UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

APLICACIÓN DE TÉCNICAS FORENSE PARA ANÁLISIS DE LA INTEGRIDAD DEL CONTENIDO EN VIDEOS DIGITALES.

AUTOR

MUÑOZ ROCA, ROGER ALEXANDER

EXAMÉN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

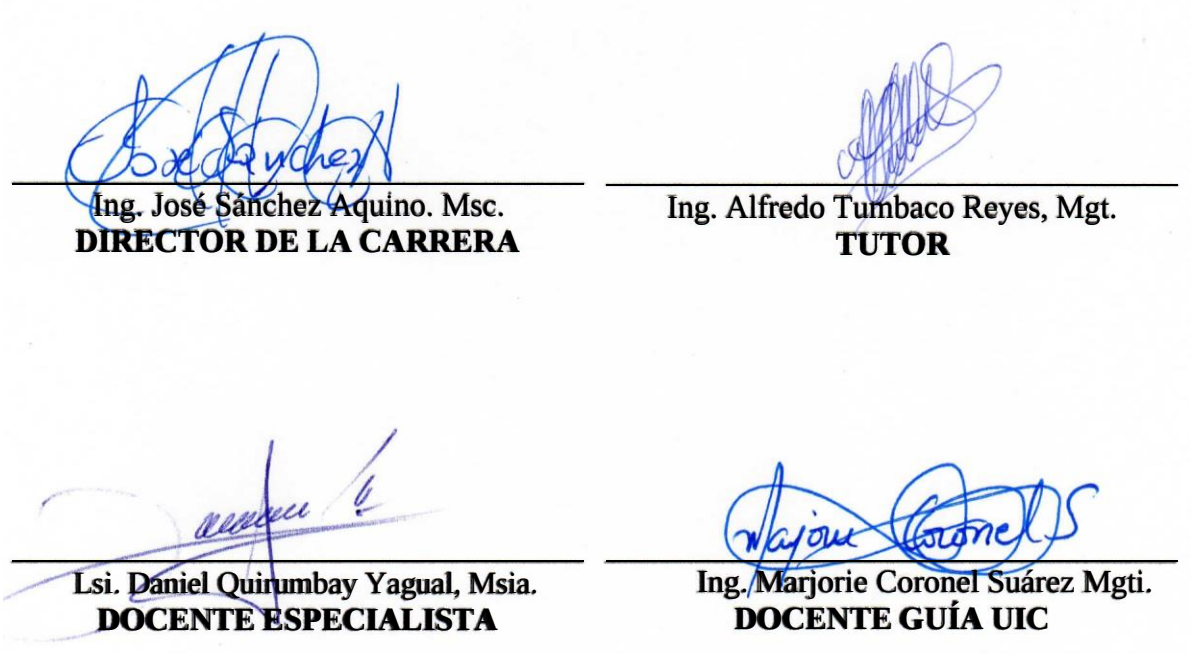
Ing. Alfredo Ramón Tumbaco Reyes, Mgti.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN



Ing. José Sánchez Aquino. Msc.
DIRECTOR DE LA CARRERA

Ing. Alfredo Tumbaco Reyes, Mgt.
TUTOR

Lsi. Daniel Quirumbay Yagual, Msia.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por MUÑOZ ROCA ROGER ALEXANDER, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 13 días del mes de diciembre del año 2024

TUTOR

Firmado electrónicamente por:
ALFREDO RAMON TUMBACO REYES

Ing. Alfredo Ramón Tumbaco Reyes, Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **MUÑOZ ROCA ROGER ALEXANDER**

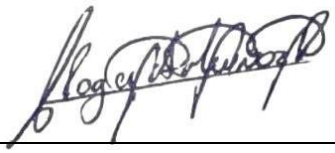
DECLARO QUE:

El trabajo de Titulación "APLICACIÓN DE TÉCNICAS FORENSE PARA ANÁLISIS DE LA INTEGRIDAD DEL CONTENIDO EN VIDEOS DIGITALES" previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 13 días del mes de diciembre del año 2024

EL AUTOR



MUÑOZ ROCA ROGER ALEXANDER

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado "APLICACIÓN DE TÉCNICAS FORENSE PARA ANÁLISIS DE LA INTEGRIDAD DEL CONTENIDO EN VIDEOS DIGITALES", presentado por el estudiante, MUÑOZ ROCA ROGER ALEXANDER fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al XX%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

RogerM;uñoz - Examen Complexivo

3% Textos sospechosos

3% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas
3% Idiomas no reconocidos (ignorado)
9% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: RogerM;uñoz - Examen Complexivo.docx
ID del documento: b90fb6e9d913c7e52542a520f6274f0570b1db66
Tamaño del documento original: 13,37 MB
Autores: []

Depositante: ALFREDO RAMÓN TUMBACO REYES
Fecha de depósito: 5/12/2024
Tipo de carga: interface
fecha de fin de análisis: 5/12/2024

Número de palabras: 11.109
Número de caracteres: 75.938

TUTOR

Firmado electrónicamente por:
ALFREDO RAMON TUMBACO REYES

Ing. Alfredo Ramón Tumbaco Reyes, Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **MUÑOZ ROCA ROGER ALEXANDER**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 13 días del mes de diciembre del año 2024

EL AUTOR

MUÑOZ ROCA ROGER ALEXANDER

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a mi director de tesis, por su invaluable orientación y apoyo durante todo el proceso de investigación. Sus consejos y paciencia fueron cruciales para la realización de este trabajo.

Agradezco también a mi familia y amigos por su constante apoyo y comprensión. Su motivación y confianza en mí han sido fundamentales para alcanzar este logro.

Roger Alexander, Muñoz Roca

DEDICATORIA

Con gratitud y amor, dedico este trabajo a mis queridos padres, quienes con su incansable apoyo, consejos sabios y amor incondicional han sido mi fuente de fortaleza y motivación durante este largo y arduo camino. Sus sacrificios y esfuerzos han sido la base sobre la cual he construido mis sueños y aspiraciones. Agradezco profundamente su confianza en mí y su constante estímulo para que nunca dejara de luchar por alcanzar mis metas.

Asimismo, quiero dedicar este trabajo a mis profesores y amigos, quienes me han acompañado y guiado en este proceso de aprendizaje

Roger Alexander, Muñoz Roca

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este proyecto se centra en la implementación de técnicas forenses para analizar la integridad de videos digitales, utilizando herramientas de código abierto que permiten verificar su autenticidad. Mediante estas técnicas se plantea un método en Python lo cual sirve para crear códigos hash, verificar y comparar videos con información guardada en un archivo JSON. Las verificaciones que se hacen en metadatos importantes tales como representaciones videográficas, el tiempo que dura un audio, voz, pequeños o grandes fragmentos, resoluciones amplia y alta, y finalmente la tasa de cuadros por segundos o fotogramas. Al mismo tiempo se efectuaron sistemáticas actuales que sirvieron para la identificación de los cambios explícitos en los contenidos multimedia o videos. Como primer plano en las conclusiones se presenta la función de PyQt6, que esta permite el perfeccionamiento del uso y facilidad que se obtiene en un análisis de una forma positiva, inclusivamente para aquellos individuos que navegan sin instrucciones previas. El código generado reduce el tiempo del proceso al proporcionar los resultados en cuestión de segundo a diferencia de otros softwares que necesitan más tiempo para llegar a un mismo resultado. Esta metodología responde un recurso eficaz y práctico para estimar la legitimidad de los videos digitales.

Palabras claves: Videos Digitales, Técnicas Forenses, Python, Funcionalidad, Software.

ABSTRACT

This project focuses on the implementation of forensic techniques to analyze the integrity of digital videos, using open source tools that allow verifying their authenticity. Using these techniques, a method is proposed in Python which is used to create hash codes, verify and compare videos with information saved in a JSON file. The verifications are made on important metadata such as videographic representations, the duration of an audio, voice, small or large fragments, wide and high resolutions, and finally the rate of frames per second or frames. At the same time, current systematics were carried out that served to identify explicit changes in multimedia content or videos. As a foreground in the conclusions, the function of PyQt6 is presented, which allows the improvement of the use and ease obtained in an analysis in a positive way, including for those individuals who navigate without prior instructions. The generated code reduces the process time by providing the results in a matter of a second unlike other software that takes more time to reach the same result. This methodology is an effective and practical resource to estimate the legitimacy of digital videos.

Keywords: Digital Videos, Forensic Techniques, Python, Functionality, Software.

INTRODUCCIÓN

En la era de la información, la manipulación de contenido multimedia se ha convertido en un problema recurrente, impulsado por la accesibilidad de herramientas avanzadas de edición digital. La facilidad con la que se pueden modificar videos digitales representa un desafío significativo para la autenticidad y la confianza en estos archivos, especialmente en contextos legales, académicos y de seguridad. En contextualización a la presente indagación se resalta la sorprendente necesidad de desplegar sistemáticas prácticas para asegurar la moralidad de la multimedia digital, proporcionando la identificación de posibles transformaciones o cambios y manteniendo su naturalidad.

El siguiente proyecto investigación para titulación denominado "Aplicación de técnicas forenses para análisis de integridad del contenido en videos digitales", presenta un procedimiento transformador a través del estudio de metodologías forenses amparados por equipos de códigos abiertos. La aplicación del siguiente trabajo se enfatiza en la ejecución de notaciones avanzados en Python que se centrarán en la automatización de hashes y la digitalización causal de videos, así como la extracción programática de metadatos para detectar alteraciones en videos y asegurar la credibilidad de la información. Se busca cubrir la accesibilidad y el uso de estos procedimientos a través de interfaces gráficas basadas en PyQt6 que ayuden en el análisis tanto de expertos como de usuarios que solo poseen conocimientos elementales.

La presente investigación presenta III capítulos, lo cual en el capítulo I se expone el marco teórico y práctico en lo que llevara a cabo el proyecto. Por primer punto se comienza revisando los antecedentes de la variable independiente y dependiente, lo cual se respalda las cuestiones de llevar a delante el proyecto de investigación. Por tanto, se tratan los métodos en las programaciones de edición y la sencillez con la que cualquier individuo, incluso sin instrucciones previas puede llegar a manipular los contenidos de plataformas audiovisual.

En el capítulo mencionado con anterioridad se enfatiza una alarmante preocupación por los cambios éticos que se tiene en los sectores tales como justicia y seguridad,

como también en los medios de comunicación, ya que en ocasiones se utilizan videos como pruebas en investigaciones judiciales.

Por consiguiente, en el capítulo también abarca datos forenses, lo cual es una disciplina principal que se envuelve con las relaciones de los análisis y las protecciones que solicitan evidencia digital. Además, estas metodologías se usan para el análisis los contenidos multimedia, que incluyen encontrar

Describe los métodos forenses que se utilizan para analizar videos digitales, incluidos la detección de modificación de fotogramas, la identificación de la fuente de archivos de video y la extracción de metadatos de los archivos de video. Los objetivos generales y específicos del proyecto también se describen aquí, especificando los resultados que se espera lograr en esta fase, como la implementación de un sistema capaz de verificar la integridad de los videos y aplicar algoritmos de hash para garantizar que los archivos no han sido modificados.

La última parte del capítulo aborda la justificación del proyecto, enfatizando la necesidad de tener herramientas que regulen la verificación rápida y eficiente de videos digitales en un país como Ecuador, donde los delitos informáticos están creciendo junto con la adopción de técnicas forenses altamente efectivas.

El Capítulo II describe los marcos teóricos y las metodologías para llevar a cabo su proyecto. La primera parte de este capítulo introduce brevemente la noción de análisis forense digital, que se refiere a un campo que permite la detección de modificaciones aplicadas a archivos multimedia. Se incluyen algunas definiciones importantes para autenticidad de video, algoritmos hash y las diversas herramientas de práctica de análisis forense, como ExifTool y FFmpeg. Se busca dar el contexto sobre lo que se basa este proyecto y también es relevante para conectar la teoría con la práctica, explicando cómo estas tecnologías se relacionan con los objetivos de análisis de video. Después de eso, se explica la metodología utilizada para desarrollar el sistema.

Se detalla el enfoque de investigación utilizado para el análisis forense de los videos, que incluye la recolección de datos a través de herramientas especializadas, el análisis de los metadatos y la detección de alteraciones en los fotogramas.

Además, se aborda la técnica de **hashing**, que es esencial para la verificación de la integridad de los videos, y se describe cómo esta técnica puede identificar alteraciones incluso a nivel de fotograma. El capítulo discute, además, las herramientas involucradas en el desarrollo del sitio, incluyendo Python para programar algoritmos o PyQt6 para construir la interfaz gráfica. La solución propuesta para el problema identificado se presenta en el Capítulo III, que constituye el núcleo técnico del proyecto.

Esta sección explica los requisitos del sistema propuesto. Los requisitos funcionales proporcionan una comprensión profunda de lo que el sistema debe hacer (por ejemplo, comparar videos a través de su hash, extraer metadatos y detectar cambios) en comparación con los no funcionales que describen sus características de rendimiento, tales como usabilidad, escalabilidad o capacidad de respuesta.

Esta sección también introduce los diagramas de casos de uso, que ilustran la interacción de los usuarios con la interfaz del sistema y las características ofrecidas en dicha interfaz. El proceso de comparación de videos, análisis de metadatos y creación de informes sobre las manipulaciones detectadas en la señal final se ilustra con esquemas.

El capítulo también elabora sobre la arquitectura del sistema, explicando cómo varios componentes, como la extracción de metadatos y el cálculo de hash, trabajan entre sí para proporcionar una solución unificada y eficiente. Describimos también el proceso de diseño de la interfaz gráfica, muy importante para que los usuarios no técnicos puedan utilizar el sistema fácilmente. Esta interfaz, diseñada con PyQt6, permite a los usuarios navegar fácilmente a través de videos y ver los resultados de su comparación de manera clara y accesible.

Se espera que esta investigación no solo avance la capacidad técnica de los investigadores en el campo del análisis forense de video digital, sino que también produzca una herramienta práctica que pueda ser utilizada por una variedad de distintas instituciones académicas, legales y de seguridad. Además, el desarrollo de este sistema fortalecerá las competencias en ciberseguridad y análisis forense dentro del ámbito nacional, alineándose con los objetivos estratégicos de seguridad integral establecidos en el Plan de Creación de Oportunidades de Ecuador.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1. Antecedentes

En la actualidad, existen numerosos programas de código abierto en internet que permiten manipular y modificar el contenido de videos digitales. Con acceso al material adecuado, cualquier persona podría realizar estos cambios, transformando el contenido original de un video y generando una versión alterada [1].

