APLICACIÓN DE LA TÉCNICA ERROR LEVEL ANALYSIS Y METADATOS PARA EL ESTUDIO FORENSE DE IMÁGENES PRODUCIDAS POR DISPOSITIVOS MÓVILES

ANDRÉS ALBERTO ACEVEDO SOSA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2017

APLICACIÓN DE LA TÉCNICA ERROR LEVEL ANALYSIS Y METADATOS PARA EL ESTUDIO FORENSE DE IMÁGENES PRODUCIDAS POR DISPOSITIVOS MÓVILES

ANDRÉS ALBERTO ACEVEDO SOSA

Monografía para optar por el título de Especialista en Seguridad Informática

MSc. Alexander Larrahondo Nuñez
Director de proyecto
Especialista en Seguridad de Redes

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D. C. Abril 18 de 2017

Dedico esta investigación a mi familia que siempre me apoyaron en mi desarrollo intelectual

AGRADECIMIENTOS

Agradezco a mi familia por impulsarme a ser alguien en la vida, son el motivo por el cual me permite seguir adelante con todas mis metas propuestas. Siempre serán el motor que impulsa de forma imprescindible en cualquier circunstancia y son mi prioridad para seguir mi camino acompañado de la bendición de Dios que siempre me provee en cualquier situación por difícil que sea. Nunca me ha abandonado.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

La siguiente monografía propuesta por el autor con el fin de aplicar la técnica ELA en el estudio forense de imágenes producidas por dispositivos móviles el cual se plasmará el estudio de la imagen partiendo del tratamiento y origen de la misma, proveniente de un dispositivo portátil como lo es un celular. Además, se desarrollará la aplicabilidad de la técnica Error Level Analysis y los metadatos impuestos en una imagen con el fin de encontrar el origen donde fue tomada una imagen, como lo es la fecha, el modelo del dispositivo móvil, el tipo de formato y validación de alteraciones realizadas con el fin de encubrir algún tipo de delito y que este expuesto como prueba acusatoria.

Frente a la problemática planteada, se abordará el desarrollo de la investigación mediante el método científico, empezando por las generalidades del proceso de adquisición de una imagen y de todos los elementos que se involucran en la obtención de la misma, por lo tanto, se dará las correspondientes definiciones y teorías que se emplean en el desarrollo de la técnica planteada.

De acuerdo a lo anterior permitirá realizar el paso a paso de la aplicabilidad de la técnica ELA para realizar el respectivo tratamiento de una imagen, donde se parametrizará el proceso para predeterminar los pasos a seguir en un análisis forense.

PALABRAS CLAVE: Formato, Error, Metadatos, Modificación, Teléfono Móvil, Análisis.

INTRODUCCIÓN

El presente documento de investigación presenta la técnica de análisis de imágenes Error Level Analysis (ELA) y metadatos para el estudio y verificación de casos forenses el cual es necesario para hallar cualquier tipo de modificación o manipulación sobre imágenes, además de poder hallar la marca y fuente del dispositivo del cual fue tomada la fotografía, en este caso solo serán objeto de estudio aquellas imágenes cuya fuente es proveniente de cámaras integradas en dispositivos móviles, no importando su sistema operativo.

El primer problema al momento de realizar el correspondiente análisis a una imagen es que posiblemente los primeros datos de cabecera arrojen resultados erróneos ya que es posible que este tipo de información, llamados metadatos sean manipulados fácilmente alterando sus características iniciales. Es en ese momento donde la aplicación de la técnica ELA ayudara a presentar con claridad las modificaciones el cual fue sometida una imagen.

Este documento iniciara con un corto estudio acerca del procesamiento de las imágenes, se nombrarán las diversas herramientas usadas en el estudio del modo de compresión y formatos usados en los diversos dispositivos y mostrara el desarrollo de la técnica ELA para el análisis de imágenes modificadas.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad la adquisición de imágenes no solo proviene de cámaras fotográficas, a nivel tecnológico se ha avanzado tanto que hay gran variedad de dispositivos móviles con cámaras integradas con diferentes características y formatos. El fin de estos equipos es que siempre vamos a tener un dispositivo portátil de fácil uso para captar cualquier tipo de situaciones. Este tipo de eventualidades se pueden dar para uso delictivos como lo son la pornografía infantil, robo de información, secuestro, extorsión etc. según el problema o situación planteada en algún momento se van a tener imágenes como prueba acusatoria de cualquiera de los delitos mencionados, por lo que hace necesario la identificación del dispositivo que fue usado para cometer tal acto.

Es de gran importancia realizar el correspondiente análisis de dichas imágenes ya que estas son susceptibles a modificaciones, la razón es encontrar todo el historial que ha tenido, ya que pueden pasar por diferentes ediciones, retoques, cambio de tamaño en donde se convierten en un inconveniente al momento de realizar el análisis forense, cuyo objetivo es de confirmar la fuente y autenticidad de la misma. Al momento de iniciar un estudio forense en este caso con imágenes digitales, el primer problema que se encontrará es el hecho de que actualmente existen diversos programas que pueden ocultar la información como la fecha y marca del dispositivo sin que este deje algún rastro detectable el cual pueda convertirse como una prueba acusatoria invalida, por lo que debe ser analizado profundamente ya que mediante el estudio forense se pueden encontrar las diversas modificaciones que se ha realizado a la imagen digital para al final reconocer la verdadera naturaleza y manipulación y hacer la respectiva identificación del dispositivo que inicialmente realizó la toma de la imagen y así comprobar la veracidad y autenticidad.

Es por eso la importancia del uso de la técnica Error Level Analysis (ELA) ya que por medio de esta se comprobará que una imagen tiene modificaciones forzadas de la fuente origen y así poder comprobar la veracidad y autenticidad de la prueba acusatoria y continuar con el análisis de metadatos para hallar los verdaderos datos de cabecera de la imagen y poder llegar a los datos del dispositivo móvil del cual fue tomada dicha fotografía.

1.1. FORMULACIÓN DEL PROBLEMA

¿Cómo la aplicación de la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles es usada para determinar la fuente y originalidad de una imagen como prueba acusatoria?

2. JUSTIFICACIÓN

En la actualidad se está desarrollando continuamente la tecnología de obtención de imágenes, por lo que siempre se encontraran dispositivos móviles en donde los fabricantes integran una cámara digital para la obtención de la misma, con el fin de satisfacer a todos los usuarios que requieran de una en cualquier momento específico. Tal evolución en la tecnología puede ser impuesta por el mal manejo de aquellas personas malintencionadas que usan este recurso para actividades ilícitas es por eso la gran importancia de la aplicación de la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles es que por medio de esta contribuirá a un mejor análisis forense de las imágenes encontradas como pruebas acusatorias afirmando las modificaciones realizadas e identificando los verdaderos datos de la misma, como lo es el formato original, ubicación, modelo de la cámara y pixeles utilizados en la adquisición.

