Diálogo Forense
Num. 4, Vol. 2, 2021
ISSN: 2789-8458

Análisis forense sobre imágenes digitales, un ejemplo de su aplicabilidad

Fredy Emanuel Sánchez Gálvez
Laboratorio de Informática Forense
Instituto Nacional de Ciencias Forenses -INACIF-
frsanchez122@gmail.com

Recibido: 20/07/2021
Aceptado: 21/10/2021

Palabras clave: Imagen digital, análisis forense, metadatos, fotoforensic, forensically, imagen alterada

Key words: digital image, forensic analysis, metadata, photoforensic, forensically, forensically, altered image.

RESUMEN

De acuerdo a Cayetano (2020) una imagen es un arreglo de píxeles, o puntos de muestreo, que contienen información sobre la intensidad de color en la ubicación de cada pixel.

Existen distintas técnicas para hacer modificaciones a una imagen digital, desde aclarar tonalidades, hasta hacer fotomontajes profesionales. El análisis forense sobre imágenes digitales comprende un conjunto de técnicas, las cuales intentan detectar las modificaciones o alteraciones realizadas a una imagen.

Cabe resaltar que estas técnicas son indiciarias, lo que significa que únicamente nos darán indicios de la existencia de una posible alteración, por lo que es necesaria la aplicación de dos o más de estas con el fin de establecer dicha alteración.

ABSTRACT

According to Cayetano (2020) an image is an array of pixels, or sampling points, that contain information about the color intensity at the location of each pixel.

There are different techniques to make modifications to a digital image, from brightening tonalities to professional photomontages. The forensic analysis of digital images comprises a set of techniques, which attempt to detect the modifications or alterations made to an image.

It should be noted that these techniques are indicative, which means that they will only give us indications of the existence of a possible alteration, therefore, it is necessary to apply two or more of these techniques in order to establish the alteration.

INTRODUCCIÓN

Actualmente los avances tecnológicos han marcado la tendencia de portabilidad y facilidad de manejo de los dispositivos electrónicos de procesamiento y/o almacenamiento de datos, lo que permite disponibilidad, acceso a información y estar siempre comunicados en cualquier lugar e incluso en cualquier momento.

Hasta enero del año 2021, We Are Social and Hootsuite reporta para Guatemala 20.7 millones de dispositivos móviles activos, excluyendo internet de las cosas (IoT por sus siglas en inglés), lo que representa el 114.7% con respecto al total de la población del país. Es evidente que en la actualidad es muy sencillo tener acceso a dispositivos móviles con suficientes prestaciones para un usuario promedio, tales como capacidad de procesamiento, almacenamiento, duración de la batería y cámaras con media o alta resolución. Dichas prestaciones han llevado a la generación y almacenamiento de grandes cantidades de contenido digital como registros, datos y archivos que se pueden localizar en un dispositivo móvil, como las imágenes digitales.

En un proceso judicial, penalmente, es posible presentar cualquier elemento que constituya una prueba, lo que podría abarcar una base de datos, un documento electrónico, un archivo de multimedia o un archivo de imagen, sin embargo, estas últimas pueden ser motivo de discordia entre las partes al suponer una posible manipulación en su contenido.

Existen programas que permiten editar imágenes digitales para agregar, alterar o quitar elementos de estas con distintos objetivos, como inculpar a personas de un hecho o bien deslindarse de una responsabilidad.En este sentido, la informática forense como disciplina desde el ámbito técnico-científico, sirve como apoyo a la administración de justicia y el derecho (Ortiz, 2019). Esta disciplina, a nivel genérico, abarca técnicas de adquisición, preservación, obtención y presentación de evidencia del tipo digital, sin embargo, es posible que cuando se trate de una presunta imagen alterada deba realizarse un análisis aún más profundo.

La Imagen Digital

A nivel físico, La Real Academia Española, define imagen como "figura, representación, semejanza y apariencia de algo" (Real Academia Española, 2001).

A nivel digital, Bustamante (2013) indica que una imagen (imagen digital) es una representación del mundo físico que tiene información importante, la cual es captada mediante un proceso de muestreo, generalmente por medios electrónicos.

Como complemento, Cayetano (2020), describe una imagen como un arreglo de píxeles, o puntos de muestreo, que contienen información sobre la intensidad de color en la ubicación de cada pixel.