La informática forense es la disciplina que se encarga de recolectar, procesar, investigar y preservar datos de dispositivos informáticos, con el fin de que puedan ser presentados como pruebas legales [2]. Para llevar a cabo este proceso de manera exhaustiva y precisa, se utilizan herramientas de software especializadas. Estas herramientas permiten realizar análisis detallados durante períodos prolongados, lo que facilita la obtención de resultados altamente precisos y confiables para investigaciones complejas [2].

Basándonos en estadísticas publicadas por el diario El Telégrafo en su artículo de junio de 2014, se presenta el siguiente diagrama. En él se observa que el año 2011 registró el mayor número de denuncias [3].

Fig. 1 Número de denuncias años 2010-2014
Fuente: Diario El telégrafo junio 2014

La facilidad para manipular imágenes y videos digitales ha crecido de manera notable en los últimos años, siendo ahora accesible para el usuario promedio a

través de programas ampliamente utilizados como Adobe Photoshop, GIMP y Adobe Premiere. Las manipulaciones inter-fotograma (inter-frame) se centran en la modificación de la relación temporal entre los diferentes fotogramas. Para alterar esta correlación temporal en los videos, es posible insertar, duplicar, intercambiar o eliminar cualquiera de los fotogramas que los componen, lo que puede llevar a resultados que alteran significativamente la percepción del contenido original [4].

En Madrid, el investigador Quinto Carlos, junto con el destacado grupo GASS, ha llevado a cabo un estudio exhaustivo sobre los distintos contenedores multimedia que almacenan la información de un video. Este análisis comprende no solo los fotogramas y su secuencia, sino también los metadatos asociados con imágenes y videos, además de la información de diseño en el caso del formato MP4, que proporciona un contexto importante sobre cómo se organiza y almacena la información audiovisual [5].

Un informe elaborado por la empresa importadora de seguridad informática, Digiware, indica que Colombia es uno de los países con más casos reportados de ataques de ciberseguridad, robo de información personal y fraude en línea, lo cual genera preocupaciones sobre la protección de los datos y la privacidad del usuario en el entorno digital actual [6].

Ecuador, Adriana Valencia es experta en perfiles de forense digital en el centro de formación en Ciber del Ecuador. Diagramación de procesos de investigación forense digital. Sin embargo, hasta donde sabemos, no se ha propuesto un modelo único universalmente aceptado que armonice sin problemas estos cuatro componentes principales: la Adquisición o Recolector, Identificación o Examinador, Evaluación o Analizador y finalmente, la Presentación [7]. Estos cuatros factores dan lugar a un enfoque basado en procesos que puede resultar en resultados confiables.

Con todos estos conceptos, procesos, técnicas forenses y elementos fundamentales en mente, nos preparamos para llevar a cabo la práctica y realizar un análisis detallado de los videos digitales, con el objetivo de verificar que su contenido no ha sido alterado de ninguna manera, asegurando así la integridad de la evidencia presentada.

1.2.Descripción del Proyecto

Las técnicas forenses aplicadas a videos digitales han evolucionado significativamente en respuesta a las crecientes necesidades de los analistas y a las regulaciones legales en constante cambio [5]. En este contexto, una de las técnicas forenses que se implementará en este proyecto de investigación es la identificación de la fuente de los videos, lo cual constituye uno de los objetivos principales de nuestro estudio.

Las manipulaciones de videos digitales representan un desafío constante para los investigadores forenses, ya que este fenómeno integra una serie de procedimientos que pueden ser ejecutados por delincuentes informáticos que operan de manera sigilosa y sin dejar rastro alguno. Además, el fácil acceso a la información que proporcionan las plataformas sociales, junto con la amplia disponibilidad y facilidad de uso de programas de edición, permiten que prácticamente cualquier persona, independientemente de su nivel de experiencia técnica, pueda manipular el contenido de los videos de forma engañosa [5].

Técnicas de análisis forense en videos digitales:

TECNICA NUMERO UNO:

Fase de identificación de la fuente

- Identificación de marca/modelo
- Identificación de dispositivo

Fase de detección de manipulaciones

- Detección de falsificación
    - Detección inter-fotograma
        - Detección de interpolación temporal
        - Detección de inserción, duplicación y eliminación
            - Imperfecciones del sensor
            - Doble compresión
            - Movimiento y luminosidad
            - Análisis a nivel de pixeles

- Detección intra-fotograma
    - Detección de escalado y recorte
    - Detección de copiar y mover
        - ❖ Características de los objetos
        - ❖ Características de movimiento

- Detección de pos-procesamiento
    - Detección de plataformas sociales
    - Detección de herramienta de procesamiento (programas de edición)
- Detección de recuperación de contenido oculto
    - Detección de ataques dirigidos
    - Detección de ataques ciegos

Fase de identificación de fuente de adquisición

- Detección de los metadatos
- Detección de las características de la imagen
- Detección de los defectos de la matriz CFA
- Detección de imperfecciones del sensor y la transformada wavelet

TECNICA NUMERO *DOS:*

Fase de análisis de Frame-Level:

- Identificación de inconsistencias en la calidad visual entre fotogramas.
- Detección de anomalías en la secuencia temporal de los fotogramas.
- Verificación de la consistencia de la marca de tiempo entre fotogramas.

Fase de análisis de Compresión:

- Identificación de artefactos de compresión que puedan indicar manipulación.
- Compresión del valor de la estructura de datos como parte de la identificación de estadísticas atipicas.
- Evaluación de la calidad visual para verificar si el video ha sido Re comprimido.

Fase de análisis de filtros y efectos:

- El descubrimiento de filtros o imágenes visibles.
- Verificación de la corrección de efectos especiales con respecto al video.

- La correspondencia de los efectos a lo largo del video no es incorrecta.

Fase de análisis de movimiento:

- Inconsistencias en las posiciones de objetos en el video.
- Detección del método de interpolación de cuadros para imitar movimiento.
- Verificación de que el movimiento tenga sentido de acuerdo a las leyes de la física.

Fase de análisis del perfil de color:

- Evaluación de la uniformidad del renderizado de color en el video.
- Identificación de cambios repentinos en el perfil de color que puedan indicar manipulación.
- Comparación basada en estándares del perfil de color del dispositivo con otros perfiles estándar usados por el dispositivo de captura para una mejor comparación.

Fase de resolución de conflictos y análisis de la relación de aspecto:

- Coherencia de aspecto y resolución en el video.
- Permite la identificación de diferencias en la resolución como indicación de manipulación.
- Análisis de la relación de aspecto para identificar estiramientos u otras manipulaciones.

Fase de análisis de exportación de metadatos:

- Detección de signos de manipulación o alteración analizando los metadatos de exportación del video.
- Características relevantes para la detección de anomalías: Puntuaciones de importancia e interpretación.

Parámetros para definir el modelo legislativo: puntuación compuesta respecto a su estándar popular, como el modelo de dos signos, el z-score. Indicadores importantes como la verificación en nombre de los datos de exportación (fecha de creación del archivo/ajustes de exportación utilizados). Luego, se proporciona una característica compensatoria que es básicamente una cantidad agregada, más allá de la cual, si se gasta cualquier cantidad límite, hará que sea sospechosa la detección de valores atípicos a través de valores mínimos y máximos, pero también se da análisis predictivos para que finalmente se puedan aplicar técnicas de gestión de control

sobre esto de manera que se reciba una alerta para monitorear operaciones comerciales basadas en predicciones aquí.

Fase de análisis de superposición e incrustación:

- Detección de objetos superpuestos que no existían en el entorno original.
- Identificación de aquellas regiones en el video que puedan mostrar signos de manipulación o edición.
- Coherencia visual entre los elementos superpuestos y el contenido original del video.

MANUAL DE AUTENTICACIÓN DE VIDEO

Fase de Identificación de Fuente:

- Recopilación de metadatos:
  - Revisar los metadatos del video para conocer la marca/modelo del dispositivo utilizado, etc.
- Análisis de marcas de agua y logotipos:
  - Ubicación/dirección URL: Algunos videos tienen marcas de agua o logotipos que pueden indicar de dónde proviene el clip.

Fase de detección de manipulación:

- Análisis inter-frame:
  - Identificación de manipulación entre fotogramas, por ejemplo, interpolación temporal, inserción o eliminación de fotogramas.
  - Estudio del ruido del sensor, doble compresión y anormalidad en movimiento/luminosidad.
- Análisis intra-frame:
  - Localización de modificaciones en fotogramas (por ejemplo, cambiar el tamaño, recortar o incluso, mover/copiar objetos innecesariamente).
  - Detección de manipulaciones mediante el análisis de propiedades de objetos y movimiento.

Fase de Análisis Visual:

- Identificación de Inconsistencias en la Calidad Visual:

- Compara la calidad visual entre fotogramas para detectar anomalías.
- Busca inconsistencias en el movimiento de objetos.

➢ Detección de Artefactos de Compresión:

- Verificar la estructura de datos comprimidos para encontrar modificaciones anormales.
- Investigar en la calidad visual para verificar la precompresión del video.

Fase de Análisis de Efectos Visuales:

➢ Detección de Filtros Visuales y Efectos Especiales:

- Confirmar con bases de datos existentes para validar si estos efectos son reales.

Fase de Analizar los metadatos de exportación:

➢ Examinar Metadatos de Exportación:

- Analizar los metadatos de exportación del video en busca de signos de manipulación.
- Verifica la credibilidad de los datos de exportación.

Fase de Análisis de Superposición:

➢ Detección de Objetos Superpuestos:

- Busca objetos superpuestos que no existen en el entorno real del video.
- Evalúa la armonía visual entre los componentes superpuestos y el contenido principal.

Las herramientas que se utilizaran para el desarrollo de este proyecto son:

ExiftoolGui-Windows: Una herramienta de línea de comandos que puede leer y escribir metadatos de videos. La mayoría de las veces, especialmente para recuperar información oculta en el video (cargar útiles de metadatos), se vuelve muy importante analizar todos estos datos incrustados [8].

Exiftool para Linux: Al igual que Windows, este software es capaz de leer y escribir metadatos de archivos de imagen, sonido o video. Utiliza una serie de módulos y una interfaz de comandos, lo que convierte a cSynapse en una de las aplicaciones más prácticas para usuarios de Linux [8].

FFprobe: Es un analizador de flujo de multimedia que funciona con la implementación de línea de comandos de la biblioteca FFmpeg. Es una descripción de lo que realmente es un vídeo, por ejemplo, la duración, la tasa de fotogramas, la resolución y podría ser útil para una exploración técnica profunda de los datos [9].

FFmpeg: El Proyecto de Software Libre FFmpeg ofrece un marco completo de aplicaciones para grabar, transformar y reproducir contenidos multimedia. Es ampliamente reconocido no solo por su capacidad para visualizar, sino también por su funcionalidad en la edición de metadatos. Todo el procesamiento se realiza a través de una interfaz de línea de comandos, lo que permite ejecutar tareas complejas de manera eficiente [10].

QT Fast Start: Este programa se basa en qt-faststart.c del proyecto FFmpeg. Su función principal es extraer los átomos principales o átomos raíz de los contenedores multimedia mediante comandos en una interfaz de línea de comandos, optimizando la carga de videos en plataformas en línea [11].

Mediainfo: Esta herramienta de código abierto y también se ha proporcionado con la versión en línea que permite sus preferencias de acceder a la funcionalidad del software sin ejecutar ni instalar directamente ningún software en la máquina [12].

Atomic Parsley: Esta pequeña, rápida y robusta utilidad puede leer etiquetas en su archivo de video en el contenedor mpeg-4. Aunque permite el examen de contenedores de medios mp4 a nivel atómico, esta herramienta carece de la capacidad de recorrer etiquetas y valores [13].

Bento4: Esta biblioteca está diseñada para facilitar la lectura y escritura de archivos MP4. Incluye herramientas que permiten la edición y lectura de metadatos de videos en formato MP4, así como un proceso de filtrado de átomos específicos desde los contenedores multimedia, lo que la convierte en una herramienta útil para manipulaciones precisas [14].

Este proyecto está relacionado con la línea de investigación en Tecnología y Sistemas de la Información (TSI) asociada a la sub-línea de investigación sobre Ingeniería y gestión de Tecnologías y Sistema de la Información con la finalidad de brindar seguridad en el contenido de los videos digitales [15].

1.3. Objetivos del Proyecto

Objetivo general

Aplicar técnicas de análisis forense, mediante el uso de herramientas de código abierto para evaluar la integridad del contenido de videos digitales.

Objetivo especifico

- Recopilar evidencia digital relevante, como metadatos y hash, para respaldar la verificación de la autenticidad de los videos digitales investigados.
- Implementar técnicas forenses para la verificar la autenticidad de los video digitales.
- Desarrollar algoritmos Python para la extracción del código hash.
- Documentar el proceso y resultados obtenidos en el análisis de la integridad del contenido de los videos digitales.

1.4.Justificación del Proyecto

El análisis forense digital como disciplina es un área de investigación en constante evolución con una influencia creciente en muchos escenarios, tales como investigaciones criminales, problemas de inteligencia y seguridad nacional. El análisis forense digital es vital para investigar y prevenir los delitos informáticos en la sociedad moderna [16].

Es específico, basado en procesos tipificados por el COIP (Código Orgánico Integral Penal de Ecuador). El estado ecuatoriano busca, a través del COIP, establecer sanciones y procesar a quienes cometen delitos cibernéticos. De hecho, en 2015, los delitos más comunes a nivel nacional fueron aquellos que afectan la información pública legalmente reservada, según estadísticas derivadas del Observatorio del Delito de la Dirección de Política Criminal de la Fiscalía de Ecuador, lo que nos muestra que debemos fortalecer las capacidades de investigación forense en este país [16].

Este estudio implementará diferentes técnicas de análisis forense para obtener información precisa y confiable. Ciertamente, identificar la fuente de estas

imágenes —basándose en sus metadatos, cuadros y características de sonido— será una de las principales técnicas que se emplearán. Usando la información obtenida en el paso anterior, se identificarán las manipulaciones cubriendo tres tipos básicos: detección de falsificaciones, detección de posprocesamiento y recuperación de contenido oculto.