Por lo anterior la aplicabilidad de la técnica ELA facilitará el análisis de imágenes permitiendo identificar el nivel de error significativo en la sección de imagen con el fin de encontrar modificaciones de la misma y afirmar los diferentes cambios tales como la información de cabecera o marca del dispositivo del que fue tomada la imagen. Además dicho análisis para el estudio forense confirmará que un persona acusada por el incumplimiento de la ley 1273 o la ley 679 en donde se tenga imágenes incriminatorias relacionadas al cambio o modificación de la información, pornografía infantil o extorsión, en este caso puntual imágenes provenientes de móviles incurrirá a la violación de las leyes anteriormente mencionadas en cualquiera de sus artículos en donde la técnica ELA será concluyente confirmando que la imagen en cuestión producida por un dispositivo móvil determinado sufrió alteraciones para obtener algún tipo de beneficio. Por lo descrito anteriormente la ventaja de la aplicación de la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles ayuda a esclarecer cualquier inconveniente con cualquier tipo de imagen que haya sufrido cambios.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Aplicar la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles

3.2. OBJETIVOS ESPECÍFICOS

- Establecer el levantamiento de información y marco conceptual de la formación de imágenes producidas por dispositivos móviles y los diferentes formatos manejados en ello.

- Establecer la necesidad del estudio forense en dispositivos móviles y elementos que se encuentra involucrados en la adquisición y creación de imágenes

- Identificar los diversos procesos de tratamiento de imágenes y técnicas de análisis forense de imágenes

- Definir el algoritmo de la Error Level Analysis y pasos a seguir para la aplicabilidad de la misma

- Documentar la aplicación de la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles y aplicar dicha técnica para análisis de un banco de imágenes.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este proyecto estará enfocado y delimitado por la aplicación de la técnica error level analysis (ELA) el cual se excluye de la investigación otras técnicas usadas para el mismo fin, el estudio de imágenes. Además, se enfatizará en el estudio forense de las imágenes producidas por dispositivos móviles, en donde se pondrá en práctica la técnica ELA, por lo que se usará la información de los metadatos que son introducidos en las imágenes al momento de tomarlas como lo es la localización GPS, características de la imagen, etc.

Esta monografía está orientado a la investigación y desarrollo del tratamiento de las imágenes producidas por dispositivos móviles. Por lo que no se aplicará el estudio en alguna organización

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

Para la aplicación de la técnica ELA y metadatos para el estudio forense de imágenes producidas por dispositivos móviles se referencia los siguientes proyectos como elemento de la investigación para el desarrollo del proyecto:

- “Aplicación de la Técnica SVM en el Análisis Forense de Imágenes de Dispositivos Móviles” presentado por Sergio Aguado Rodríguez y Pedro Luis Antona Díaz en la ciudad de Madrid, España. Aplican la técnica de la máquina de soporte virtual para el análisis de imágenes.

- “Fotografía forense: uso de la fotografía digital en las escenas del crimen de delitos contra la vida” presentado por Ligia María Saquiché Sum en la ciudad de Guatemala de la asunción, Guatemala. Se analiza el uso de la fotografía digital en escenas de crimen.

- “Análisis forense de imágenes de móviles mediante el uso de metadatos” presentado por David Manuel Arenas González en la ciudad de Madrid, España. Estudio del tratamiento de las imágenes producidas por dispositivos móviles.

- “Diseño de una guía para la auditoría de análisis forense en dispositivos móviles basados en tecnología Android para legislación colombiana” presentado por Luz Stella Larrota Ardila, Jeimy Marcela Martinez Zabala y Viviana Francenet Orjuela López en la ciudad de Bogotá, Colombia. Guía para el análisis forense en dispositivos móviles el cual puede tener aplicabilidad en cualquier empresa que tenga un área de seguimiento informático con dispositivos móviles con Android

- “Metodología de análisis forense orientada a incidentes en dispositivos móviles” presentado por Diego Pinto en la ciudad de Sangolqui, Ecuador. Aplicación de técnicas de estudio forense en dispositivos móviles.

- “Técnicas de identificación de la fuente de adquisición en imágenes digitales de dispositivos móviles” presentado por David Manuel Arenas González en la ciudad de Madrid España. Análisis de diversas técnicas para el estudio de imágenes de dispositivos móviles.

5.2. MARCO TEÓRICO

Para conformar y poder aplicar la técnica ELA hace necesario realizar la correcta documentación y definir los siguientes conceptos para contemplar todo el tema:

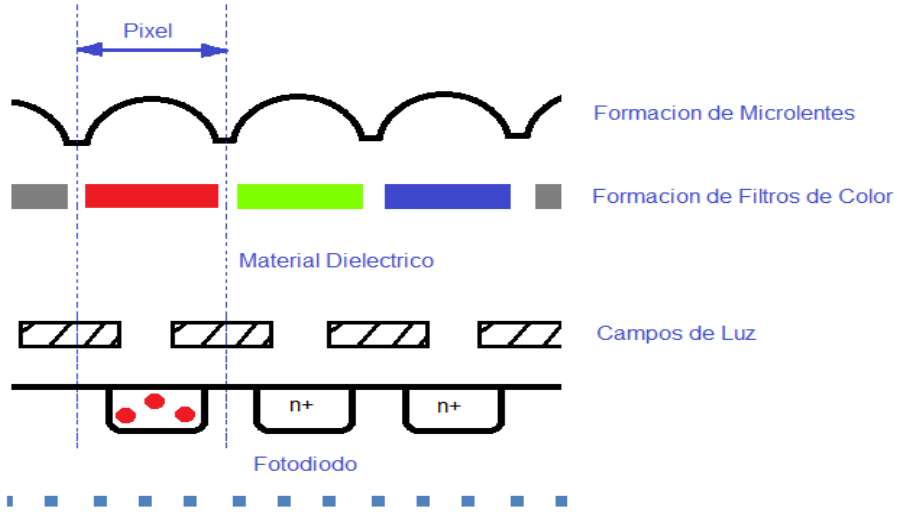
5.2.1. Proceso de adquisición de una imagen. Hace necesario describir el proceso de adquisición de imagen, ya que el medio en que se obtiene es el mismo proceso de una cámara fotográfica o en este caso un dispositivo móvil que será objeto de estudio más adelante.

La formación de imágenes digitales, mediante dispositivos como la cámara digital maneja un procesamiento interno el cual hace necesario describir, ya que por medio del entendimiento de dicho proceso hace posible el mejor entendimiento de la aplicación de la técnica Error Level Analysis.