Con estos conceptos y definiciones se puede aseverar que la imagen digital es la representación de algo físico, que a través de procesos de digitalización se transforma en un archivo que consiste en una matriz de puntos o píxeles que contienen información sobre la intensidad de color.

Existen dos modos que se utilizan para representar imágenes digitales: 1) imagen como Mapa de Bits, que es una matriz de puntos con distintas tonalidades de color; y 2) como imágenes vectoriales que son gráficos orientados a objetos que almacenan reglas para dibujado de objetos geométricos (Pelayo, 2017).

Para la elaboración de la presente investigación se hará referencia a la representación de mapas de bits, como lo son, las fotografías digitales.

Técnicas Para el Análisis de Imágenes Digitales

En el análisis de imágenes digitales existen diferentes técnicas que permiten obtener información de interés que sean de valor para la investigación.

En cuanto a la aplicación de estas técnicas, es importante mencionar que se necesita de software específico, capacitación, conocimiento y experiencia del analista para ubicar errores de compresión, inconsistencias de zonas, patrones repetidos, metadatos originales o alterados, ruido o interferencia en la imagen y otras características indiciarias que permitan establecer la autenticidad de una imagen.

Cabe destacar que no existe una técnica 100% fiable que permita obtener una conclusión definitiva para establecer la plena autenticidad de una imagen digital, por lo que muchas de estas técnicas son únicamente indiciarias y se debe acudir a la aplicación de dos o más de estas.

A continuación se describen algunas de las técnicas de análisis forense de imágenes digitales:

1. **Análisis de metadatos**
   Es el primero que se recomienda realizar para un análisis de imágenes digitales ya que los archivos de imagen cuentan con características que brindan información de interés, tales como tipo de cámara o dispositivo con la cual fue capturada la imagen, apertura de la lente, fechas de creación y/o modificación que permiten obtener líneas de tiempo, modo de color utilizado, datos de geolocalización, software de manipulación (si así fuera), entre otros.

   El mayor problema que tiene este tipo de análisis es que los metadatos son bastante vulnerables a cambios que pudieran hacer terceros sobre estos, entiéndase alteración de fechas o la eliminación de toda la información. Asimismo es importante mencionar que todas las imágenes pierden propiedades al ser compartidas a través de mensajería instantánea o bien al publicarse en una red social.

2. **Análisis por matriz de cuantificación**
   Consiste en la extracción de matrices de cuantificación de las imágenes. Una matriz de cuantificación es un conjunto de valores utilizados para la representación de las imágenes.

   Para la aplicación de esta técnica es necesario un patrón de cotejo o comparación con la cual se puedan analizar ambos resultados.

   Tal vez el mayor problema que enfrenta esta técnica, es posiblemente, que una matriz de cuantificación puede ser alterada o modificada con el simple hecho de aclararle tonalidades a la imagen.

3. **Análisis de ruido de foto respuesta no uniforme (PRNU)**
   El ruido de una fotografía o imagen digital es la diferencia entre el valor teórico de la transcripción de luz que incide en los píxeles y el valor registrado por estos (Igual, 2019).

   El ruido de foto respuesta no uniforme (PRNU) es una característica de cada sensor en una cámara digital, el cual está formado principalmente por la uniformidad de pixel (*Pixel Non-Uniformity*) y los defectos de baja frecuencia como la configuración del zoom y la refracción de la luz en las partículas de polvo y lentes (Rosales, 2013).

   Un análisis de este tipo requiere contar con el dispositivo que hizo la captura de la imagen y generar con este dos o más imágenes planas que deben ser tomadas bajo las mismas condiciones de iluminación y sin ningún tipo de escena. Esto generará un PRNU aún más simple de encontrar, el cual servirá de patrón de referencia.

   Teniendo el PRNU de referencia, se debe obtener el patrón PRNU de la imagen a analizar y utilizando software forense específico se debe verificar a través de un proceso de correlación que muestre la correspondencia de ambos PRNU.

   "Una imagen digital adquirida con el dispositivo en cuestión obtiene un valor de correlación cercano a uno, mientras que para imágenes que no fueron obtenidas con el dispositivo analizado, los valores de correlación tienden a cero e incluso pueden ser negativos" (Luengo, 2017, párr. 9).