La idea de manipular el marco esta principalmente involucrada en la detección de falsificaciones, al verificar la extracción de inserciones, eliminadas y duplicados de uno o varios marcos. La manipulación de cada marco individual también se tiene en cuenta, en el sentido de que sucedería si se han realizado cortes o si alguna sección del video ha sido copiada, pegada o movida de un lugar a otro. La detección de posprocesamiento, por otro lado, se refiere a cualquier edición realizada después de que el video fue creado. Con este fin, la recuperación de contenido oculto (estenografía), es decir, para descubrir que una fuente de información secreta estaba oculta en el video.

Así, se puede elaborar el informe mas detallado y elaborado de resultados a partidos de estas técnicas forenses. Este informe proporcionara un resumen de como se anotaron los hallazgos de la investigación, así como las recomendaciones futuras específicas que se proponen. Esperamos que, de esta manera, sea posible contribuir a la creación de una referencia fácil de seguir que ayude a implementar técnicas forenses para el análisis de video digital.

El tema propuesto está alineado a los objetivos del Plan de Creación de Oportunidades específicamente al siguiente eje:

Eje 2: Eje Seguridad Integral

Objetivo 9: Garantizar la seguridad ciudadana, orden público y gestión de riesgo [17].

Política 9.1: Fortalecer la protección interna, el mantenimiento y control de orden público, que permita prevenir y erradicar los delitos conexos y la violencia en todas sus formas, en convivencia con la ciudadanía en el territorio nacional y áreas jurisdiccionales [17].

Objetivo 7: Garantizar la soberanía nacional, integridad territorial y seguridad del

Estado [17].

Política 10.1: Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del ciberespacio y proteger su infraestructura critica [17].

1.5. Alcance del Proyecto

El alcance de un proyecto de análisis forense de la integridad del contenido en videos digitales puede abarcar una variedad de aspectos técnicos y legales para garantizar una evaluación completa y precisa de la evidencia multimedia. Para empezar, el proyecto debe dejar claro cuáles son sus objetivos para este análisis: la honestidad del contenido (identificar falsificaciones), la detección de manipulación o un sentido que guíe el interés deseado. Estos objetivos se utilizarán para decidir cómo se emplearán las técnicas y metodologías.

Además, el alcance del proyecto debe tener en cuenta los recursos disponibles en términos de experiencia tecnológica, así como humana. Esto podría implicar el uso de software específico adaptado para el análisis de video digital y, potencialmente, trabajar con especialistas forenses en multimedia y ciberseguridad. Considerando la literatura existente hasta la fecha, se debe tener en cuenta que el tiempo es clave para realizar un análisis sistemático y exhaustivo mediante la resolución de casos aún más complejos que involucren un mayor detalle.

Al definir el alcance de cualquier proyecto, también es necesario incorporar los requisitos legales/regulatorios pertinentes. Dichos procedimientos incluyen los requisitos de cadena de custodia para evitar alteraciones en la evidencia, así como la adhesión a prácticas estándar sobre cómo se deben presentar los informes forenses en el tribunal. El propio análisis debe realizarse de manera que garantice la confidencialidad y privacidad de la información, respetando las pautas éticas.

El alcance del proyecto también debe incluir la documentación de los hallazgos o resultados del análisis forense. Es posible que también se redacten informes técnicos que expliquen los métodos utilizados, los resultados obtenidos y sus conclusiones. Además, en caso de que los hallazgos del análisis forense requieran validación profesional, lo mejor es prepararse para brindar testimonio como experto en un tribunal o en otras actividades judiciales.

En resumen, un proyecto de análisis forense de video digital puede comenzar desde la definición de los objetivos del proyecto y la estimación de la financiación adecuada hasta la aplicación de aspectos legales y la documentación de los resultados, orientando todo el proceso para asegurar la integridad y confianza de los datos de video utilizados para tareas de seguridad o presentados como evidencia en el tribunal.

1.6. Beneficiarios del proyecto

Un beneficiario específico del proyecto es el departamento de comunicación de la Universidad Politécnica Salesiana del Ecuador (UPSE), junto con los estudiantes que estarán involucrados en diversas actividades que fomentan el crecimiento profesional. Creará una oportunidad para que los estudiantes adquieran experiencia en el campo del análisis forense digital, mejorando sus habilidades y competencias.

1.7. Variables

Con la implementación de la solución tecnológica propuesta, se busca lograr una reducción significativa en el tiempo de respuesta en comparación entre el prototipo y las herramientas actualmente utilizadas. Esta mejora en la eficiencia no solo optimizará los procesos de análisis forense, sino que también permitirá un manejo más ágil y efectivo de la evidencia multimedia en situaciones críticas.

CAPÍTULO 2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1. Marco Conceptual

La validación forense automatizada de la integridad de videos digitales es importante tanto para los refuerzas de ciberseguridad como para la investigación criminal. Los videos pueden ser modificados mediante tecnologías de edición, por lo que podrías ser engañado sin darse cuenta. Estos archivos pueden ser analizados a través de métodos consistentes y herramientas dedicadas, con el fin realizar análisis forense sobre ellos, mientras se preserva su metadato de procedencia mediante el uso técnicas de hash específicas [18]. Aquí hay una lista de los conceptos y técnicas centrales sobre este tema.

2.1.1. Análisis Forense Digital

El análisis forense digital trata con la recolección, preservación y análisis de evidencia digital. En vídeos, se trata de confirmar su autenticidad basado en factores como los metadatos, huellas digitales y estructura interna. Esta disciplina incorpora procedimientos estandarizados y herramientas técnicas para salvaguardar la integridad de la evidencia en contextos judiciales [19]. Por lo tanto, verificar la autenticidad de los vídeos digitales es un componente crítico para la aceptación de estas técnicas en investigaciones legales y científicas.

2.1.2. Autenticidad Falsa en Videos Digitales

La autenticidad significa la garantía de que un video no ha cambiado desde que fue grabado. La verificación de autenticidad observa aspectos como la consistencia de los metadatos, si los cuadros son continuos y no se han caído, y la verificación de la integridad de un archivo digital. Farid afirma que el análisis forense detectaría anomalías como ediciones o manipulaciones que comprometan la fiabilidad de los videos [20]. Esta evaluación es esencial para validar los archivos orientados a la evidencia y procesos éticos.

2.1.3. Exageración en Videos Manipulados Digitalmente

Las manipulaciones pueden ir desde técnicas simples, como recortes, a complejas como los Deepfakes, que representan medios sintéticos donde la semejanza de una persona en otro cuerpo ha sido alterada usando software de inteligencia artificial

(IA). Stamm et al. discuten que estos cambios no siempre son visibles a simple vista y necesitan algunas herramientas especializadas para detectarlos [21]. Esto socava la integridad del contenido, porque luego se vuelve difícil reconocer si estás viendo el video original o no.

2.1.4. Algoritmos de HAsh

Un hash genera una firma digital única correspondiente a cada archivo, y es posible verificar la integridad del archivo usando esta firma. Métodos como MD5 y SHA-256 son ampliamente utilizados en análisis forense porque cualquier alteración del archivo cambia su valor de hash [22]. Kaur et al. enfatizan que si el contenido está marcado como tal es crucial para mantener la consistencia durante el proceso analítico [23]. Entonces, para mantener la evidencia digital, los algoritmos de hash son muy importantes.

2.1.5. Herramientas de Código Abierto

El análisis forense con herramientas de código abierto es esencial ya que ofrecen flexibilidad, escalabilidad además de ser accesibles y fácilmente apoyadas por la comunidad. Herramientas como ffmpeg o exiftool se pueden utilizar para examinar los metadatos en imágenes y videos [24]. Estas herramientas también desempeñan un papel clave en la replicación de procesos, particularmente para investigaciones académicas y judiciales [25].

2.2. Marco Teórico

Los recientes avances en el estudio forense de videos digitales lo sitúan como una disciplina dentro de la ciberseguridad y la informática forense. Su objetivo principal es preservar la autenticidad e integridad de las evidencias de videos digitales, que son cruciales en investigaciones legales [26]. Esto se llama autenticidad, lo que significa confirmar que un video proviene de su fuente declarada, mientras que integridad se refiere a asegurar que ningún contenido ha cambiado desde el momento de la grabación [27]. Estos son críticos para asegurar la confianza en la evidencia de video digital en legal y forense [28].

La Referencia Cruzada de Metadatos es el método más básico para verificar la integridad de videos digitales. Estos metadatos (por ejemplo, la fecha y hora de

creación, dispositivo utilizado, parámetros técnicos del archivo) [29], si se encuentran inconsistencias, puede dar algunas pistas sobre qué tipo de manipulaciones tienen lugar. Por ejemplo, un video comunica que fue capturado en ciertas condiciones, pero su metadato muestra lo contrario [31].

También son conceptos útiles para filtrar manipulaciones de videos digital. Dichos algoritmos consideran las discrepancias entre fotogramas y ruidos para resaltar la manipulación [32]. Las técnicas comunes incluyen el análisis de comprensión y la detección de doble compresión MPEG para detectar ediciones de video [33]. También emplea fotogrametría y esteganografía para ver cambios mínimos, que pueden pasar desapercibidos. Estas técnicas ayudan a los investigadores a identificar la edición, inserción o eliminación de contenido en videos [34].

De hecho, la autenticación de un video requiere el análisis de su procedencia y verificaciones de firmas digitales. Las firmas digitales son herramientas criptográficas que confirman que el video no ha cambiado desde el formato en que fue inicialmente creado [35]. Los metadatos luego pueden compararse con fuentes previamente conocidas y confiables para verificar la procedencia del video [36]. Sin embargo, esto no funcionará si los propios metadatos también han sido manipulados. El análisis forense también ha estado incorporando técnicas avanzadas de inteligencia artificial y aprendizaje automático para mejorar la precisión de la detección de manipulaciones. Las redes neuronales convolucionales (CNN) son una de ellas, que ayudan a reconocer variaciones en patrones de video que implican interferencia [37].

Las técnicas de aprendizaje automático han sido efectivas en la detección de manipulaciones de video. Estas técnicas permiten el análisis de enormes cantidades de datos y la detección de patrones que pueden no ser aparentes usando enfoques convencionales, como se muestra en [38]. Analizan secuencias del video y detectan inconsistencias temporales utilizando modelos de aprendizaje profundo como las redes neuronales recurrentes (RNN) [39]. Además, los algoritmos de aprendizaje supervisado pueden ser entrenados usando ejemplos de videos manipulados y no manipulados para mejorar su efectividad en la detección de fraudes [40].

2.3. Metodología del Proyecto

2.3.1. Metodología de Investigación

El análisis forense de videos digitales sigue un enfoque orientado a varios pasos. Etapa uno: una revisión bibliográfica exhaustiva de la literatura de investigación considerando técnicas forenses aplicadas al video digital. En esta revisión nos enfocamos en las grandes amenazas a la integridad y autenticidad del contenido, y en técnicas sólidas que son prácticamente útiles en la detección de manipulaciones. También abarca la revisión de algunos datos [41] sobre estudios previos destinados a utilizar técnicas forenses en videos digitales en múltiples escenarios.

Luego, la siguiente fase de definición del problema se realiza de acuerdo con vulnerabilidades específicas que potencialmente pueden llevar a comprometer la integridad y autenticidad de videos digitales [42]. Hipotetizar qué técnicas de manipulación pueden haber sido utilizadas y la mejor manera de detectarlas. Hipótesis, por ejemplo, es que la compresión doble MPEG es un buen indicador de manipulación de video [43]. La formulación de estas hipótesis ayuda a dar forma al diseño de la investigación y la elección de métodos y herramientas de análisis [44]. Las hipótesis deben ser probadas para apoyar un diseño de investigación para medir sus resultados. Este paso trata de codificar una muestra de videos que serán analizados con los métodos forenses elegidos. La muestra puede incluir videos manipulados deliberadamente, así como videos originales legítimos para probar la precisión de los algoritmos de detección [45]. La recolección de datos es una fase muy importante en la que se recogen las muestras de videos reales para su análisis. Se seleccionan y organizan teniendo en cuenta una serie de posibles estrategias de manipulación [46].

La última fase donde las muestras son analizadas de manera sistemática con herramientas y técnicas definidas para interpretar los resultados y validar que el contenido es tanto genuine como no adulterado [46]. Esto incluye verificar si los resultados obtenidos se ajustan a las hipótesis formuladas inicialmente, evaluando si las técnicas de recuperación probadas son efectivas, entre otros, para ayudar a encontrar los algoritmos de detección [47].

2.3.2. Métodos y herramientas de Recolección de Datos

Para el análisis forense de video de cualquier Fuente digital, se aplican una variedad de métodos y herramientas para importar la información necesaria. En segundo lugar, el software de análisis forense como Amped Authenticate y VideoInspector nos permite ver que hay dentro video y cómo funciona [48].Tales herramientas pueden identificar ediciones y manipulaciones al examinar las propiedades técnicas de un archivo de video, incluida su tasa de bits, resolución y formatos de compresión [49]. Herramientas especializadas como MediaInfo se utilizan para la extracción de metadatos para producir detalles técnicos sobre un archivo de video [50].

En el análisis forense de imágenes, el análisis de compresión es crucial para determinar si un área de interés detectada en un archivo podría haber sido manipulada. Utiliza algoritmo diseñados para identificar los artefactos de compresión introducidos por la edición. Por ejemplo, es posible detectar una compresión doble JPEG o MPEG que puede mostrar que un video ha sido alterado y comprimido nuevamente. Este método es particularmente útil para detectar manipulaciones más sutiles que no pueden ser percibidas con el ojo humano [51]. Además, rechazamos videos inconsistentes a través de un proceso de revisión manual, comparación de cuadro por cuadro y contraste de los contenidos del cuadro. Al emplear tanto herramientas automáticas como análisis humano, este método garantiza que la integridad del video sea evaluada exhaustivamente [52]. Y a través de enfoques de análisis cuadro por cuadro, se pueden identificar diferencias apenas detectables que podrían ser indicadores de manipulación [53]. Por ejemplo, los cambios en la iluminación o las estadísticas de ruido de cuadro a cuadro podrían indicar cortes [54].