En la actualidad existen dos clases de tecnologías para la obtención de imágenes digitales el cual son la CCD y CMOS

Al interior de una cámara digital se encuentra un transductor o sensor el cual es el encargado de convertir lo análogo “LUZ” en cargas eléctricas para su procesamiento

Figura 1.Sensor conversor de luz a cargas eléctricas



Fuente: http://www.chw.net/2011/05/captura-de-imagen-en-una-camara-digital-chwonders/

5.2.2. Transductor CCD. En la actualidad la mayoría de las cámaras digitales su funcionamiento está basado en el sensor CCD (*Charge Coupled Device*) o dispositivo de carga acoplada, dicho sensor es uno de los más comunes y usados en la imagen digital. Dicho sensor proporciona una buena calidad de imagen, pero el costo de su fabricación es muy elevado, por lo que los dispositivos que usan esta clase de sensor tienen un coste alto. Una de las desventajas al usar este sensor es que consume mucha energía. Su funcionamiento depende de un microdispositivo el cual se encarga de convertir las señales análogas a digitales, más comúnmente llamada ADC, el cual se encarga de convertir cada uno de los pixeles en datos digitales para que pueda ser leído desde cualquier terminal virtual o PC.

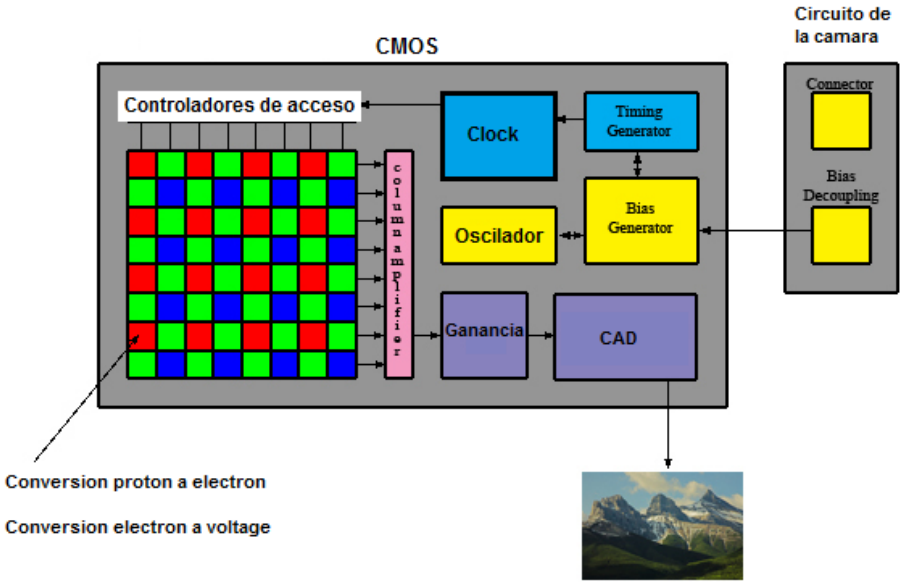
.Figura 2. Procesamiento del sensor CCD

Fuente: http://www.xatakafoto.com/camaras/sensores-con-tecnologia-ccd-vs-cmos

5.2.3. Transductor CMOS. Dicho sensor proporciona una baja calidad de imagen, el procesamiento de la imagen consiste en que dentro del sensor realiza la conversión de los pixeles a digital binarios no necesito de un circuito externo para realiza dicha conversión. Son más baratos de fabricar dicho sensor lleva en cada celda un transistor. Una de las desventajas al usar un sensor CMOS (*Complementary Metal Oxide Semiconductor*) es que a veces tienden a saturarse, es decir cuando el transistor recibe un haz de luz el pixel se puede saturar y este mismo satura a los que están al lado obteniendo una imagen de mala calidad. En la actualidad aún se está desarrollando esta tecnología ya que podría mejorar.

Como se muestra en la Figura 3. Cada celda es independiente y la diferencia principal es que la digitalización de los pixeles se realiza internamente.

Figura 3. Procesamiento del sensor CMOS



Fuente: http://www.xatakafoto.com/camaras/sensores-con-tecnologia-ccd-vs-cmos

5.2.4. Resolución. El detalle de la captura de la imagen es comúnmente llamado resolución la unidad de medida es dada en pixeles. Entre más pixeles tenga una imagen es mayor la calidad de la misma, es decir se podrán capturan con más detalle los colores característicos a la realidad.

En la tabla 1 se muestra en referencia la calidad de los pixeles, en donde se observa que a medida que aumentan, es mejor la calidad de imagen

Tabla 1. Referencia de Pixeles Vs Calidad

Pixeles	Observación
256x256	Se ven en las cámaras más baratas, esta resolución es tan baja que la calidad de la imagen es casi inaceptable. Son en total solo 65.000 pixeles
640x480	Esta es la gama baja en la mayoría de las cámaras de celular. Esta resolución es ideal para enviar mails o para publicar en sitios webs.

Tabla 1. (Continuación)

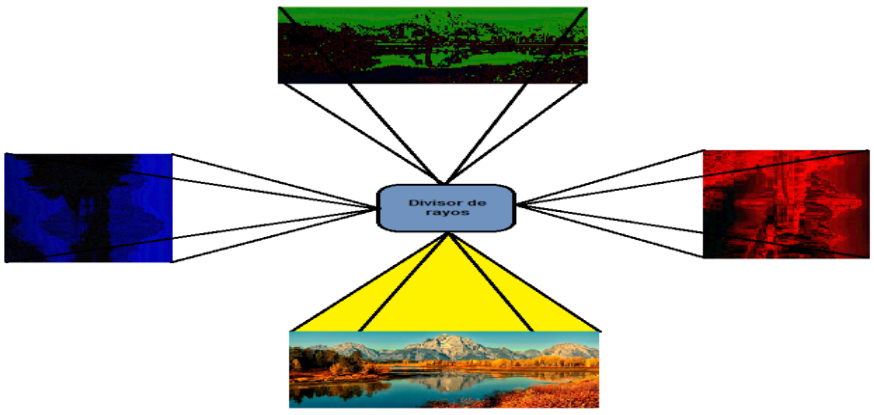
Pixeles	Observación
1216x912	Esto es 1 megapíxel, que equivale a un total de 1.109.000 pixeles es una calidad decente para imprimir.
1600x1200	Con casi 2 millones de pixeles, esto ya se considera alta resolución. Con esto ya puedes imprimir una foto de 4x5 pulgadas obteniendo una calidad similar a la de un laboratorio fotográfico.
2240x1680	Aquí ya podemos obtener una buena calidad para fotos de 16x20 pulgadas, es una resolución de 4 megapíxeles.
4064x2704	Estos son 11.1 megapíxeles y ya se encuentra en la gran mayoría de las cámaras en el mercado.

Fuente: http://www.chw.net/2011/05/captura-de-imagen-en-una-camara-digital-chwonders/

5.2.5. Captura del color. Existen varios métodos de para capturar el color por medio de una cámara digital los cuales se procederán a describir:

1. El primer método es usado por cámaras de gama alta, el cual consiste en usar tres filtros RGB (Red*, Green, Blue*) en donde el sensor ya sea CCD o CMOS recibe el haz de luz y este haz es dividido en forma igual por un “divisor de Luz” en donde los tres filtros reciben la misma imagen, pixel por pixel. Es decir, cada filtro u sensor recibe la misma imagen con la diferencia del color. este proceso es usado por cámaras grandes y de un coste más alto.