4. **Análisis de zonas clonadas, copiadas o movidas**
   Esta técnica consiste en identificar posible patrones que se repiten en una imagen, debido a la técnica de manipulación denominada "*Copy-Move*", la cual consiste en tomar un fragmento de la misma y sobreponerlo para ocultar un objeto, o bien, para duplicar los ya existentes en esta.

   Como se ha mencionado, esta técnica de detección de manipulaciones en imágenes digitales, se centra puntualmente en la búsqueda de áreas duplicadas (Armas, Sandoval y García, 2020).

   Al igual que las anteriores, esta técnica se enfrenta a que si la manipulación "*copy-move*" se combina con otras tales como aplicación de filtros, será muy difícil ubicar o detectar las áreas que se ha modificado y es que muchos de los programas de edición de imágenes cada día mejoran sus funciones que evitan la detección del clonado.

5. **Análisis de bordes:**
   La detección de bordes es una técnica de análisis digital que puede ser aplicada sobre imágenes en dos o tres dimensiones, la cual intenta ubicar la frontera entre dos regiones diferentes de esta (Técnica en Laboratorio, s.f.).

   Un borde puede ser el resultado de cambios en la absorción de la luz (color/sombra), que pueden determinar la profundidad, tamaño, orientación y propiedades de la superficie.

Los bordes en una imagen, en su forma más simple, pueden ser identificados, grabando los cambios en la intensidad de luz sobre un número de píxeles, cambiando toda la imagen a una escala de grises (Tecnica en Laboratorio, s.f.).

A través de esta técnica se pueden detectar los bordes que se generan entre dos fragmentos de imágenes distintas o de la misma imagen con distintas tonalidades de intensidad de luz.

No es posible detectar bordes cuando los fragmentos copiados pasan por un proceso de suavizado de bordes o denominados filtros paso-bajo, los cuales reducen los picos de ruido y hacen menos bruscos los cambios de intensidad de la imagen (Aguirre, 2013).

6. **Error Level Analysis (ELA):** El análisis de nivel de error es el análisis de los artefactos de compresión en datos digitales con compresión con pérdida como lo es el formato JPEG (R. F, 2017).

   El análisis de nivel de error de la imagen se basa en mostrar el nivel de compresión de cada pixel, aplicando distintos colores a las áreas con mayor error. Esto brinda como resultado que la imagen pueda tener variaciones entre blanco, negro, azul y rojo (Luengo, 2017).

   Uno de los mayores problemas es que no brinda resultados con archivos en formatos distintos a JPEG nativos, ya que se fundamenta en la naturaleza de su proceso de compresión.

   El algoritmo de compresión JPEG organiza la imagen en bloques de 8x8 píxeles que una vez sometidos a diversos ciclos de compresión generan lo que se conoce como el **error level** (Pereira, 2015).

   Una imagen no editada mostrará un ELA uniforme con un nivel de intensidad muy bajo (negro) pero a medida que se introducen ajustes o fotomontajes se muestran inconsistencias entre los elementos de la imagen, de forma que el ELA va tomando más intensidad (blanco).

   Es importante hacer mención que una imagen nativa JPEG (original), tiene errores ELA altos, por lo que tiende a mostrar más tonalidades blancas, mientras que cada vez que se guarda la imagen, reducirá el potencial de nivel de error, produciendo un resultado ELA más oscuro.

   El análisis de nivel de error (ELA) proporciona indicios, pero no confirma o concluye que una imagen digital haya sido modificada.

Ejemplo de análisis forense sobre imágenes digitales

A continuación se muestra un ejemplo del análisis forense de imágenes digitales de algunas de las técnicas descritas anteriormente.

En esta práctica se hizo uso de herramientas gratuitas, que permiten obtener información sobre la autenticidad de una imagen. Se hizo uso de las siguientes herramientas de software:

a) FOCA (*Fingerprinting Organizations with Collected Archives)*: Es una herramienta de software desarrollada con el objetivo de extraer los metadatos e información oculta de distintos archivos, no importando si estos se encuentran en sitios web o localmente.

b) *ExifTool*: Es una herramienta en línea de comando que se utiliza para extraer metadatos de archivos de imagen.

c) *Forensically:* Es una solución web de uso libre que permite la aplicabilidad de distintas técnicas de análisis sobre imágenes digitales, análisis de nivel de error (ELA), análisis de zonas clonadas, análisis de ruido. Incluso permite analizar los más mínimos detalles a nivel de píxeles.

d) *Fotoforensic:* Al igual que la solución anterior, es una herramienta web especializada en el análisis ELA, la cual permite el uso de archivos en formato JPEG, PNG y otros formatos de compresión con pérdida.