La aparición del procesamiento de imágenes y videos ha llevado al despliegue de nuevas herramientas y técnicas de recolección de datos forenses. Tecnología fotogramétrica avanzada, que analiza la geométrica y el movimiento de los objetos en el video para descubrir ediciones. Este método se utiliza para la reconstrucción de escenas en 3D y evalúa si las posiciones de los objetos que se mueven en el video son consistentes [55]. Además, la implementación de técnicas de esteganografía en

el análisis forense digital también nos permite no solo encontrar nuevas formas para identificar aquellas falsificaciones ocultas en los medios [56].

Aunque podrían detectar alteraciones utilizando esteganografía: el método de oscurecer datos en el video y pasar desapercibido. Donde se encuentran estas desviaciones, procesos como operaciones de lectura, escritura de archivos y manejo de datos usando esteganografía pueden ser detectados en cuadros de video basados en los patrones de bits que ayudan a identificar, si esta oculto, el ocultamiento de datos para camuflar asuntos [57]. Además, es posible complementar la estenografia con otras técnicas de análisis forense que traerán una evaluación de integridad más completa en un video [58].

2.3.3. Metodología del desarrollo

El proceso para el desarrollo metodológico de DVFA consiste en una serie de pasos sistemáticos. Primero, herramientas apropiadas y presentarlas cuando sean eficientes y creíbles [59]. Este paso consiste en identificar el mejor software y algoritmos que estarán presentes cuando se trate de la operación de detección de las manipulaciones. Posteriormente, se establece un entorno seguro para la investigación forense a fin de realizar el análisis sobre los datos sin perder su integridad durante el proceso [60]. Protocolos estándar enfocados en el análisis, pasos detallados para validar que el contenido es completo y genuino.

Los protocolos se desarrollan para un análisis estandarizado, incluyendo procedimientos detallados para verificar la integridad y autenticidad del contenido. Estos protocolos garantizan que todo el trabajo sea coherente y repetible, con resultados verificables y fiables [61]. Las pruebas piloto realizadas representan una etapa importante en la que se refinan los sondeos, los protocolos, herramientas, etc. Esto permite identificar y corregir cualquier problema antes de aplicar los protocolos en un análisis sistemático [62].Finalmente, se realiza un análisis detallado de las muestras de video, aplicando los protocolos desarrollados y registrando detalladamente los hallazgos.

Dar sentido a un resultado es importante para poder emplear estas técnicas en estudios de integridad y autenticidad de contenido de video. Este proceso implica registrar cada acción realizada, todos los resultados obtenidos y cualquier

irregularidad observada. En segundo lugar, este grupo de manipulaciones detectadas podría ser analizado para identificar patrones comunes y actualizar el algoritmo de detección [63].

El desarrollo de metodologías también implica la creación de bases de datos de referencia que contienen ejemplos de videos manipulados y no manipulados. Estas bases de datos son fundamentales para el entrenamiento y la evaluación de algoritmos de detección de manipulación [64]. Se recibe más información mediante la colaboración con investigadores relevantes y la asistencia a conferencias, talleres especiales, etc., lo cual ayuda a realizar actualizaciones adicionales de la metodología junto con los avances futuros dentro del ámbito forense [65]. Los métodos de análisis forense evolucionan continuamente, al igual que las técnicas y herramientas que crean contenido falso [66].

CAPÍTULO 3. PROPUESTA

3.1. Requerimientos

3.1.1. Requerimientos Funcionales

R01. Primero, si la aplicación quiere verificar la autenticidad de un video, necesita investigar información como detalles de la cámara, fecha y hora de grabación, ubicación, etc., a través de herramientas de extracción.

R02. Los servicios ofrecidos por el sistema deben incluir, pero no se limitan a: generación de informes detallados del análisis forense realizado, hallazgos y evidencias recolectadas según las conclusiones.

R03. La aplicación debe contar con una interfaz de usuario intuitiva y fácil de usar, que haga simple para los usuarios realizar análisis forenses.

R04. La aplicación también debe admitir varios formatos de video de diversas fuentes, comunes como MP4, AVI, MKV, etc.

R05. La aplicación debe detectar y resaltar posibles clonaciones o duplicaciones de partes del video.

R06. La aplicación trabajará para encontrar algún signo de falta de originalidad precisa, por ejemplo, superposiciones de imágenes o expulsión de objetos, la sucesión en el movimiento de cuadros.

R07. Todas las técnicas de esteganografía que se utilicen para ocultar información en un video deben ser buscadas por la aplicación.

R08. Examinar los metadatos del video para detectar anomalías o discrepancias que sugieran una posible manipulación o falsificación del video.

R09. Utilizar gráficos, tablas y otras herramientas de visualización numérica para permitir la interpretación de resultados complejos.

3.1.2. Requerimientos no Funcionales

R01. Maximizar las características en vivo mientras se minimiza el tiempo de inactividad y los errores del sistema, asegurando que la aplicación esté siempre disponible para los usuarios.

R02. Utilizar un código limpio, modular y bien documentado para facilitar la comprensión y modificación del código fuente.

R03. La aplicación debe ser escalable para adaptarse a un aumento en la cantidad de casos y videos a analizar sin perder calidad en el proceso.

3.2. Componente de la Propuesta

3.2.1. Requerimientos Mínimos.

A continuación, se describen el hardware y software como requerimientos mínimos para la realización del proyecto:

Hardware

Cantidad	**Descripción**	**Requisitos mínimos.**
1	Laptop HP	2.80 GHz procesador o superior. 500 Gb SSD o superior. 12 Gb RAM o superior.

Tabla 1 Componentes de hardware

Software

Cantidad	**Herramientas**	**Requisitos mínimos.**
1	Sistema Operativo Windows	Versión Windows 10 Profesional o superior.
1	Python	Versión 2.7 o superior.
1	Librerías de Python	Versión 2.7 o superior.
1	Visual Studio Code	Versión 1.7 o superior.
1	Exif Tool GUI-Windows	

1	Exif Tool para Linux	
1	FFprobe	
1	Ffmpeg	
1	QT Fast Start	
1	MediaInfo	
1	Atomic Parsley	
1	Bento4	

Tabla 2 Componentes de software

3.2.1. Arquitectura del Sistema

La siguiente grafica representa la arquitectura del sistema de manera sencilla y fácil de entender: (Agregue descripción o explicación de la imagen)

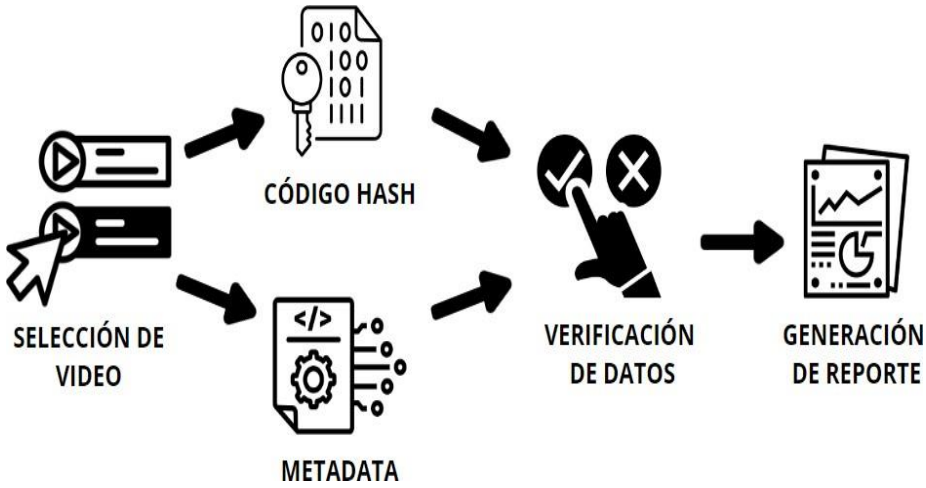
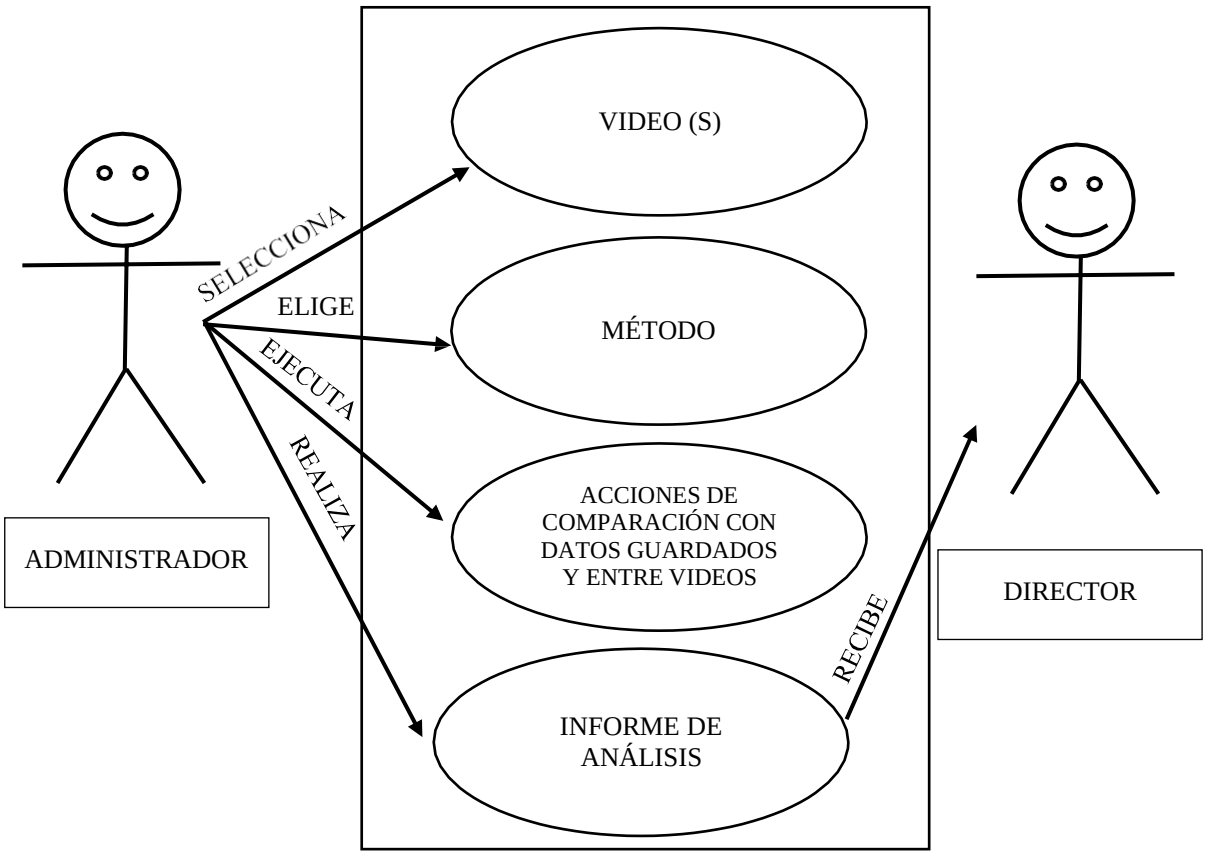


Fig. 2 Arquitectura del sistema

3.2.2. Diagramas de casos de uso

Caso de uso: Elección de método de comparación	
Actor(s)	Administrador, director.
Propósito	Selección de la forma de comparación de videos, mediante hash guardados o eligiendo los videos implicados



Pasos realizados:

- Selección del método de comparación de videos
- Elegida la opción de comparación se procede con el proceso de comparación.

Tabla 3 Selección de método de comparación

Caso de uso: Comparación de videos con datos guardados previamente	
Actor	Administrador
Propósito	Comparar el nuevo video con los datos ya guardados de videos anteriores.
 Elegir los videos a comparar Extraer la metadata Comparar con datos guardados	
Pasos realizados: • Elegir la opción de seleccionar video. • Comparar la meta data del nuevo video con los datos guardados. • Mostrar mensajes según sea el caso.	

Tabla 4 Comparación de video mediante hash

Caso de uso: Comparación entre dos videos	
Actor	Administrador
Propósito	Comparación entre dos videos elegidos con el administrador.

Elegir Video 1

Elegir Video 2

Extraer metadata

Comparación de datos

Pasos realizados:

- Selección de videos a comparar.
- Guardar datos de comparación.

Tabla 5 Comparación entre dos videos

3.2.3. Modelado de Datos

Los datos se guardarán en archivos JSON para su posterior visualización, los datos a guardar serán el hash y los metadatos, entre los cuales se encuentrar; format, format_profile, codec_id, duration, bit_rate, width, height, frame_rate, codec, audio_codec, audio_bit_rate, y también se guarda un contador en caso de que los datos coincidan, la estructura en que se manejaran los datos es la siguiente:

```
"hashes": [
    {
        "video": "D:/Escritorio/ROGER/WhatsApp Video 2024-06-02 at 18.01.16.mp4",
        "analisis_count": 2,
        "analisis": [
            {
                "hash": "0e91a50bd2d8b8763a785084f78b6644c01bdaafb8475526e3e72ccff13e8d64",
                "metadatos": {
                    "format": "AVC",
                    "format_profile": "High@L3",
                    "codec_id": "avc1",
                    "duration": 4198,
                    "bit_rate": 1324349,
                    "width": 480,
                    "height": 864,
                    "frame_rate": "30.000",
                    "codec": null,
                    "audio_codec": null,
                    "audio_bit_rate": "1 324 kb/s"
                }
            },
            {
                "hash": "0e91a50bd2d8b8763a785084f78b6644c01bdaafb8475526e3e72ccff13e8d64",
                "metadatos": {
                    "format": "AVC",
                    "format_profile": "High@L3",
                    "codec_id": "avc1",
                    "duration": 4198,
                    "bit_rate": 1324349,
                    "width": 480,
                    "height": 864,
                    "frame_rate": "30.000",
                    "codec": null,
                    "audio_codec": null,
                    "audio_bit_rate": "1 324 kb/s"
                }
```


Fig. 3 Estructura de datos

Para la comparación entre dos videos, los datos a guardan son los mismos que en el caso anterior con la diferencia de que se guardan los datos de los dos videos en mismo dato y tendrá la siguiente estructura:

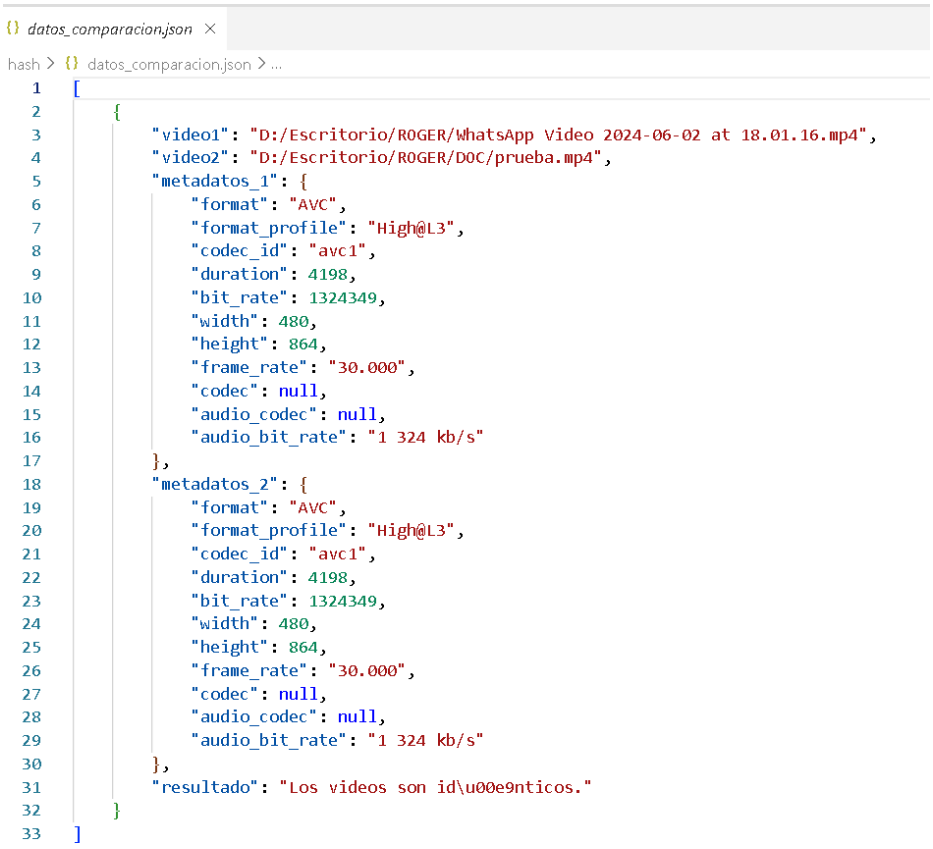


Fig. 4 Estructura de datos de comparación de videos

Los hashes de todos los frames se codifican en formato bytes. Estos hashes se concatenan y se calcula un hash SHA-256 de esta concatenación, para esto se usa la librería HASHLIB de Python, al calcular y almacenar los hashes de los videos, se puede garantizar la integridad de los archivos. Cualquier alteración, incluso a nivel de un solo frame, resultará en un hash diferente. Esto es crucial para asegurar que los videos no han sido manipulados desde su almacenamiento inicial, proporcionando una capa adicional de seguridad en la preservación de evidencia digital y se logra con el fragmento del código que se muestra a continuación:

```
# Codificar cada hash en formato bytes antes de unirlos
encoded_hashes = [hash.encode() for hash in frame_hashes]
hash_valor = hashlib.sha256(b''.join(encoded_hashes)).hexdigest()
self.resultado_label.setText(f"Hash del video '{nombre_video}' guardado con éxito: {hash_valor}")
```

Fig. 5 Código de creación de código hash

Para la extracción de los metadatos de los videos, se usa la librería METAINFO, la cual permite extraer información de los archivos multimedia, para poder guardarlos y posteriormente compararlos con los demás metadatos. Además del hash, el sistema extrae y almacena metadatos detallados de los videos, incluyendo duración, ancho, alto y frame rate. Estos metadatos son esenciales para proporcionar un contexto adicional en el análisis forense, permitiendo una comprensión más profunda del contenido y las características técnicas del video, con el siguiente código se puede realizar este proceso:

```
def obtener_metadatos_video(nombre_archivo):
    media_info = MediaInfo.parse(nombre_archivo)
    for track in media_info.tracks:
        if track.track_type == 'Video':
            return {
                "format": track.format,
                "format_profile": track.format_profile,
                "codec_id": track.codec_id,
                "duration": track.duration,
                "bit_rate": track.bit_rate,
                "width": track.width,
                "height": track.height,
                "frame_rate": track.frame_rate,
                "codec": track.codec,
                "audio_codec": track.other_audio_format_list[0] if track.other_audio_format_list else None,
                "audio_bit_rate": track.other_bit_rate[0] if track.other_bit_rate else None
            }
    return None
```

Fig. 6 Código de extracción de metadatos

3.3. Diseño de Interfaces

El sistema tendrá una opción de menú de ingreso, mediante el cual se va a poder elegir las opciones selección de video, comparación de videos, mostrar hashes y metadatos guardados y mostrar comparación de videos.

Fig. 7 Interfaz de menú principal

Visualización de los datos guardados mediante la comparación de hash anteriormente guardados.

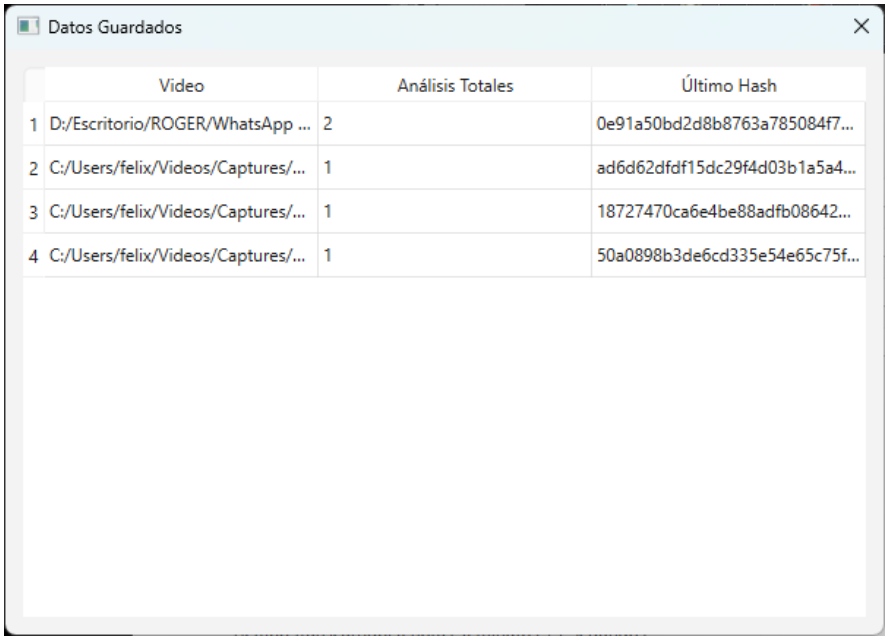


Fig. 8 Visualización de datos guardados

En caso de que los datos coincidan en la comparación se guardará como uno nuevo, como se muestra a continuación:

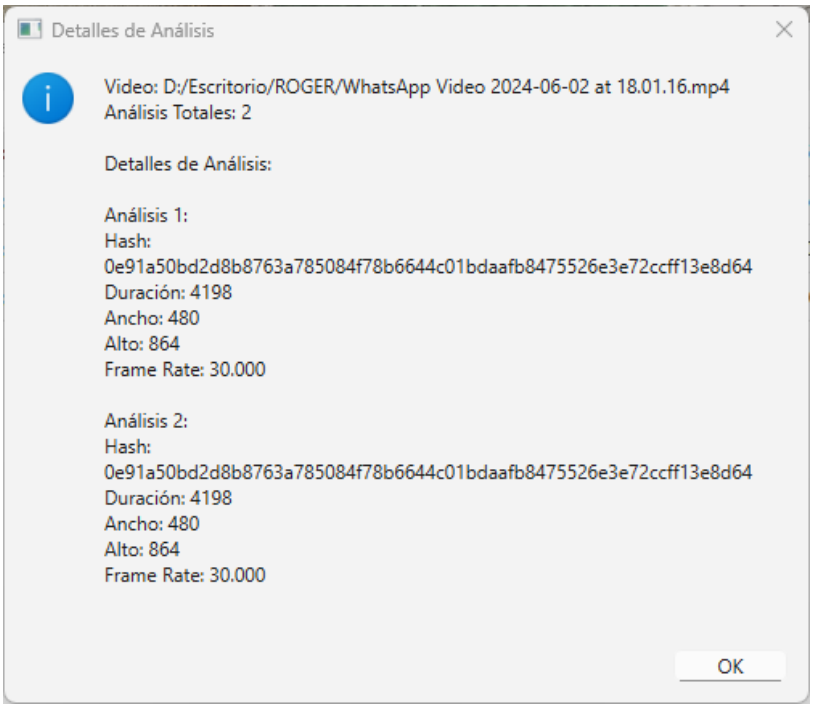


Fig. 9 Visualización de datos que coinciden

Visualización de los datos en la comparación entre dos videos:

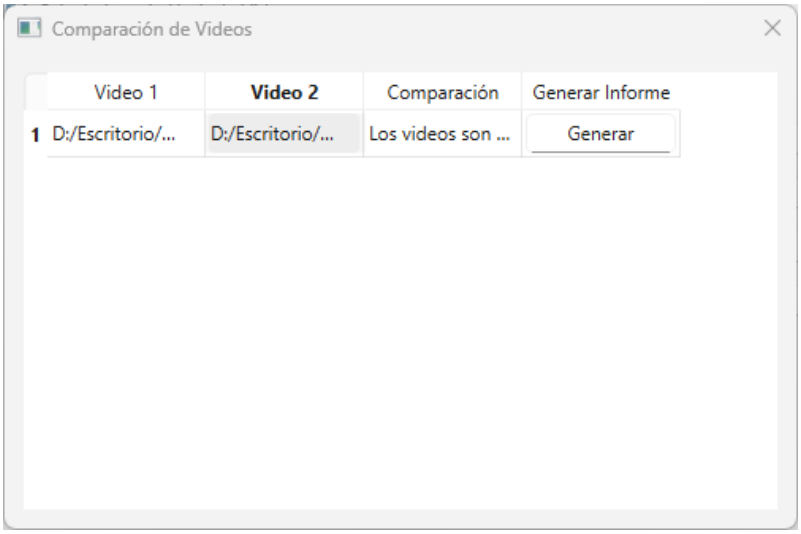


Fig. 10 Visualización de comparación entre dos videos

Visualización de datos de forma detalla en la comparación de videos:

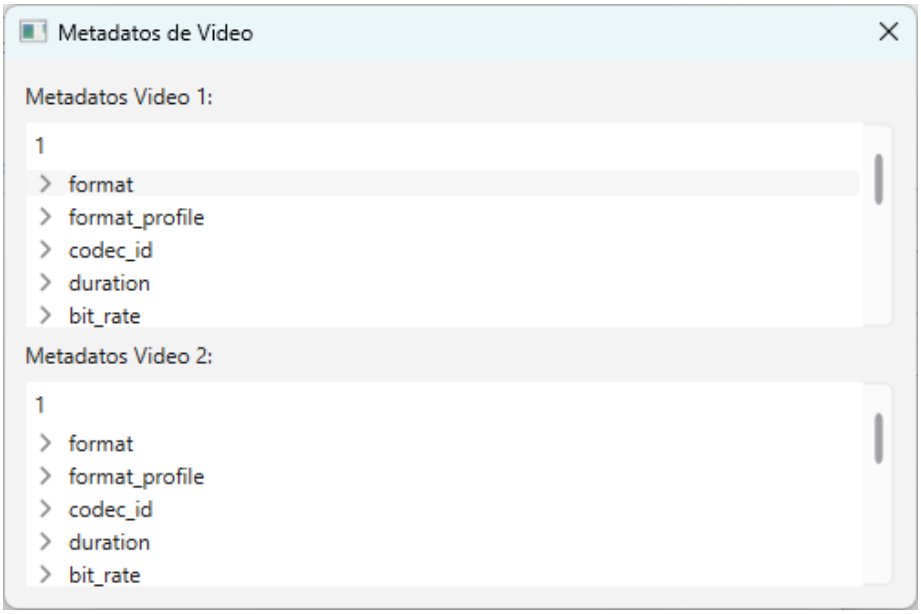


Fig. 11 Visualización de datos detallados de comparación

3.4. Pruebas

Para las pruebas se comprobó que la aplicación detecta que el mismo video, mediante la comparación del mismo video, pero con nombres distintos, es el único cambio que se realizó, y efectivamente lo detectó como el mismo video, puesto que compara la metadata entre los videos.

	Video 1	Video 2	Comparación
1	D:/Escritorio/...	D:/Escritorio/...	Los videos son idénticos.

Fig. 12 Pruebas de funcionalidad del sistema

Una prueba separada midió el tiempo que tomo descargar un video de la red social de la universidad. El video fue examinado y se extrajeron metadatos, lo que resulto en algunos cambios realizados en el video. En este caso, se superpuso un filtro transparente durante toda la duración del video para un examen adicional. Los resultados produjeron los siguientes datos:

Video 1: D:/Descargas/MASIVA PARTICIPACIÓN DE ESTUDIANTES DE ENFERMERÍA EN INTEGRACIÓN DEPORTIVA.mp4

Propiedad	Valor
format	AVC
format_profile	High@L3.1
codec_id	avc1
duration	53054
bit_rate	2161740
width	1280
height	720
frame_rate	29.970
codec	None
audio_codec	None
audio_bit_rate	2 162 kb/s

Fig. 13 Datos de video original

Video 2: D:/Descargas/MASIVA PARTICIPACIÓN DE ESTUDIANTES DE ENFERMERÍA EN INTEGRACIÓN DEPORTIVA edit ■ Hecho con Clipchamp.mp4

Propiedad	Valor
format	AVC
format_profile	Constrained Baseline@L4.1
codec_id	avc1
duration	53067
bit_rate	17745711
width	1920
height	1080
frame_rate	30.000
codec	None
audio_codec	None

Fig. 14 Datos de la modificación.

CONCLUSIONES

El uso de herramientas de código abierto es fundamental para garantizar un análisis forense completo y preciso en videos digitales. Herramientas como **ExifTool**, **FFmpeg**, **Amped Authenticate** y **Forensically** permiten recopilar metadatos detallados y huellas digitales, extrayendo información crucial como fechas de creación, modificaciones, detalles de la cámara y otros parámetros técnicos. Estas herramientas facilitan la detección de manipulaciones de manera precisa, mejorando la confiabilidad del proceso. Además, es esencial implementar protocolos estandarizados que garanticen la correcta recolección, almacenamiento y análisis de datos, diseñados para mantener la cadena de custodia y preservar la integridad de la evidencia durante todo el proceso.