Figura 4. Captura de color por divisor de luz



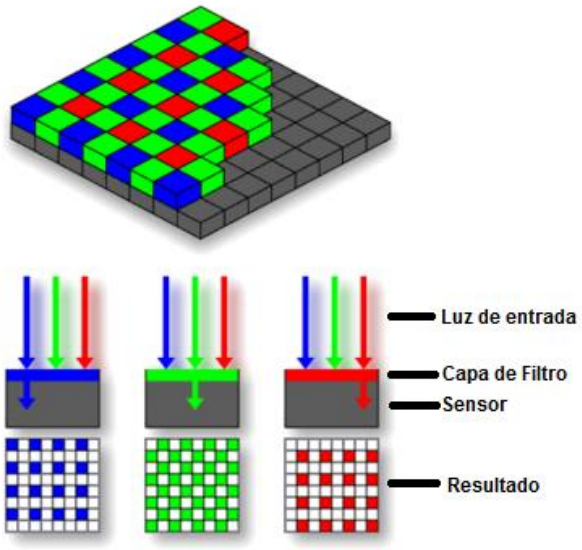
Fuente: Autor

2. El segundo método de captura de color consiste en tener los tres filtros y secuencialmente se rotan por el mismo haz de luz de tal forma que todos los filtros tengan la imagen pixel por pixel. Este método tiene una gran desventaja ya que para sacar una imagen optima, el objeto debe mantenerse inmóvil mientras se realiza la captura.

3. El método más usado practico y económico es el de la interpolación ya que consiste en agregarle al sensor de luz una matriz de filtrado RGB el cual al momento de percibirse un pixel este es dividido en colores Rojos, verdes y Azules en donde es posible realizar una mejor codificación y predicción del verdadero color.

Dicho patrón se llama Bayer el cual consiste en que al momento de entrar el haz de luz esta es alternado entre las filas verdes y rojas y filas de verdes y azules de tal manera que se obtendrá el reflejo de una imagen con tres colores. A la imagen obtenida se le conoce como RAW por lo que es una muestra de pixeles rojos, verdes y azules en diferentes intensidades. El tratamiento de la imagen depende del procesador de la cámara el cual se encargará por medio de un algoritmo de realizar el “des mosaico” para convertir una imagen con colores reales muy parecido al original.

Figura 5. Tratamiento de la imagen con el patrón Bayer

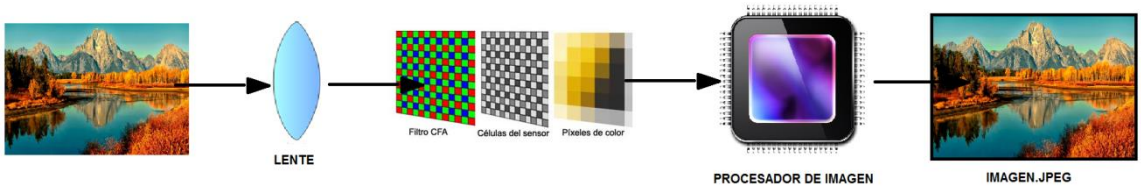


Fuente: Pentax K-3 II. http://pentaxclick.blogspot.com.co/2015/04/pentax-k-3-ii.html

En la actualidad se utiliza este método ya que difiere en costos de los dispositivos, resulta más económico, práctico y con buena calidad en las imágenes.

En resumen, la adquisición de una imagen pasa por varios procesos, en donde primero se debe calcular físicamente la distancia de la toma de imagen, apretar el obturador, luego la cámara digital o el dispositivo expone el sensor CCD a la luz, luego la imagen pasa por los diferentes celdas de filtros RGB, después la imagen pasa por el procesador del dispositivo el cual es tratado para reconstrucción de la imagen realizando algún algoritmo para dar al final lo requerido, una imagen con colores apropiados. El dispositivo puede utilizar varios mecanismos de compresión, pero el más utilizado es del JPEG el cual finalmente la imagen es almacenada en la memoria interna del dispositivo.

Figura 6. Proceso de adquisición de una imagen



Fuente: El Autor

5.2.6. Compresión de imágenes. La compresión de imágenes va directamente ligada a la adquisición de la misma ya que hace necesario transformar o trasladar la imagen en formato de compresión el cual es imprescindible para el tratamiento posterior de la misma. El tratamiento de compresión de una imagen puede ser comprendida en dos clases:

a. Compresión sin pérdida de información.
b. Compresión con pérdida de información.

Dicha compresión es el conjunto de técnicas aplicadas para el almacenamiento y la transmisión es por eso la importancia de este tema, ya que se usan técnicas de compresión digital. “Es el proceso de reducción del volumen de datos para representar una determinada cantidad de información” [1]

Algunas imágenes pueden ser tratadas con técnicas de compresión sin pérdida de información como lo son las imágenes de tratamientos médicos o las imágenes de pruebas acusatorias. Como objetivo se identifican tres tipos o formas de representación de imágenes, como lo son la eliminación del código redundante, eliminación de pixeles redundantes y eliminación de redundancia visual.

[1] González R, W. R. (2008). *Tratamiento digital de imágenes.* USA: Addison-Wesley.

5.2.7. Formatos de imágenes. Existen varios formatos que representan las imágenes el cual la finalidad es almacenarla y transmitirla a continuación se presenta un cuadro descriptivo de los formatos más utilizados.

Tabla 2. Tipo de formatos de imagen

Tipo de fichero	Observación
TIFF	Es el de mayor calidad el cual es usado por las cámaras digitales, se recomienda usar este formato para cualquier modificación
JPG	Es el formato más elegido ya que tiene una excelente calidad de compresión. No es recomendable para hacer modificaciones ya que acumula errores, este es un método de compresión con pérdidas.
GIF	Es un formato de 256 colores. No es recomendable su uso para cámaras fotográficas ya que solo usa 256 colores, por lo tanto, la calidad de imagen sería mala.
PNG	Es un formato de compresión ideal ya que trababa con el método de compresión sin perdidas. Es capaz de almacenar 16 millones de colores.