METODOLOGÍA

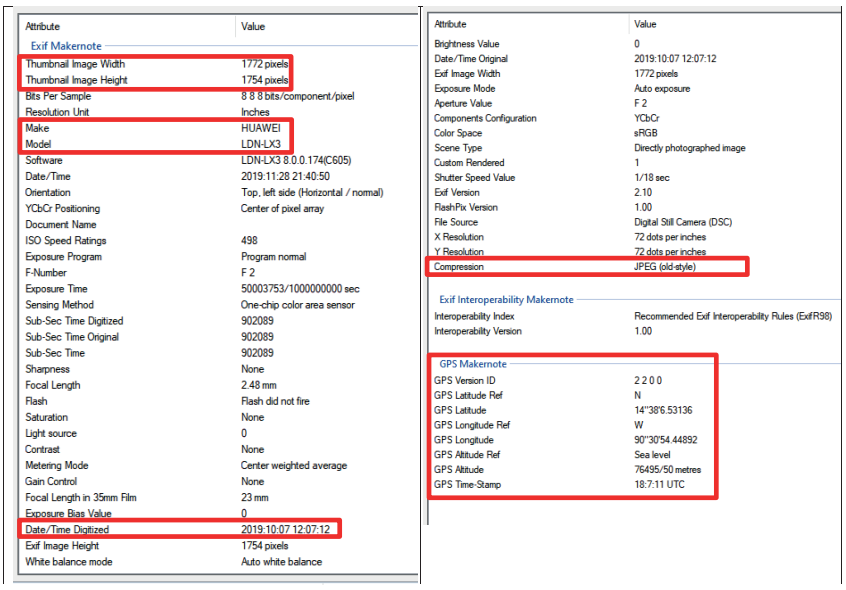
- Se realizó la extracción de metadatos de una imagen digital adquirida de manera controlada.
- Se interpretaron los metadatos de interés para fines de este ejemplo.
- Se interpretaron alteraciones a la imagen digital y se procedió a leer nuevamente sus metadatos.
- Se interpretaron análisis de zonas clonadas, análisis de bordes y análisis ELA, utilizando las herramientas *web Forensically y Fotoforensic*.

A continuación se muestra la imagen digital denominada imagen original, la cual fue adquirida utilizando procesos forenses que garantizan su integridad.

Imagen 1. Imagen original

Utilizando el programa FOCA *(Fingerprinting Organizations with Collected Archives)*, se realizara la lectura de metadatos. Estos metadatos muestran información de valor que permite al analista una visión más clara para poder determinar si una imagen es original.

Se puede observar en los metadatos (imagen 2), que el archivo de imagen tiene un tamaño de 1772 píxeles de ancho por 1754 píxeles de alto, fue creado con un dispositivo móvil marca HUAWEI, modelo LDN-LX3, su fecha de captura o digitalización fue el 07/10/2019 a las 12:07:12 horas, la imagen tiene formato de compresión JPEG, asimismo se puede observar que la imagen tiene etiquetas de georeferencia (GPS), con lo cual se podría ubicar en *Google Maps* (imagen 4).



Attribute	Value
Exif Makernote	
Thumbnail Image Width	1772 pixels
Thumbnail Image Height	1754 pixels
Bits Per Sample	8 8 8 bits/component/pixel
Resolution Unit	Inches
Make	HUAWEI
Model	LDN-LX3
Software	LDN-LX3 8.0.0.174(C605)
Date/Time	2019:11:28 21:40:50
Orientation	Top, left side (Horizontal / normal)
YCbCr Positioning	Center of pixel array
Document Name	
ISO Speed Ratings	498
Exposure Program	Program normal
F-Number	F 2
Exposure Time	50003753/1000000000 sec
Sensing Method	One-chip color area sensor
Sub-Sec Time Digitized	902089
Sub-Sec Time Original	902089
Sub-Sec Time	902089
Sharpness	None
Focal Length	2.48 mm
Flash	Flash did not fire
Saturation	None
Light source	0
Contrast	None
Metering Mode	Center weighted average
Gain Control	None
Focal Length in 35mm Film	23 mm
Exposure Bias Value	0
Date/Time Digitized	2019:10:07 12:07:12
Exif Image Height	1754 pixels
White balance mode	Auto white balance