El análisis de metadatos y el uso de algoritmos hash son elementos clave en la detección de alteraciones en archivos digitales. Algoritmos como **MD5**, **SHA-1** y **SHA-256**, combinados con herramientas como **HashMyFiles**, permiten generar valores de checksum confiables que evidencian modificaciones en los archivos. Complementar este análisis con herramientas como **OpenCV** ayuda a identificar cambios sutiles en los fotogramas, que de otro modo podrían pasar desapercibidos. Estas estrategias garantizan resultados precisos y contribuyen significativamente a la verificación de la autenticidad de los videos digitales.

La capacitación continua es otro aspecto crucial para mejorar las competencias técnicas de los analistas. Entrenar a los usuarios en el manejo de herramientas forenses y fomentar la creación de bases de datos de referencia que incluyan ejemplos de videos manipulados y no manipulados fortalece las habilidades profesionales. Estas bases también pueden utilizarse para entrenar algoritmos de detección automática, incrementando la precisión y eficiencia de los análisis. La formación continua asegura que los profesionales estén actualizados frente a las nuevas técnicas de manipulación digital.

Por último, la documentación exhaustiva de los procedimientos y hallazgos es indispensable para garantizar la replicabilidad y validez del análisis forense. Utilizar herramientas como **Case Notes** y **DFXML** permite registrar cada paso del proceso de manera clara y detallada. Esto asegura que los resultados puedan ser auditados y utilizados como evidencia confiable en contextos legales

RECOMENDACIONES

Es esencial emplear herramientas de código abierto como ExifTool para recopilar metadatos detallados y huellas digitales de los videos. Estos programas permiten extraer información crucial como fechas de creación, modificaciones y detalles de la cámara. Es importante establecer un protocolo estandarizado para la recopilación y almacenamiento de esta evidencia para mantener su integridad durante el análisis forense.

El análisis de metadatos indica las modificaciones en un fotograma del video digital, ese cambio particular a menudo puede se detectado mediante el análisis del hash. La detección de análisis a nivel pequeño y mediano se pueden llevar a cabo utilizando herramientas como Ffmpeg o OpenCV, que ayudaran a identificar pequeños cambios que son difíciles de reconocer, pero que en realidad pueden señalar una alteración.

Los cambios y manipulaciones de videos digitales pueden ser detectados con una variedad de herramientas específicas, como Amped Authenticate y Forensically, que son indispensable para este propósito. Tales posibles cambios pueden ser detectados usando algoritmo deseados o programas de computadora y analizan imágenes y videos.

Realizar algoritmos hash mediante MD5, SHA-1, Hash Calc y SHA-256, y usar herramientas como HashMyFiles. Estos algoritmos deben integrarse y archivarse en el flujo de trabajo forense, que genera un valor de checksum de los archivos de video y lo verifica para identificar cualquier alteración realizada durante el análisis.

Desarrollar un sistema de documentación detallada que incluya cada paso del análisis forense, utilizando herramientas como Case Notes y DFXML. La documentación debe ser clara, precisa y replicable, proporcionando un registro exhaustivo de los procedimientos y hallazgos.

Referencias

[1] Y. Fernández, «xataka,» 16 Mayo 2022. [En línea]. Available: https://www.xataka.com/basics/siete-editores-de-video-gratis-para-usar-en-windows.. [Último acceso: 11 Octubre 2024].

[2] A. Informatica, 2024. [En línea]. Available: https://aprendeinformaticas.com/#google_vignette. [Último acceso: Octubre 2024].

[3] E. Telegrafo, «El telegrafo el decano digital,» Junio 2014. [En línea]. Available: https://www.eltelegrafo.com.ec/. [Último acceso: Octubre 2024].

[4] F. Pita, «INVESTIGACIÓN CUANTITATIVA Y CUALITATIVA,» España, CAD ATEN PRIMARIA, 2002, pp. 9:76-78.

[5] Q. H. Carlos, «Universidad Complutense de Madrid,» 28 Mayo 2021. [En línea]. Available: https://docta.ucm.es/entities/publication/9609c1ee-e1f6-4d83-ac56-0f599cbd9dd3.. [Último acceso: Octubre 2024].

[6] M. L. Torres Moncada y D. A. Jaramillo Arciniegas, «Repositorio Universidad Militar Nueva Granada,» 09 Agosto 2016. [En línea]. Available: https://repository.unimilitar.edu.co/handle/10654/14401. [Último acceso: Octubre 2024].

[7] V. S. A. Ivonne, «Repositorio Digital Universidad Internacional SEK,» Octubre 2020. [En línea]. Available: https://repositorio.uisek.edu.ec/bitstream/123456789/4020/1/Valencia%20Sasil%20Adriana%20Ivonne.pdf.

[8] P. Harvey, «ExifTool by Phil Harvey,» [En línea]. Available: Phil Harvey. [Último acceso: Octubre 2024].

[9] FFmpeg, «FFmpeg,» [En línea]. Available: https://ffmpeg.org/ffprobe.html. [Último acceso: Diciembre 2023].

[10] «FFmpeg,» [En línea]. Available: https://ffmpeg.org/. [Último acceso: Diciembre 2023].

[11] «GitHub,» [En línea]. Available: https://github.com/danielgtaylor/qtfaststart. [Último acceso: Octubre 2024].

[12] «MediaInfo,» [En línea]. Available: https://mediaarea.net/en/MediaInfo. [Último acceso: Octubre 2024].

[13] «AtomicParsley,» [En línea]. Available: https://atomicparsley.sourceforge.net/. [Último acceso: Octubre 2024].

[14] «Bento4,» [En línea]. Available: https://www.bento4.com/. [Último acceso: Octubre 2024].

[15] U. E. P. d. S. Elena, «Lineas de Investigación,» 16 Junio 2022. [En línea]. Available: https://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Ite. [Último acceso: Octubre 2024].

[16] G. J. Cabrera, «Dialnet,» *Apuntes de Ciencia y Sociedad,* vol. 1, nº 2, 2011.

[17] S. N. d. Planificación, «Plan de Creacion de Oportunidades,» 2021. [En línea]. Available: https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Plan-de-Creaci%C3%B3n-de-Oportunidades-2021-2025-Aprobado_compressed.pdf. [Último acceso: Octubre 2024].

[18] E. Casey, «Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet,» *Academic Press*, vol. 3, 2011.

[19] H. Farid, «Photo Forensics,» *MIT Press,* 2016.

[20] S. Stamm, W. Wu y K. J. Liu, «Information forensics: Detecting falsified multimedia content,» *Signal Processing Magazine,* vol. 26, nº 2, pp. 27-36, 2009.

[21] H. Kaur y R. Singh, «Review on hash-based techniques in digital forensics,» *Forensic Science International,* vol. 287, pp. 1-8, 2017.

[22] L. Verdoliva, «Media forensics and deepfakes: An overview,» *Journal of Selected Topics in Signal Processing,* vol. 14, nº 5, pp. 982-992, 2020.

[23] P. Richardson, «ExifTool: Metadata extraction for forensic analysis,» *Digital Investigation Tools and Techniques,* vol. 6, nº 3, pp. 103-107, 2012.

[24] A. F. Smeaton, P. Over y W. Kraaij, «Evaluation campaigns and TRECVID,",» *Proceedings of the ACM International Conference on Multimedia Retrieval,* vol. 12, nº 2, pp. 1-8, 2010.

[25] C. Krotofil y M. Golling, «Open-source tools in digital forensic investigations: Challenges and benefits,» *Journal of Digital Forensics,* vol. 9, nº 4, pp. 24-31, 2014.

[26] A. Swaminathan, M. Wu y K. R. Liu, «IEEE Xplore,» *Digital image forensics via intrinsic fingerprints,* vol. 3, nº 1, pp. 101-117, 2008.

[27] B. Gurunlu1 y S. Ozturk, «A Survey on Photo Forgery Detection Methods,» Enero 2018.

[28] W. Wang y H. Farid, «Exposing digital forgeries in video by detecting double MPEG compression,» pp. 37-47, 2006.

[29] J. He, Z. Lin, L. Wang y X. Tang, «Detecting doctored JPEG images via DCT coefficient analysis,» vol. 3, pp. 423-435, 2006.

[30] M. C. Stamm, S. K. Tjoa, W. S. Lin y K. J. R. Liu, «Anti-forensics of JPEG compression,» de *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, Dallas, TX, USA, 2010.

[31] S. Bayram, H. T. Sencar y N. Memon, «An efficient and robust method for detecting copy-move forgery,» pp. 1053-1056, 2009.

[32] F. Yang, Y. Li, K. Chong y B. Wang, «Double JPEG Compression Detection Based,» 2018.

[33] A. C. Popescu y H. Farid, «Exposing Digital Forgeries by Detecting Traces of Re-sampling,» vol. 53, nº 2, pp. 758-767, 2005.

[34] J. Fridrich, «Digital image forensics,» vol. 26, nº 2, pp. 26-37, Abril 2009.

[35] B. Mahdian y S. Saic, «Detecting double compressed JPEG images,» 2010.

[36] Z. Lin, J. He, X. Tang y C.-K. Tang, «Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis,» *Pattern Recognition,* vol. 42, nº 11, p. 2492–2501, 2009.

[37] N. Memon y H. T. Sencar, «Overview of State-of-the-Art in Digital Image Forensics,» pp. 325-347, 2008.

[38] W. Wang y H. Farid, «Detecting Re-projected Video,» vol. 5284, pp. 47-52, 2006.

[39] D. G. Lowe, «Distinctive Image Features from Scale-Invariant Keypoints,» *International Journal of Computer Vision,* vol. 60, pp. 91-110, 2004.

[40] A. Rocha, W. Scheirer, T. Boult y S. Goldenstein, «Vision of the unseen: Current trends and challenges in digital image and video forensics,» *ACM Computing Surveys,* vol. 43, nº 4, pp. 1-42, 11 Octubre 2011.

[41] N. Xie, T. Liu y Y. Fu, «Forensic Analysis of Video Files Using Metadata,» 2021. [En línea]. Available: https://ieeexplore.ieee.org/document/9523116. [Último acceso: Noviembre 2024].

[42] A. Piva, «An Overview on Image Forensics,» *International Scholarly Research Notices,* vol. 2013, 2013.

[43] A. C. Popescu y H. Farid, «Statistical Tools for Digital Forensics,» *International Workshop on Information Hiding,* vol. 3200, pp. 128-147, 2004.

[44] M. C. Stamm y K. J. R. Liu, «Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints,» vol. 5, nº 3, pp. 492-506, 2010.

[45] W. J. Scheirer, A. Rocha, R. J. Micheals y T. E. Boult, «Meta-Recognition: The Theory and Practice of Recognition Score Analysis,» *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 33, nº 8, pp. 1689-1695, 2011.

[46] S. Lyu y H. Farid, «How realistic is photorealistic?,» *IEEE Transactions on Signal Processing,* vol. 53, nº 2, pp. 845-850, 2005.

[47] T. Pevny, P. Bas y J. Fridrich, «Steganalysis by Subtractive Pixel Adjacency Matrix,» *IEEE Transactions on Information Forensics and Security,* vol. 5, nº 2, pp. 215-224, 2010.

[48] J. J. Harmsen y W. A. Pearlman, «Steganalysis of additive-noise modelable information hiding,» *Proc. SPIE 5020, Security and Watermarking of Multimedia Contents V,* 2003.

[49] A. Westfeld, «F5—A Steganographic Algorithm,» *Information Hiding,* pp. 289-302, 2001.

[50] K. Huixian, Y. Biao y W. Hanzhou, «Recent Advances in Text Steganography and Steganalysis,» *Journal of Applied Sciences,* vol. 39, nº 6, pp. 923-938, 2021.

[51] G. Chetty y M. Wagner, «Audio-Visual Multimodal Fusion for Biometric Person Authentication,» *ACM International Conference Proceeding Series,* vol. 163, pp. 17-24, 2006.

[52] T. Alldieck, M. Kassubeck y M. Magnor, «Optical Flow-based 3D Human Motion Estimation from Monocular Video,» *Computer Vision and Pattern Recognition,* pp. 347-360, 2017.

[53] W. Luo, J. Huang y G. Qiu, «Robust Detection of Region-Duplication Forgery in Digital Image,» *18th International Conference on Pattern Recognition (ICPR'06),* pp. 746-749, 2006.

[54] V. Christlein, C. Riess, J. Jordan, C. Riess y E. Angelopoulou, «An Evaluation of Popular Copy-Move Forgery Detection Approaches,» *IEEE Transactions on Information Forensics and Security,* vol. 7, nº 6, pp. 1841-1854, 2012.

[55] S. Milani, M. Fontani, P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi y S. Tubaro, «An overview on video forensics,» *APSIPA Transactions on Signal and Information Processing,* vol. 1, 2012.

[56] J. v. Neumann, « Probabilistic logics and the synthesis of reliable organisms from unreliable components,» de *Automata studies*, 1956, pp. 43-98.

[57] W. Wang y H. Farid, « Exposing digital forgeries in video by detecting double MPEG,» *Proceedings of the 8th workshop on Multimedia and security*, pp. 37-47, 2006.

[58] A. Swaminathan, M. Wu y K. R. Liu, «Digital image forensics via intrinsic fingerprints,» *IEEE Transactions on Information Forensics and Security*, vol. 3, nº 1, pp. 101-107, 2008.

[59] H. T. Sencar y N. Memon, «Overview of State-of-the-Art in Digital Image Forensics,» pp. 325-347, 2008.

[60] A. Popescu y H. Farid, «Exposing digital forgeries by detecting traces of resampling,» *IEEE Transactions on Signal Processing*, vol. 53, nº 2, pp. 758-767, 2005.

[61] J. Fridrich, «Digital image forensics,» *IEEE Signal Processing Magazine*, vol. 26, nº 2, pp. 26-27, 2009.

[62] Z. Lin, J. He, X. Tang y C.-K. Tang, «Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis,» *Pattern Recognition*, vol. 42, nº 1, pp. 2492-2501, 2009.

[63] W. Wang y H. Farid, «Detecting Re-projected Video,» p. 72–86, 2008.