Fuente: http://alojamientos.us.es/gtocoma/pid/pid6/pid61.htm

5.2.8. Codificación de imágenes. de dos dimensiones o bidimensional el cual se encuentra involucrado la intensidad de la luz y un punto cualquiera, donde dicha función es proporcional a la luz por lo tanto hace posible expresarla de la siguiente manera:

$$Imagen\ digital = f(x, y) \qquad (1)$$

el cual la hace discreta en coordinadas espaciales, proporcional al brillo de la misma, por lo tanto, una imagen se hace vectorial ya que estas se componen por contornos y rellenos definidos por lo tanto se permiten que sean escalables[2]

para la obtención de cualquier color, se realiza a partir de una mezcla entre los colores básicos como lo es el rojo, verde y azul, por lo que a través de estas combinaciones se pueden completar los espacios de baja luminosidad de las imágenes, mediante diferentes bases matemáticas. El espacio más conocido es el

[2] (Grimados, Tratamiento digital de imágenes, s.f.)

espacio RGB. Los componentes son codificados cada uno con 8 bits el cual arrojan un total de 24 bits por pixel donde es el formato básico de cualquier dispositivo móvil o cámara. la idea es la de usar la compresión de una señal obteniendo cualquier tipo de ahorro como lo es en las luminancias y crominancias, esto es debido a que, si se controla el nivel de crominancias, el ojo humano no podrá percibir este tipo de niveles por lo que es más sensible a las luminancias por lo que la imagen podrá obtenerse en un modo de compresión sencilla. Por esta razón la mayoría de los dispositivos manejan un estilo de compresión estándar por lo que es usado en el espacio de colores desde el formato básico RGB a otro formato[3].Es posible realizar una conversión de color dentro de los espacios vectoriales con el fin de controlar las luminancias y la crominancia de una imagen mediante una diferencia sencilla. Las fórmulas de conversiones son las siguientes:

Nivel de brillo o luminancia

$$Y = 0.3R + 0.6G + 0.1\text{s} \tag{2}$$

Diferencia de color azul, Cb

$$U = B - Y \tag{3}$$

Diferencia de color rojo, Cr

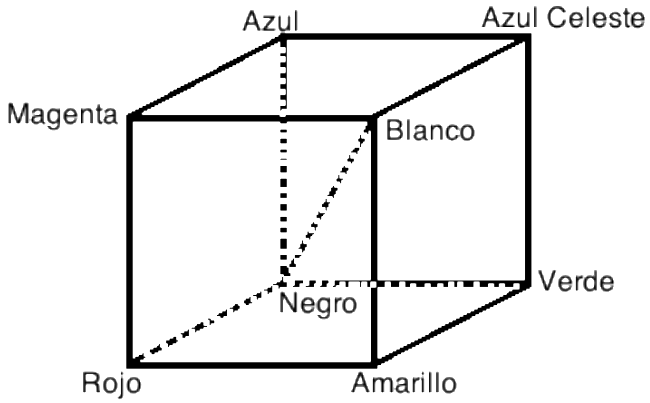
$$V = R - Y \tag{4}$$

Donde U y V son la crominancia

Lo anterior es el formato de la recomendación CCIR 601, las ecuaciones representan los espacios de colores para su representación digital, por lo tanto, la resultante es una matriz espacial, donde el resultado esta codificado en espacios de 8 bits resultantes. A continuación, se representa el sistema RGB en espacio, para la combinación y sumarización de los colores resultantes en forma vectorial.

Figura 7. Sistema RGB

[3] P. A. C. Castillo, Codificación y transmisión robusta de señales de vídeo MEPG-2 de caudal variable sobre redes de transmisión asíncrona ATM[, Valencia: Ediciones de la Universidad Castilla - La Mancha, 1999.



Fuente: Autor

5.2.9. Técnicas de compresión de imágenes. El tratamiento de una imagen es necesario ya que todas ellas al venir de un medio análogo y convertirlas a un medio digital se crean muchas redundancias, la cual a través de las técnicas de compresión de imágenes se eliminan aquellos bits redundantes que al momento de quitarlos no altera la imagen misma. Lo anterior indica que se puede dividir en dos grupos: la primera en técnicas de compresión con pérdidas de información y la segunda técnicas de compresión sin perdidas de información. En la segunda las imágenes que estén comprimidas se regeneran igual a la original sin omitir las redundancias[4], la cual es usada para procesos médicos en donde se necesitan todas las características de la imagen, por ende, según técnica de compresión no será objeto de estudio en esta investigación.

5.2.9.1. Técnicas de compresión de imágenes con pérdida de información. Dicha técnica la imagen reconstruida no es igual a la original, por lo que es empleado normalmente por los dispositivos móviles con el fin de no ocupar espacio dentro del disco duro interno, para la comodidad del usuario. Esto se emplea cuando las imágenes tienen bits redundantes donde pueden ser eliminados para que la imagen no quede con información susceptible a cambios[5]. A continuación, se nombrarán las técnicas más usadas de decodificación basados en la fuente.

[4] M. T. L. Bonal, Notas de visión y apuntes sobre ingeniería del software, Albacete: Ediciones Universidad Castilla la Mancha, pp. 83-95.
[5] M. Fernandez, «Harvard,» [En línea]. Available: http://lmi.bwh.harvard.edu/papers/pdfs/2003/martin-fernandezCOURSE03f.pdf.

5.2.9.2. Codificación por transformación. En la codificación por transformación, se usa la transformada de Fourier discreta en donde es caracterizada por una transformada lineal lo cual por medio de esta hace en cierto modo corresponder la imagen en compresión con el conjunto de coeficientes par o impar de la transformada en donde después del proceso se cuantifican y se hace codificable. Tal método es efectivo ya que a partir de una imagen natural el cual en ella se puede encontrar cualquier cantidad de bits redundantes bien sea de forma significativas en donde serán dados con un coeficiente y serán eliminados sin tener efecto alguno sobre el resultado de la imagen. No dispone de una distorsión de la imagen significativa. La siguiente ecuación describe la transformada discreta con sus correspondientes coeficientes (Imagen, s.f.).

$$T(u,v) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) g(x,y,u,v) \tag{5}$$

donde $T(u,v)$ es la transformada de $f(x,y)$;

$g(x,y,u,v)$ es el núcleo de la transformación directa;

u y v toman valores de 0 a $N-1$.

Análogamente, la transformada inversa se expresa como:

$$f(u,v) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} T(x,y) h(x,y,u,v) \tag{6}$$

Donde $h(x,y,u,v)$ es el núcleo de la transformación inversa.

5.2.10. Vector de cuantización. El vector de cuantización trata de agrupar en vectores aquellos bits redundantes el cual son formados en una matriz vectorial donde se debe realizar una serie de pasos para realizar la cuantización para reordénalos en una nueva matriz, a continuación, se enumeran pasos a seguir para realizar el vector de cuantización[6]:

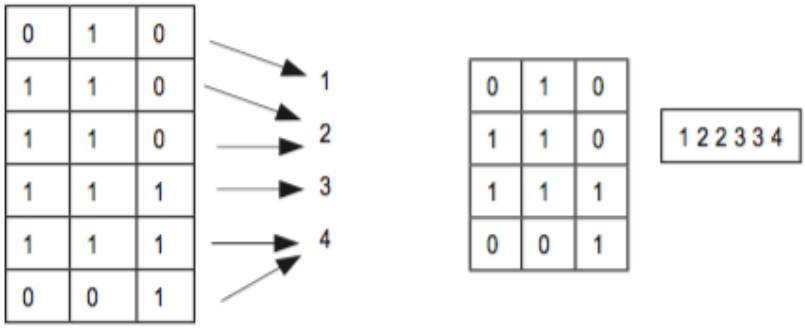
1. Para la construcción de la cuantización principalmente la imagen se debe dividir en partes fijas el cual son llamados vectores de iniciación.