Attribute	Value
Brightness Value	0
Date/Time Original	2019:10:07 12:07:12
Exif Image Width	1772 pixels
Exposure Mode	Auto exposure
Aperture Value	F 2
Components Configuration	YCbCr
Color Space	sRGB
Scene Type	Directly photographed image
Custom Rendered	1
Shutter Speed Value	1/18 sec
Exif Version	2.10
FlashPix Version	1.00
File Source	Digital Still Camera (DSC)
X Resolution	72 dots per inches
Y Resolution	72 dots per inches
Compression	JPEG (old-style)
Exif Interoperability Makernote	
Interoperability Index	Recommended Exif Interoperability Rules (ExifR98)
Interoperability Version	1.00
GPS Makernote	
GPS Version ID	2 2 0 0
GPS Latitude Ref	N
GPS Latitude	14°38'6.53136
GPS Longitude Ref	W
GPS Longitude	90°30'54.44892
GPS Altitude Ref	Sea level
GPS Altitude	76495/50 metres
GPS Time-Stamp	18:7:11 UTC

Imagen 2. Metadatos de la imagen original

Las etiquetas de georeferencia en las imágenes digitales, se muestran en grados, minutos y segundos, sin embargo para ubicar un punto de referencia en *Google Maps*, se necesitan datos en grados decimales, por lo que es necesario apoyarse de otras herramientas para la conversión, para efectos de este ejemplo se utilizó la página web "Coordenadas-gps.com", con la cual se obtuvo el formato de puntos de referencia (latitud y longitud) adecuado.

Imagen 3. Conversión a grados decimales

A continuación se muestra en Google Maps la posible ubicación en donde fue tomada la fotografía, según los metadatos registrados.

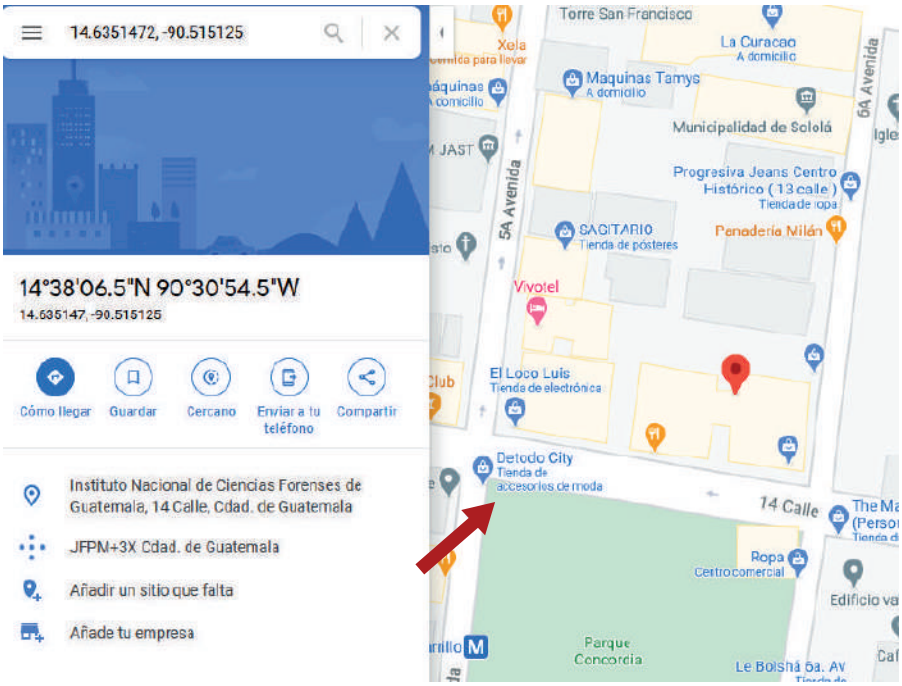


Imagen 4. Posible ubicación de captura de imagen

En muchas ocasiones, cuando una imagen digital es mejorada, alterada, es subida a una red social o es compartida a través de programas de mensajería instantánea, puede perder, adquirir o modificase algunos de sus metadatos, lo que brinda uno o más indicios que indican la posible modificación o alteración de esta.