[64] D. G. Lowe, «Distinctive Image Features from Scale-Invariant Keypoints,» *International Journal of Computer Vision*, vol. 60, pp. 91-110, 2004.

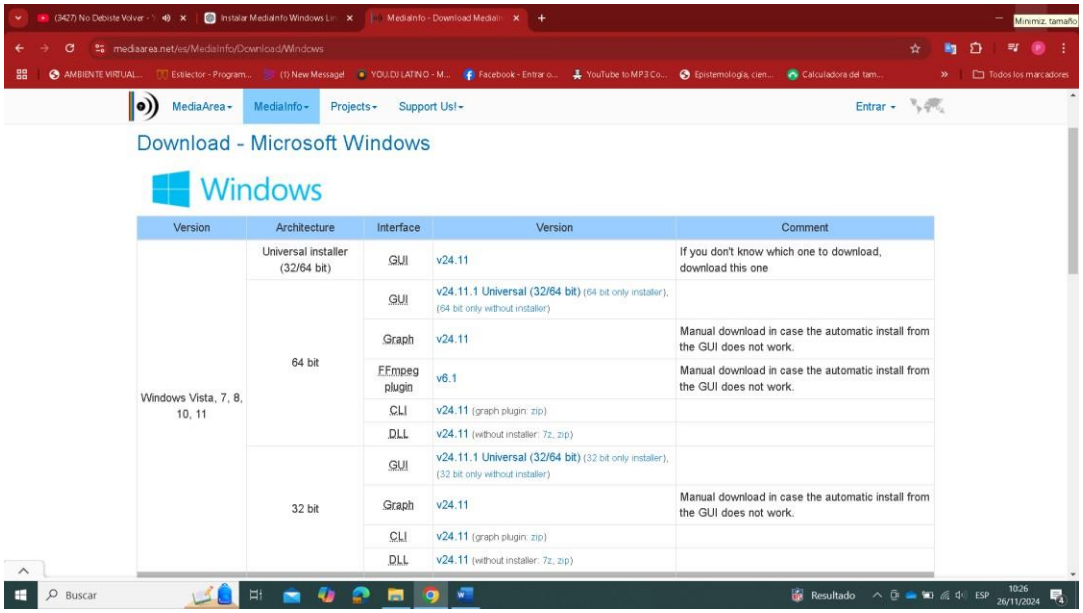
[65] A. Rocha, W. Scheirer, T. Boult y S. Goldenstein, «Vision of the unseen: Current trends and challenges in digital image and video forensics,» *ACM Computing Surveys,* vol. 43, nº 26, pp. 1-42, 2011.

[66] D. Skraparlis, «Design of an efficient authentication method for modern image and video,» *IEEE Transactions on Consumer Electronics,* vol. 49, nº 2, pp. 417-426, 2003.

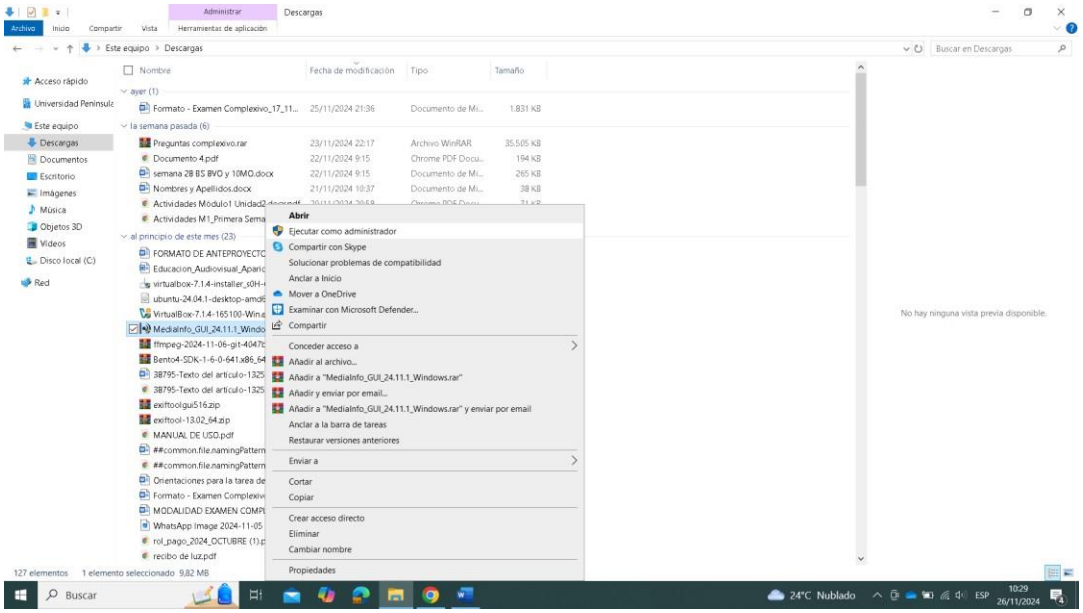
[67] Sampieri, Metodología de la Investigación, México: McGRAW-HILL, 2010.

ANEXOS

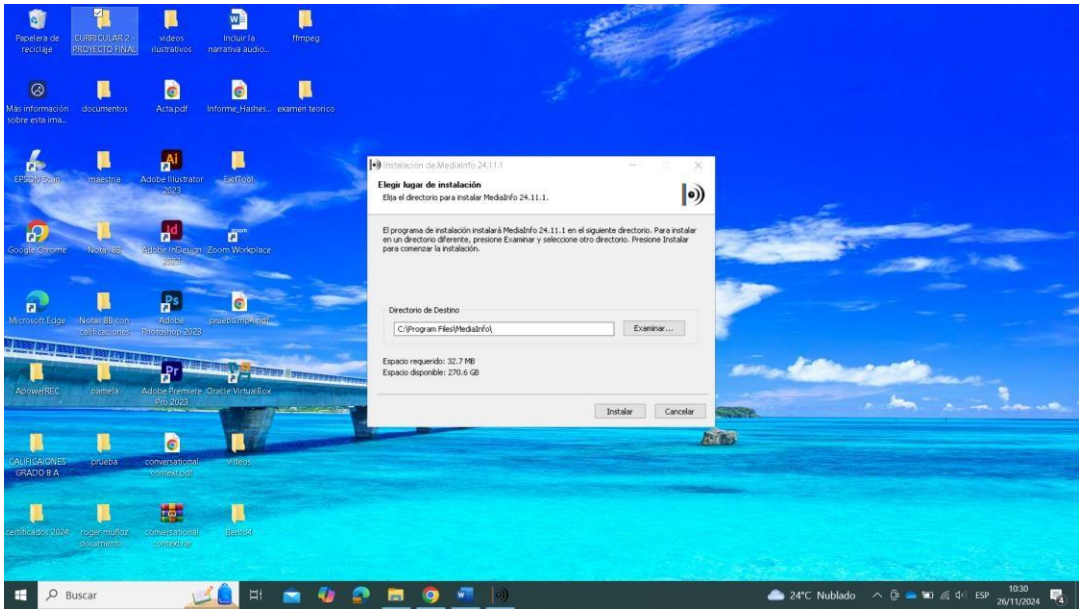
Anexo 1: Descargamos de la página oficial MediaInfo para Windows "https://mediaarea.net/es/MediaInfo/Download/Windows".



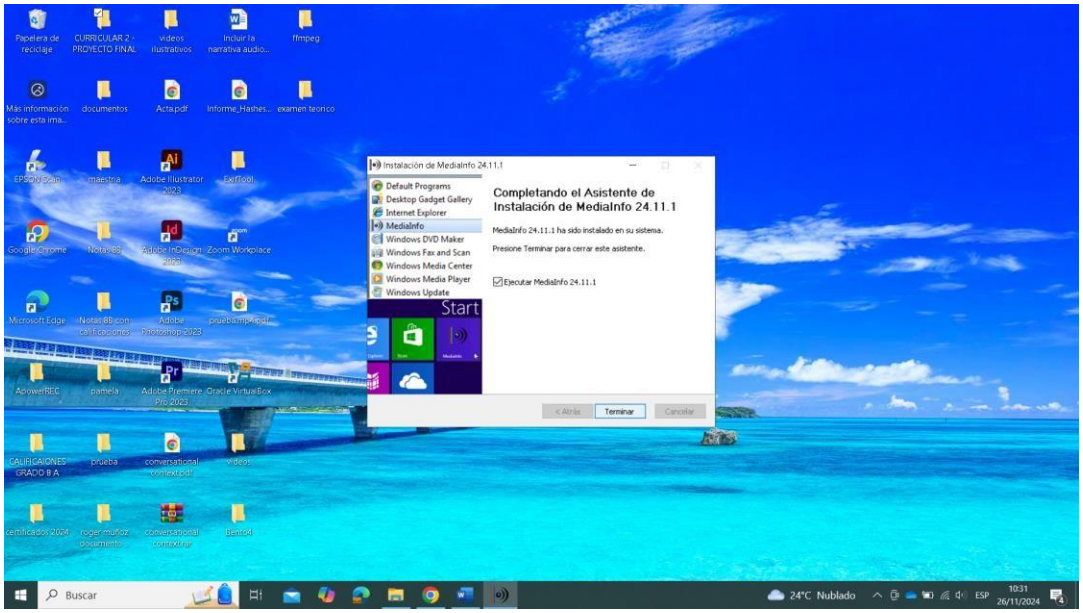
Anexo 2: Ejecutamos el archivo descargado (.exe) y lo ejecutamos como administrador.



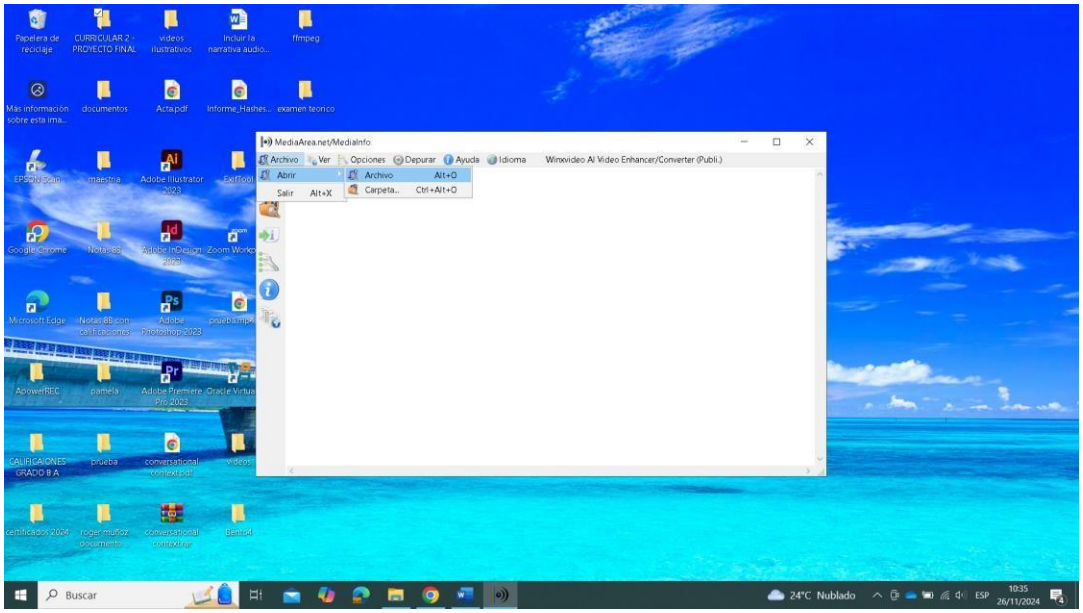
Anexo 3: Colocamos la opción “**INSTALAR”** para continuar.



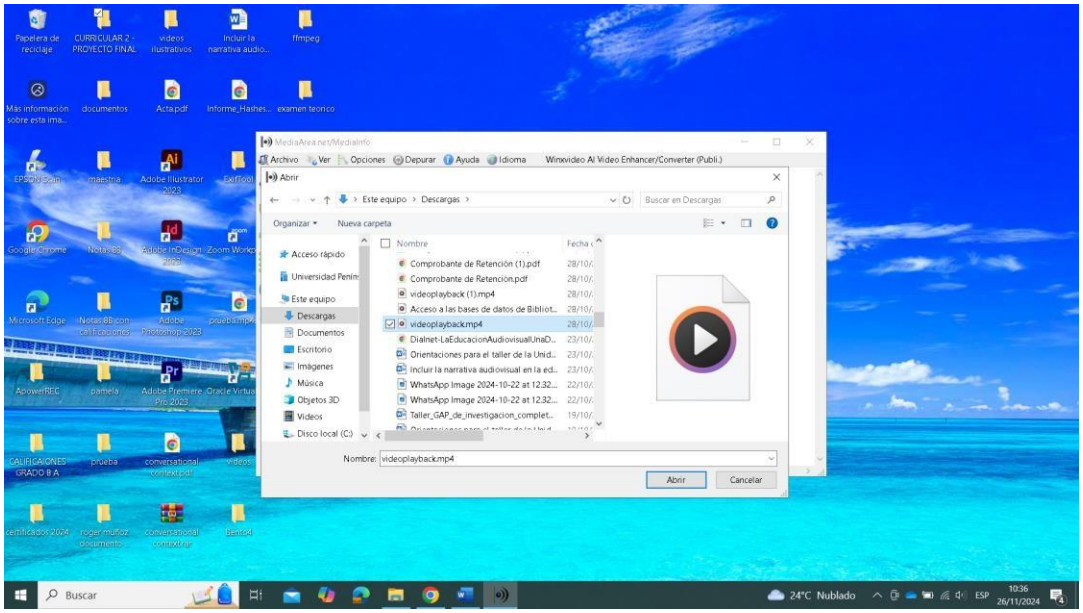
Anexo 4: Presionamos “TERMINAR” para comenzar a utilizar.