[6] A. L. Franco. [En línea]. Available: http://www.sav.us.es/formaciononline/asignaturas/asigpid/apartados/textos/recursos/codificadorvq03/presenta.ppt.

2. En un bloque se debe construir una nueva tabla en donde están asignados aquellos valores diferentes a los redundantes en donde son hallados en la imagen original.
3. Los datos de la tabla anterior se deben transferir al vector de iniciación para poder realizar una comparación bit a bit de cada uno de los subespacios vectoriales creados, con el fin de formar un paralelo entre los bits y poder diferenciarlos entre sí. Aquellos datos iguales se podrán eliminar de la matriz vectorial obteniendo una reducción significante de datos dentro de la imagen.

Se obtendrá una serie de índices el cual se clasificarán para poder formar la imagen final, tal como se muestra en la Figura 8

Figura 8. Codificación por cuantización



Fuente: Autor

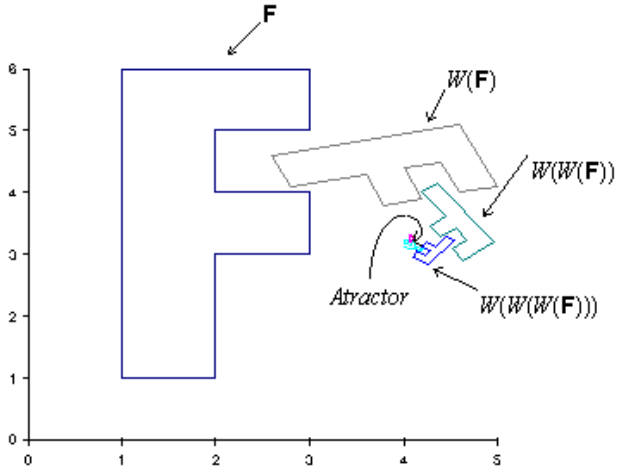
Esta técnica puede ser usada para un conjunto de imágenes, en donde la tabla de vectorización se convierte de forma dinámica, cabe decir que este tipo de método es usado en algoritmos para su simplicidad.

5.2.11. Compresión fractal. Un fractal es la respuesta a la medición de aquellos elementos que no pueden ser expresados en la geometría normal u euclidiana, por lo tanto, es una forma de modelo matemático para describir aquellas formas como lo son las nubes, las montañas, hojas, arboles, copos de nieve, etc. El método de la compresión fractal es comúnmente usado en la fotografía digital ya que la función especial de este método es usar la transformación, por lo que consiste en un sistema de identificación de un “frame” por sectores de la imagen el cual son asignados a coeficientes limitados, tal algoritmo encuentra similitudes entre los coeficientes por lo que hace es duplicarlos cuantas veces sea necesario encontrando un patrón de imagen.

La compresión fractal está basado en un tipo referente de transformación lineal, este tipo de transformaciones son llamadas contractivas por lo que a medida que se realiza la transformación esta siempre va a ser más pequeña que la

transformación original, en la figura 9, se muestra que a medida que se toma una transformación contractiva, la toma de la imagen será más pequeña que la anterior.

Figura 9. Transformaciones contractivas sucesivas



Fuente: http://sabia.tic.udc.es/gc/Contenidos%20adicionales/trabajos/Imagenyvideo/compresion%20fractal/trabajo.html

En resumen, la base de la compresión fractal comprende en iterar o repetir las transformaciones almacenadas en las regiones hasta formar una imagen definida, este modelo matemático es llamado SFI (Sistemas de Funciones Iteradas)[7]

$$W = \bigcup_{i=1}^{n} W_i \qquad (7)$$

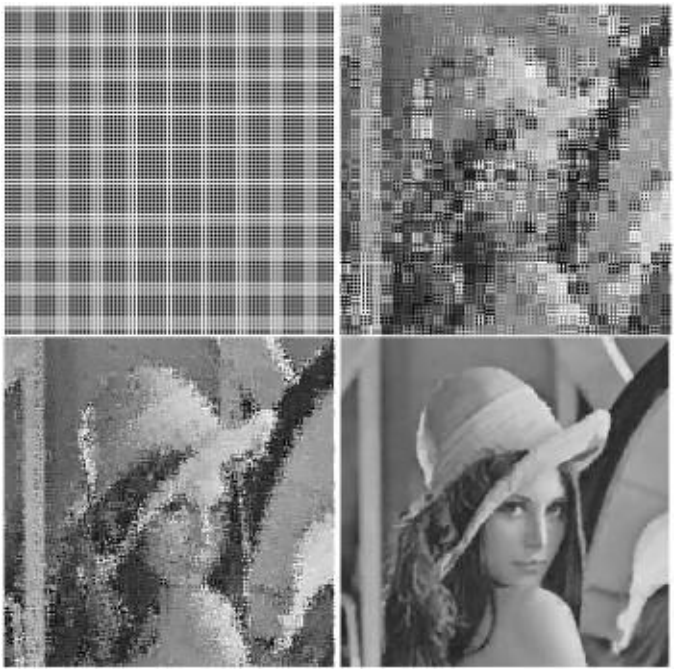
El proceso de compresión es el siguiente:

- La imagen original se procede a dividir en subregiones de dominio, en donde se buscarán redundancias de bit.
- Para cada subregión de dominio, se escoge una subregión de rango, el cual es mayor tamaño que la de dominio.
- A todas las subregiones se les aplica rotación en todos los grados, se le conoce como transformación contractiva.
- La transformación a fin encontrada en cada una de las transformaciones contractivas, se almacenan en un fichero llamado fractal el cual constituyen la descompresión para así reconstruir y definir la imagen.

A continuación, un ejemplo de la compresión fractal

[7] J. L. Rodriguez, «Compresion Fractal de Imagenes,» [En línea]. Available: http://sabia.tic.udc.es/gc/Contenidos%20adicionales/trabajos/Imagenyvideo/compresion%20fractal/trabajo.html .

Figura 10. Compresión fractal



Fuente: http://sabia.tic.udc.es/gc/Contenidos%20adicionales/trabajos/Imagenyvideo/compresion%20fractal/trabajo.html

5.2.11.1. Eficacia de la compresión fractal. Para medir la eficacia del método de compresión fractal, basta con usar la razón matemática, llamada argumento de Barnsley, el cual mide la eficacia de la compresión:

razón = núm. de bytes imagen sin comprimir/núm. de bytes imagen comprimida

dicha eficacia se debe calcular cada vez que se utilice el modelo SFI, con el fin de determinar si la imagen descomprimida es parecida a la original.