A continuación se muestran los metadatos de la imagen alterada, esta vez se hizo uso del programa *ExifTool*, que al igual que FOCA, pueden leer metadatos de archivos de imagen.

En la imagen 5, se muestran algunos metadatos que dan indicios que una imagen fue alterada, por ejemplo la fecha de modificación, la cual fue 29/03/2021 a las 08:30:05 horas, zona horaria -6; otro indicio es el registro de un software de edición de imágenes, *Paint.Net* Versión 3.5.11, el cual efectivamente se utilizó intencionalmente para alterar dicha imagen.

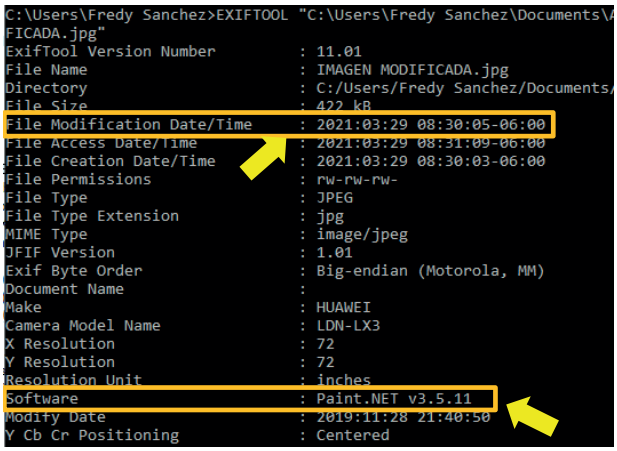


Imagen 5. Metadatos de imagen Modificada

Como bien se ha indicado anteriormente, se debe aplicar dos o más técnicas para determinar si una imagen fue alterada, por lo que en la imagen 6 se aplicó la técnica de detección de zonas clonadas, en donde se observan distintas líneas que marcan los bordes de posibles objetos clonados y la similitud en la intensidad de sus píxeles, este resultado da indicios de posibles objetos clonados a través de una técnica *copy-move*.

Imagen 6. Técnica de zonas clonadas

La siguiente técnica que se aplicó es la denominada **detección de bordes**, esta permitió visualizar la frontera entre objetos de una imagen, tal como se observa en la imagen 7. La herramienta *forensically* tiene la opción de aplicar esta técnica utilizando el gradiente de luminancia que puede detectar contornos de objetos difusos. En la imagen 7 se observa que el objeto (un papel) fue copiado y movido, alrededor de este se alcanza a visualizar un recuadro con bordes que no corresponden a la superficie, así como un rectángulo vertical que no pertenece a la misma.

Por último, se aplicó el análisis de nivel de error (ELA), con el cual se pudo observar aquellos elementos que posiblemente no pertenezcan a dicha imagen, los cuales son detectados por error en la compresión de sus píxeles. En la imagen 8 se observa el análisis ELA utilizando la herramienta *Forensically* y en la imagen 9 se observa el mismo análisis utilizando la herramienta FotoForensic, en ambas se puede apreciar en un color blanco, más fuerte que otras áreas, aquellos elementos pegados que no corresponden a dicha imagen.