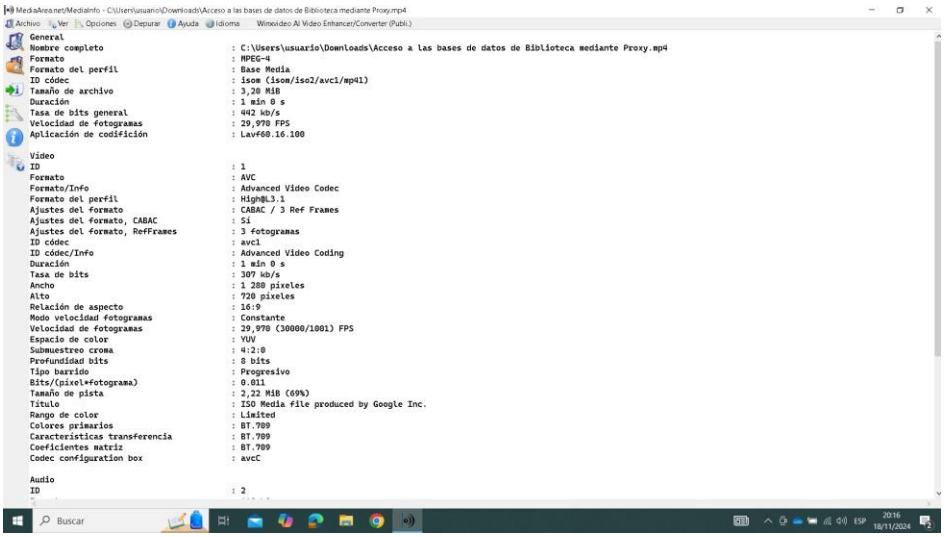
Anexo 5: Una vez abierto procedemos a abrir el archivo a trabajar.



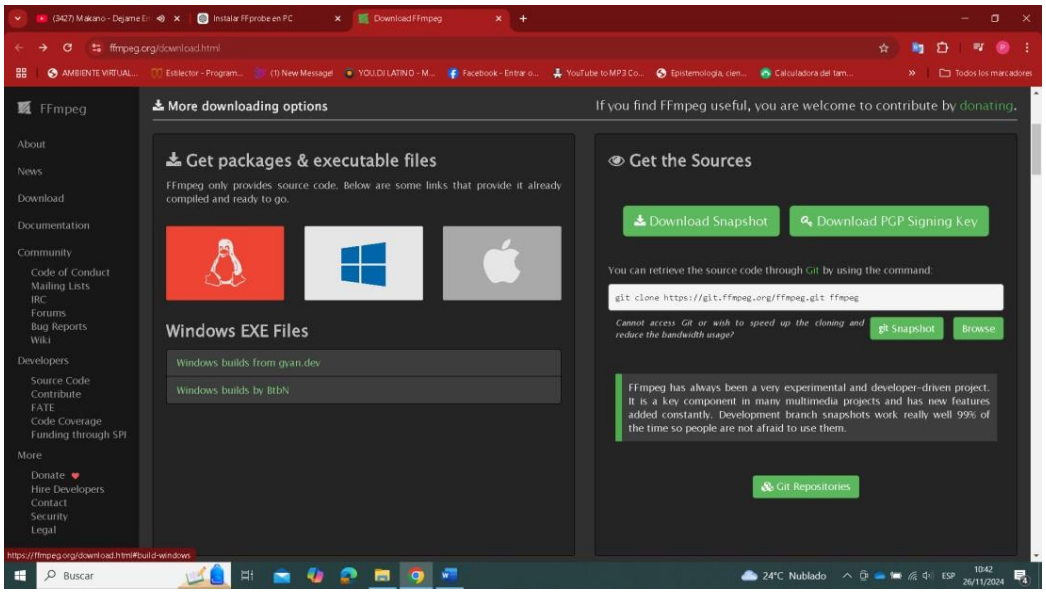
Anexo 6: Seleccionamos el archivo y esperamos los resultados.



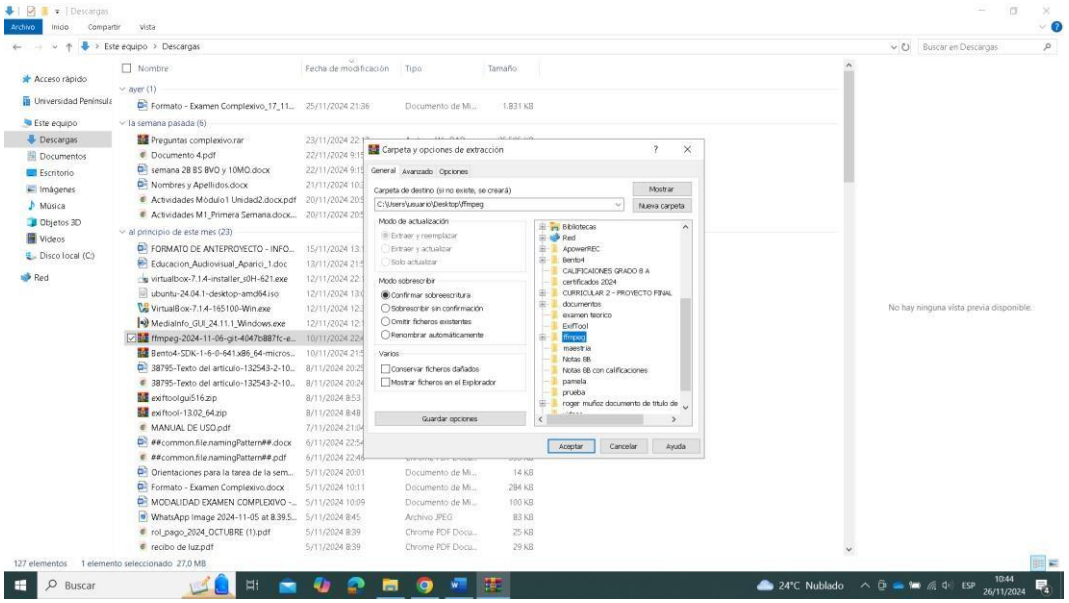
Anexo 7: Resultado obtenido de la herramienta MediaInfo.



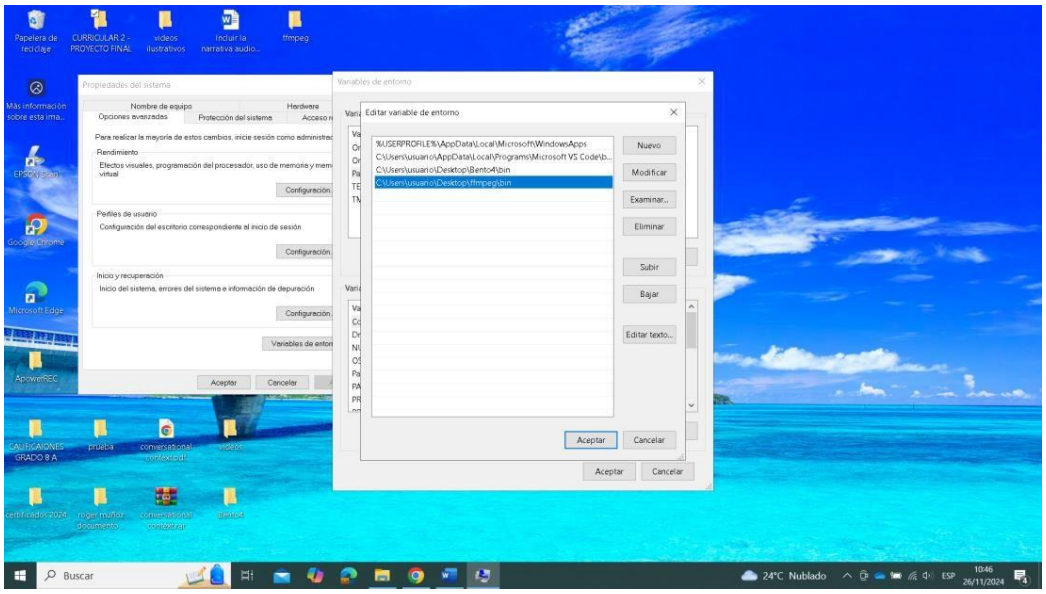
Anexo 8: Vamos a al siguiente link para poder descargar el ejecutable para Windows “https://ffmpeg.org/download.html”.



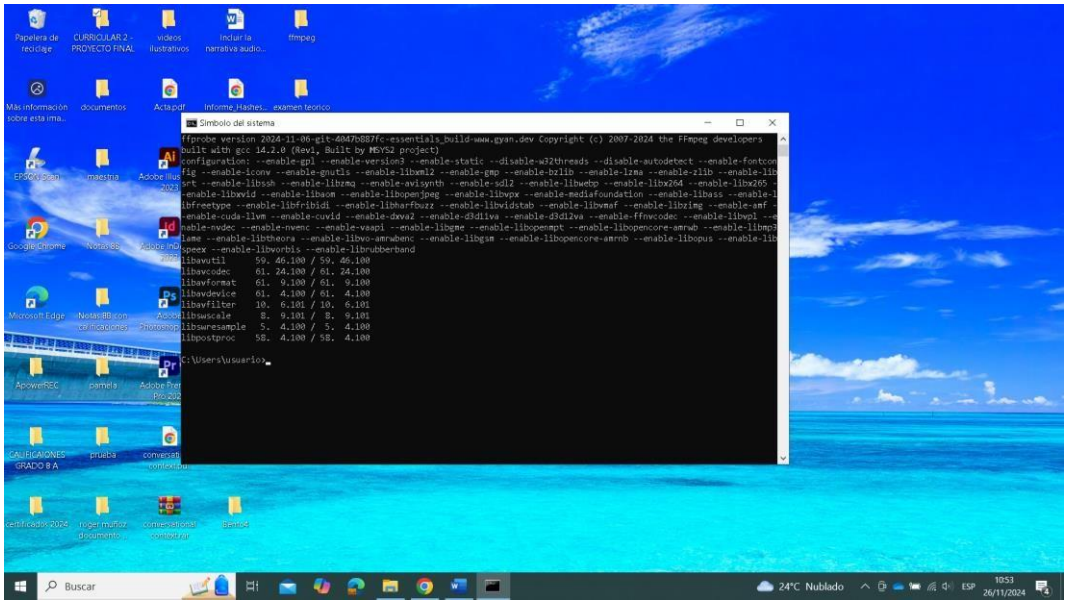
Anexo 9: Descomprimimos el archivo en una carpeta creada en el escritorio con el nombre **“FFPROBE”.**



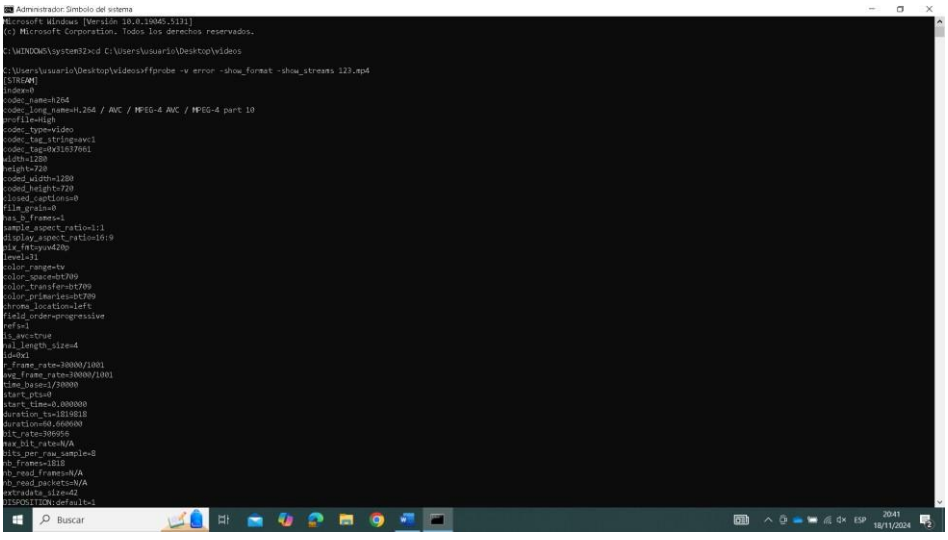
Anexo 10: Abrimos “Panel de control” elegimos “Sistema y seguridad” la opción “Sistema” hacemos clic en “Configuración avanzada del sistema” en la ventana que aparece y seleccionamos “Variables de entorno” buscamos la variable “Path” en las “Variables del sistema” editamos y colocamos la ruta donde esta ffprobe “C:\Users\usuario\Desktop\ffmpeg\bin”.



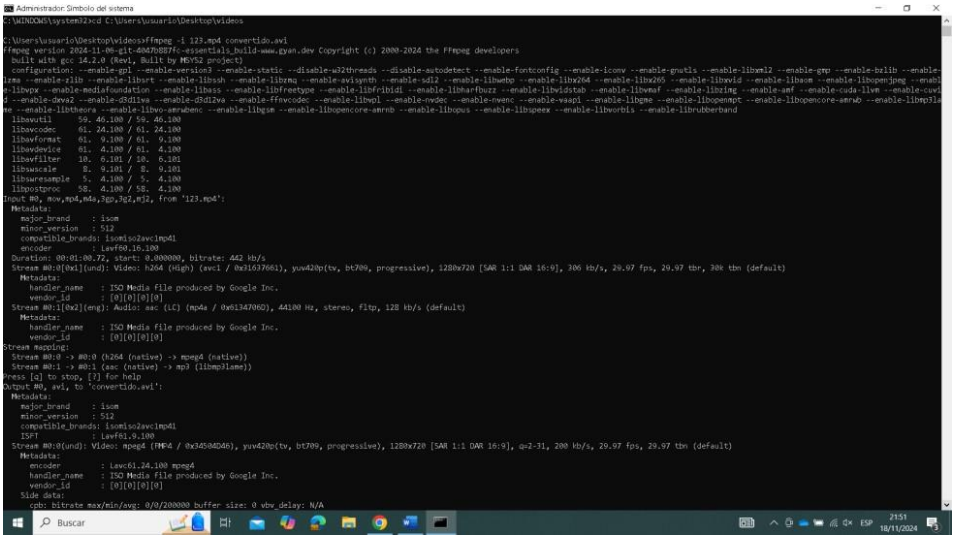
Anexo 11: Abrimos “cmd” y comprobamos si esta correctamente instalado y la versión que tenemos con el siguiente comando “ffprobe -version”.



Anexo 12: Resultado obtenido de la herramienta FFprobe con el siguiente código “ffprobe -v error -show_format -show_streams 123.mp4”.



Anexo 13: Resultado obtenido de la herramienta FFmpeg cambiando a formato **avi** con el siguiente código “ffmpeg -i 123.mp4 convertido.avi”.



Anexo 14: Resultado obtenido de la herramienta FFmpeg extrayendo el audio al formato mp3 con el siguiente código “ffmpeg -i 123.mp4 -q:a 0 -map a audio.mp3”.