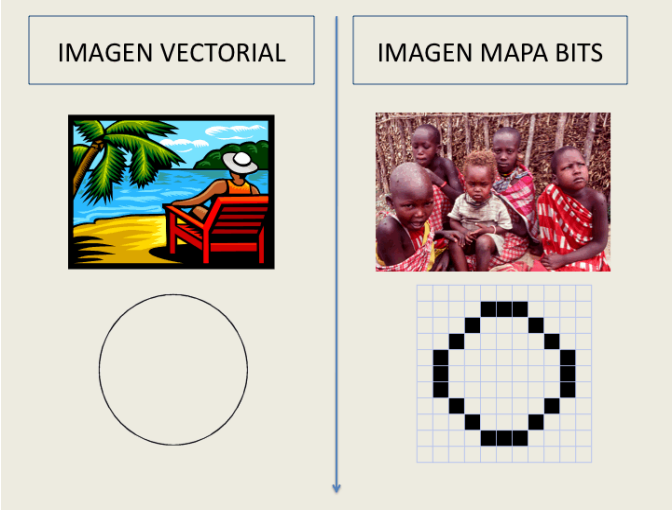
5.3. FORMATOS DE ARCHIVO DE IMAGEN, USADO EN EL MÉTODO ERROR LEVEL ANALYSIS (ELA)

Para la aplicación de la técnica ELA para el estudio de imágenes producidas por dispositivos móviles es de gran importancia recalcar que el estudio de aplicabilidad va ser en el formato JPEG ya que dicho formato es el más utilizado por los dispositivos móviles. Para iniciar el estudio de dicho formato se empezará por indicar que todas las imágenes parten de dos categorías que son básicas como lo es el mapa de bits "Bitmap" o vectores[8].

Un mapa de bit, comprende de un pixel de imagen el cual se convierte en un mapa de bit y un vector es un conjunto de bits asignados a vectores, el cual es representado por fórmulas matemáticas, con el fin de no afectar a la imagen final, este tipo de archivos vectoriales son de gran calidad para no perder resolución en la imagen

Los mapas de bit, generalmente se usa en imágenes o fotografías de fotos reales, mientras que las imágenes de vector son usadas en el diseño y composición gráfico[9].

Figura 11. Mapa de bits vs Vectores



Fuente: https://creagrafico.wordpress.com/2010/02/05/illustrator-y-la-imagen-vectorial/

[8] F. H. [En línea]. Available: http://fotoforensics.com/tutorial-ela.php.
[9] C. p. D. grafico, «Crea grafico,» [En línea]. Available: https://creagrafico.wordpress.com/2010/02/05/illustrator-y-la-imagen-vectorial/.

5.3.1. Formatos JPEG (Joint Photographic Experts Group). Es un formato estándar el cual surge por la necesidad de comprimir imágenes para ser compartidas a través de internet por lo que el grupo Joint Photographic Expert Group realizó el estándar y que muchos fabricantes de dispositivos móviles la adoptaron. Actualmente cualquier dispositivo, usa el formato JPEG con el fin de ser compatibles en cualquier circunstancia. El formato JPEG es usado comúnmente para la fotografía de escenas reales en donde permite en cierto modo nivelar la compresión o ajustarla al requerimiento de cada uno de los usuarios, por lo tanto, el método de compresión JPEG realiza la compresión en tres etapas, en donde se describen a continuación[10]:

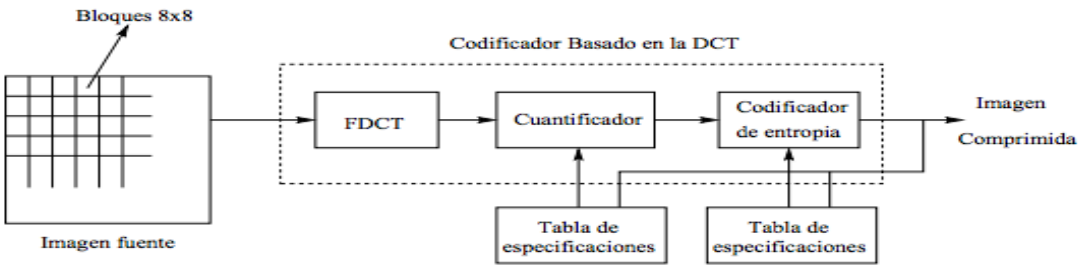
Etapa 1: Preparación de la imagen

- Una vez tomada la imagen, esta se prepara en el espacio RGB y el espacio YUV (Luminancia y Crominancia).
- Se utiliza el método de compresión fractal, realizando submuestreo para obtener archivos más pequeños que el original.
- La imagen se divide en tramas o bloques de 8x8 pixeles.

Etapa 2: Codificación fuente, codificación con perdidas

- A la imagen ya subdividida en bloques se aplica el momento de compresión por transformada discreta a cada trama de 8x8 pixeles por lo cual se obtiene un dominio de frecuencia, esto es nombrado matriz de coeficientes.
- La sumarización y/o cuantificación de cada uno de los coeficientes de cada uno de los vectores 8x8 es dividido por una constante y el resultado se redondea a una forma entera. Por último, se eliminan los coeficientes restantes para terminar con la compresión.

A continuación, se muestra la secuencia de pasos que sigue el método JPEG.
Figura 12. Secuencia de pasos método JPEG



Fuente: http://lmi.bwh.harvard.edu/papers/pdfs/2003/martin-fernandezCOURSE03c.pdf

[10] M. Martín, «Estandar JPEG,» [En línea]. Available: http://lmi.bwh.harvard.edu/papers/pdfs/2003/martin-fernandezCOURSE03c.pdf.

Etapa 3: Preparación de la imagen

- Se aplica la codificación de los diferentes elementos de un Frame 8x8, para agrupar los componentes nulos.
- Se aplica el método de compresión Huffman para comprimir más información y así completar el modelo JPEG.

5.4. MARCO CONCEPTUAL

Las variables de la temática propuesta en este caso la aplicación de la técnica ELA y metadatos para el estudio forense de imágenes producidas por dispositivos móviles y las que están implícitas en el proceso son la investigación de adquisición de una imagen por medio de dispositivos móviles comprobando la autenticidad de la misma aplicando la técnica ELA y comprobar el origen de la imagen es decir identificar el dispositivo del cual fue tomada la evidencia.

Es razón por la cual se debe desarrollar un algoritmo de estudio forense el cual permita identificar cualquier tipo de modificación en las imágenes de ahí la gran importancia de la técnica Error Level Analysis ya que se pretende desarrollar un patrón que sirva para identificar modificaciones u alteraciones de cualquier tipo permitiendo conocer y dar un diagnóstico claro respecto al estudio forense de la mismo confirmando la originalidad de esta.Para comprobar y conocer el origen de una imagen como lo es la marca del dispositivo, ubicación, modelo, entre otras. Lo que se parte del uso y desarrollo de un algoritmo forense para identificación de las características descritas anteriormente. Dichas características se diferencian en base a la imagen en evidencia el cual se llevará a un uso estadístico que determinará el modelo del dispositivo. Este proceso se llevará a cabo en el transcurso del desarrollo del proyecto en donde se verá la objetividad de la resultante misma.

5.5. MARCO LEGAL

El proyecto debe ser aplicado para el cumplimiento de las siguientes leyes ya que es la aplicación de una técnica forense para el estudio de imágenes como prueba acusatoria de diferentes hechos.