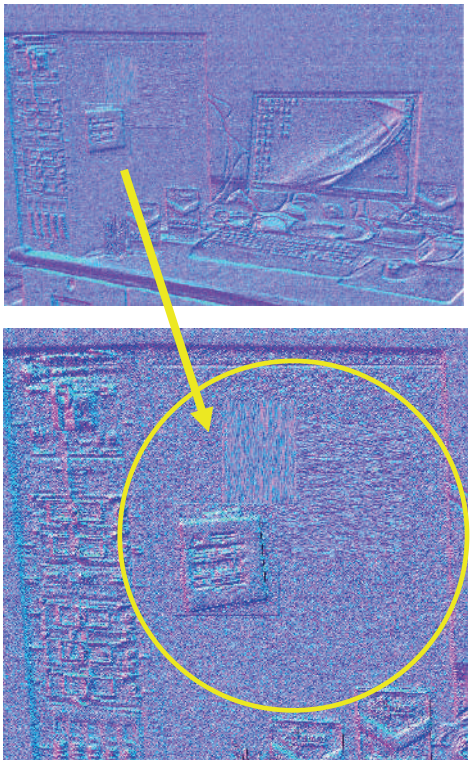


Imagen 7. Técnica de detección de bordes

Cada una de las técnicas descritas y ejemplificadas en la presente investigación, tienen la capacidad de detectar el tipo de modificación realizada sobre la imagen digital, por lo que es importante y recomendable la aplicación de dos o más de estas para establecer la posible alteración de la imagen en cuestión.

Para la ejemplificación del caso, se utilizaron distintas técnicas de alteración, las cuales no son detectadas utilizando simplemente una técnica de análisis, por lo que fue necesaria la aplicación de al menos cuatro. En la imagen 10 se muestra, tanto la imagen original (A), como la imagen alterada (B), la cual en muchos aspectos los cambios no son visibles a simple vista.

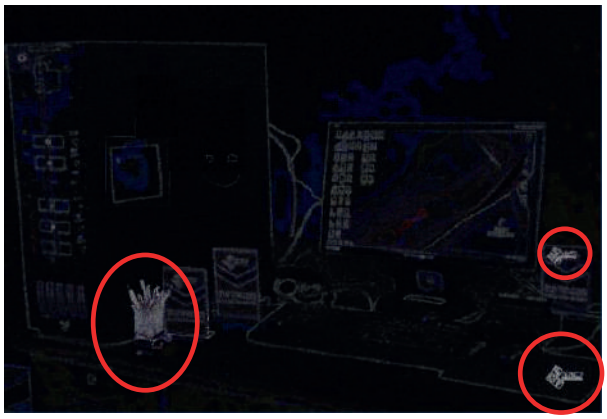


Imagen 8. Análisis ELA con Fotoforensic

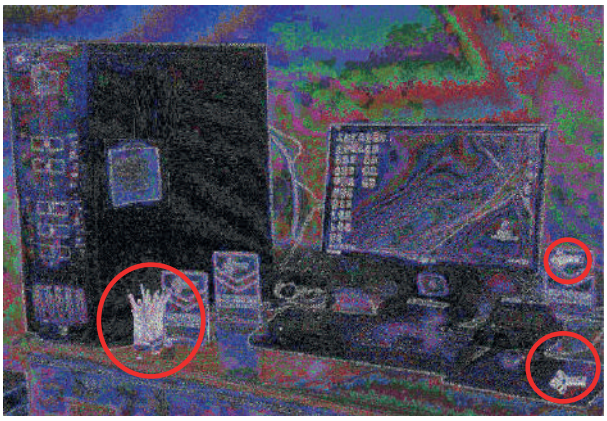


Imagen 9. Análisis ELA con Forensically

(A) (B)

Imagen 10. Imagen original e imagen alterada

CONCLUSIONES

La imagen digital es la representación del mundo físico, que a través de procesos de digitalización se transforma en un archivo que consiste en una matriz de puntos o píxeles los cuales contienen información sobre la intensidad de color.

Para la aplicación de las distintas técnicas de análisis descritas en la presente investigación, se necesita software específico, capacitación constante, conocimiento y experiencia del analista, para ubicar errores de compresión, inconsistencias de zonas, patrones repetidos, metadatos originales o alterados, ruido o interferencia y otras características indiciarias que permitan establecer la autenticidad o posible alteración de una imagen digital.

Existen distintas técnicas de procesamiento para manipular una imagen, tales como aclaración de tonalidades, clonación de alguna de las zonas de esta, rotación, sobreposición de un fragmento de otra imagen, técnicas de suavizado de bordes, entre otras. Estas modificaciones realizadas no pueden ser detectadas utilizando, simplemente, una técnica de análisis, debido a que no existe una técnica cien por ciento fiable, que permita obtener una conclusión definitiva para establecer la plena autenticidad o posible alteración de una imagen digital, por lo que es necesario acudir a la aplicación de dos o más de estas.

