watermarkero.blogspot.com/2009/01/

Aguilera, d. G. (2010). *Introducción al análisis de imagen.* Salamanca: Universidad de Salamanca.

Antonio, p. (s.f.). *Comunicación e información, perspectivas teóricas.* México: trillas.

C.P.Sumathi, T.Santanam, G.Umamaheswari. (2013). A study of various steganographic techniques used for information hiding. *International journal of computer science & engineering survey (ijcses) vol.4, no.6,* 17.

Cad. (s.f.). *Tecnologías de la informaación*. Obtenido de edición de imágenes: http://platea.pntic.mec.es/~lgonzale/tic/imagen/conceptos.html

Carlos Alberto Chávez García, Leonardo Alfonso Silva Armijos. (2019). *Encriptación de imágenes dicom en hdfs para big data.* Quito, Ecuador: Universidad Politécnica Salesiana Sede Quito.

Carlos Eduardo Rodríguez Guayaquil, Freddy Acosta B. (2016). *Estudio y desarrollo de una aplicación de esteganografía para enviar datos en archivos de audio, orientado a la seguridad en los sistemas de comunicación.* Sangolquí: Universidad de las Fuerzas Armadas-ESPE.

Carlos Eduardo Rodriguez Guayaquil, Freddy Roberto Acosta Buenaño. (2016). *Estudio y desarrollo de una aplicación de esteganografia para enviar datos en archivos de audio, orientado a la seguridad en los sistemas de comunicación.* Sangolquí: Universidad de las Fuerzas Armadas - ESPE.

Cjmagnate. (10 de marzo de 2017). *Electrónica digital*. Obtenido de introducción a la electrónica digital: http://electronicadigitaltu.blogspot.com/2017/

Cristian Marcelo Vasco Estupiñan, Freddy Roberto Acosta Buenaño. (2018). *Una nueva técnica de transmisión segura de imágenes aplicando transformaciones de color reversibles en zonas ruidosas de la imagen.* Sangolquí: Universidad de las Fuerzas Armadas-ESPE, Ecuador.

Cuzco R., Mantilla C., Vaca B. & Acosta R. (2018). *Mejora en la seguridad de un método esteganográfico aplicando criptografía.* Revista electrónica ciencia digital.

Daniel Lerch-Hostalot, David Meglas. (2014). *Esteganografía en zonas ruidosas de la imagen.* Recsi 2014.

Ecured. (2019). *Ecured*. Obtenido de ecured: https://www.ecured.cu/esteganograf%c3%ada#la_criptograf.c3.ada_y_la_esteganograf.c3.ada

Eterovic Jorge, Cipriano, Marcelo. (2018). *Una aproximación a la seguridad de las comunicaciones en internet de las cosas usando criptografía ligera.* Investigadores USAL.

Fernandez, D. P. (mayo de 2018). *Tecnonucleous*. Obtenido de tecnonucleous: https://tecnonucleous.com/2018/03/26/encriptar-o-cifrar/

Herrera Arcentales Xavier Eduardo, Acosta Buenaño Freddy. (2018). *Análisis del método esteganográfico como soporte a la seguridad de la información mediante la ocultación de información secreta dentro de un video.* Sangolquí, Ecuador: Universidad de las Fuerzas Armadas-ESPE.

Images, S. H. (15 de agosto de 2018). *Alamy.* Obtenido de https://www.alamy.es/cifrado-de-cesar-ilustracion-image245868009.html

John G. Proakis y Dimitris G. Manolakis. (2007). *Tratamiento digital de señales.* Madrid: Pearson Educación s.a.

London, a. (21 de abril de 2018). *Techradar*. Obtenido de explicación de hfr: https://www.techradar.com/news/hfr-explained-high-frame-rate-is-coming-to-tvs-heres-what-you-need-to-know

Lugo., Pedro Chávez. (2018). *La criptografía clásica en la privacidad y protección de datos.* Universidad Michoacana de San Nicolas de Hidalgo.

Martinez, E. (10 de julio de 2017). *Artículos sobre redes, telecomunicaciones y tecnologías de la información*. Obtenido de conversión analógico-digital (adc): http://www.eveliux.com/mx/curso/conversion-analogico-digital.html

Messner., Victor Cracel. (2018). *Estudio e implementación eficiente de algoritmos criptográficos.* Instituto alberto luiz coimbra de posgraduación de ingeniería (coppe) Universidad Federal de Rio de Janeiro.

Onofre Concha Gabriela Estefanía, Acosta Buenaño, Freddy. (2016). *Desarrollo y análisis de una técnica esteganográfica en zonas ruidosas de la imagen mediante transformaciones de color reversibles.* Sangolquí: Universidad de las Fuerzas Armadas-ESPE, Ecuador.

Pinargote., Hermes Quintero. (2019). *Análisis de esteganografía sobre el protocolo ipv6 como alternativa para una comunicación segura de datos.* Riobamba, Ecuador: Escuela Superior Politécnica de Chimborazo.

Press, e. (30 de junio de 2010). *Portal tic*. Obtenido de el fbi destapa una red de espías rusos que encriptaban datos en webs públicas: https://www.europapress.es/portaltic/internet/noticia-fbi-destapa-red-espias-rusos-encriptaban-datos-webs-publicas-20100630111528.html

Rodríguez, H. (s.f.). *Imagen digital conceptos básicos* (2da ed., vol. Colección bit & píxel). Marcombo.

Salgero, J. L. (22 de mayo de 2018). *Aenoa*. Obtenido de subvención estatal ocupados 2018 de formación de tics.: http://www.aenoa.com/subvencion-estatal-ocupados-2018-de-formacion-de-tics/

School, O. B. (2019). *Obs*. Obtenido de seguridad de la información, un conocimiento imprescindible: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

Seo, C. (3 de junio de 2019). *Caymans seo*. Obtenido de caymans seo: https://caymansseo.com/diferencias-entre-informacion-y-datos

Soliman, Samir S. (1999). *Señales y sistemas contínuos y discretos.* Madrid: Prentice Hall Iberia.

The Mathworks, Inc. (11 de julio de 2019). *Documentación mathworks*. Obtenido de documentación mathworks: https://la.mathworks.com/help/index.html

Vidal, M. (s.f.). *Dzoom*. Obtenido de https://www.dzoom.org.es/descubre-que-es-la-proporcion-aurea-y-como-puede-ayudarte-en-la-composicion-de-tus-fotos/

Ya-Lin Lee, Wen-Hsiang Tsai. (2014). A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. *IEEE transactions on circuits and systems for video technology, vol. 24, no. 4*, 695.

Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, Eero P. Simoncelli. (2014). Image quality assessment: from error visibility to structural similarity. *Ieee transactions on image processing, vol. 13, no. 4*, 14.

Anexos