BIBLIOGRAFÍA

Aguirre Dobernak, N. (abril de 2013). *DETECCIÓN DE SEÑALES DE TRÁFICO MEDIANTE VISIÓN ARTIFICIAL BASADO EN FPGA.* Recuperado el marzo de 2021, de http://bibing.us.es/proyectos/abreproy/12112/fichero/Documento_por_capitulos%252F3_Cap%C3%ADtulo_3.pdf

Armas Vega, E., Sandoval Orozco, A., & García Villalba, L. (enero de 2020). *Detección de Manipulaciones Copy-Move en Ficheros Multimedia mediante la Transformada Discreta del Coseno.* doi:10.12804/si9789587844337.04

Bustamante Almaraz, A. (26 de septiembre de 2019). *PROCESAMIENTO DIGITAL DE IMÁGENES Ó TRATAMIENTO DE IMÁGENES.* Obtenido de https://www.youtube.com/watch?v=FuVjRuFSyCY

Cayetano, I. (15 de septiembre de 2020). *Introducción al procesamiento digital de imagen.* Obtenido de https://www.youtube.com/watch?v=Xnc5JQxWVys

DragonJar. (s.f.). FOCA - *Herramienta para análisis de Meta Datos.* Obtenido de https://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml

Fernandez, L. (09 de septiembre de 2020). *Procesamiento de imágenes.* Obtenido de Redes Zone: https://www.redeszone.net/tutoriales/seguridad/forensically-analisis-forense-fotos-online/

Forensically. (s.f.). *Forensically.* Obtenido de https://29a.ch/photo-forensics/#forensic-magnifier

Fotoforensic. (2021). *Tutorial: Error Level Analysis.* Obtenido de https://fotoforensics.com/tutorial-ela.php

Gutiérrez, J. (17 de noviembre de 2018). *FOCA: herramienta para encontrar metadatos en documentos.* Obtenido de Ciber Patrulla: https://ciberpatrulla.com/foca-metadatos/

Igual, J. (2019). *El ruido en fotografía digital: sensores y exposición.* Valencia, España: Universitat Politecnica de Valencia. Obtenido de: https://riunet.upv.es/bitstream/handle/10251/123415/Igual%20-%20El%20ruido%20en%20fotograf%C3%ADa%20digital%3A%20sensores%20y%20exposici%C3%B3n.pdf?sequence=1

Luengo Cabanillas, A. (16 de mayo de 2017). *Introducción al análisis forense de imágenes.* Obtenido de Luengo Cabanillas
:http://luengocabanillas.com/2017/05/16/introduccion-al-analisis-forense-de-imagenes/

Mendoza, M. A. (09 de diciembre de 2016). *Técnicas de análisis forense en imágenes digitales.* Obtenido de We Live Security: https://www.welivesecurity.com/la-es/2016/12/09/analisis-forense-imagenes-digitales/

Pelayo Gómez, S. D. (octubre de 2017). *DETECCION DE REGIONES CLONADAS EN IMAGENES DIGITALES.* Obtenido de http://bibliotecavirtual.dgb.umich.mx:8083/xmlui/bitstream/handle/DGB_UMICH/3532/FIE-M-2017-1681.pdf?sequence=1&isAllowed=y

Pereira, J. (06 de marzo de 2015). *Análisis forense de fotografías digitales*. Obtenido de Digital Heritage: http://www.jpereira.net/apuntes-breves/analisis-forense-de-fotografias-digitales

R. F, J. (18 de diciembre de 2017). *ELA (Error Level Analysis).* Obtenido de CRIMIBLOG: https://javier97rf.wordpress.com/2017/12/18/ela-error-level-analysis/

RAE. (s.f.). *Real Academia Española.* Obtenido de https://dle.rae.es/imagen

Rosales Corripio, J. (2013). *Algoritmo de Identificación de Fuente en Imágenes Digitales de Dispositivos Móviles.* Universidad Complutense de Madrid, España. Obtenido de https://core.ac.uk/download/pdf/19724201.pdf

Tecnica en Laboratorio. (s.f.). *Detección de Bordes.* Obtenido de http://www.tecnicaenlaboratorios.com/Nikon/Info_deteccion_de_bordes.htm

We are Social & Hootsuite. (11 de febrero de 2021). *Digital 2021*: Guatemala. Recuperado el abril de 2021, de https://datareportal.com/reports/digital-2021-guatemala