5.5.1. Modificación de evidencias

Ley 1273 del 2009[11]

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

[11] Tomado de: Ley 1273 del 2009 disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la

transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen:

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

5.5.2. Pornografía infantil

LEY 679 DE 2001

ARTÍCULO 1o. OBJETO. Esta ley tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio, y la expedición de otras disposiciones en desarrollo del artículo 44 de la Constitución[12]*.*

[12] Tomado de: Ley 679 de 2001 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18309

LEY 1236 DE 2008[13]

CAPITULO IV

Del Proxenetismo

"Artículo 218. Pornografía con menores. El que fotografíe, filme, venda, compre, exhiba o de cualquier manera comercialice material pornográfico en el que participen menores de edad, incurrirá en prisión de diez (10) a catorce (14) años y multa de ciento treinta y tres (133) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima. Para efectos de determinar los miembros o integrantes de la familia habrá de aplicarse lo dispuesto por el artículo 35 y siguientes del Código Civil relacionados con el parentesco y los diferentes grados de consanguinidad, afinidad y civil"

"Artículo 219-A. Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores. El que utilice o facilite el correo tradicional, las redes globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con estos, incurrirá en pena de prisión de diez (10) a catorce (14) años, y multa de sesenta y seis (66) a setecientos cincuenta (750) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad (1/2) cuando las conductas se realizaren con menores de catorce (14) años".

5.5.3. Extorsión

Artículo 244. Extorsión[14]. Extorsión. Artículo modificado por el artículo 5 de la Ley 733 de 2002. Penas aumentadas por el artículo 14 de la Ley 890 de 2004, a partir del 1o. de enero de 2005. El que constriña a otro a hacer, tolerar u omitir alguna cosa, con el propósito de obtener provecho ilícito o cualquier utilidad ilícita o beneficio ilícito, para sí o para un tercero, incurrirá en prisión de ciento noventa y dos (192) a doscientos ochenta y ocho (288) meses y multa de ochocientos (800) a mil ochocientos (1.800) salarios mínimos legales mensuales vigentes.

[13] Tomado de: Ley 1236 de 2008 Nivel Nacional disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31612

[14] Artículo 244 del Código Penal disponible en: http://tituloviipenalespecialuno.blogspot.com.co/2013/04/articulo-244-extorsion_17.html

6. MARCO METODOLÓGICO

Para establecer el desarrollo de proyecto ya que es la aplicación de una nueva técnica de análisis forense se basará en el método científico, en donde se iniciará por la investigación descriptiva, luego exploratoria y por último explicativa.

Sobre el tipo de investigación, Canales (1996)[15] señala:
"Hay diferentes tipos de investigación, los cuales se clasifican según distintos criterios..." (p. 53). Los diferentes tipos de investigación relacionados por el autor son de gran importancia para dar de manera adecuada el desarrollo del proyecto

Investigación Descriptiva:

Se establece este tipo de investigación, ya que se requiere en principio realizar una culturización de la adquisición de una imagen y el algoritmo con la cual trabajan las cámaras digitales que en la actualidad se encuentran incorporadas en los dispositivos móviles.

Investigación Exploratoria:

Es realmente importante este tipo de investigación ya que por medio de este se complementará el marco teórico ya que definirá y establecerá el concepto de la técnica Error Level Analysis para encontrar modificaciones sobre imágenes expuestas como prueba o evidencia en algún caso donde se infrinja las leyes mencionadas en el marco legal

Investigación Explicativa:

Hace necesario finalizar el proyecto con este tipo de investigación ya que por medio de esta se aplicará la técnica ELA y metadatos para el estudio forense de imágenes producidas por dispositivos móviles, explicara detalladamente el uso de la misma y las diferentes herramientas que intervienen en el proceso.

6.1. METODOLOGÍA DE DESARROLLO

Para el establecimiento de la aplicación de la técnica ELA y metadatos hace necesario realizar el cumplimiento de las siguientes etapas dentro del proyecto para realizar una correcta documentación de la misma y un correcto desarrollo de la aplicabilidad de la técnica propuesta, a continuación, se proponen las siguientes etapas:

[15] Ceron, M. C. (2006). *Metodologias de investigacion social.* chile: LOM Ediciones.

Etapa 1: levantamiento de mapa de procesos

Para la realización de la primera etapa hace necesario realizar una investigación exhaustiva a cerca de los métodos de algoritmos usados en el análisis forense, de tal modo permitirá el establecimiento del mapa de procesos para la aplicabilidad de la técnica ELA. Para regir el desarrollo de la primera etapa hace necesario aplicar los siguientes ítems:

- Identificación de aplicabilidad del algoritmo usado en la técnica ELA
- Identificación de los principales metadatos usados en las imágenes producidas por dispositivos móviles.
- Establecimiento de la herramienta a usar para la aplicación de la técnica ELA.

Etapa 2: Análisis de la información

En esta etapa se realizará el respectivo análisis de la información del mapa de procesos. Está implícito el desarrollo de cada uno de los ítems mencionados ya que el análisis de cada uno de estos llevará la importancia del proyecto, lo que llevara a conclusiones importantes dentro del mismo proceso que se llevará a cabo para la aplicación de la técnica.

El análisis de las imágenes se llevará a cabo con la aplicación de Error Level Analysis para encontrar las modificaciones sobre las imágenes en este caso producidas por dispositivos móviles, por lo que se analizara solo un formato JPEG ya que es el más común producido por los móviles y que tiene ser un parámetro con mayor modificación.

- Características del formato JPEG
- Herramientas para verificación de modificaciones
- Análisis de metadatos en una imagen JPEG

Etapa 3: Aplicabilidad de la técnica ELA

Es la etapa principal del desarrollo del proyecto ya que en esta se tendrán en cuenta diferentes imágenes producidas de diferentes dispositivos móviles, para la aplicabilidad de la técnica ELA y distinción de los metadatos producidos en cada una de las imágenes producidas por los dispositivos móviles. Esto permitirá realizar un análisis estadístico del análisis de las imágenes. Esta etapa permitirá la correcta documentación del paso a paso de la aplicación de la técnica Error Level Analysis.

- Desarrollo del banco de imágenes
- Aplicación estadística del análisis ELA sacado del banco de imágenes

Etapa 4: Conclusiones

En la etapa final del proyecto se mostrará las principales conclusiones del proyecto realizado.

7. DESARROLLO DEL PROYECTO

7.1. ALGORITMO FUENTE DE LA TÉCNICA ELA Y METADATOS

Para el desarrollo y la aplicabilidad de la técnica hace necesario identificar el algoritmo de funcionabilidad de la misma, ya que por medio de ella permitirá la identificación de las modificaciones realizadas en la imagen, es por ello que se debe identificas las diferentes distinciones entre una imagen tomada desde un dispositivo móvil y una imagen cuya fuente es proveniente de un scanner, ya que por medio de esta distinción hace posible la continuidad de la aplicación de ELA ya que una imagen escaneada deja por fuera la utilidad de la técnica puesto que el objeto de esta es el estudio de imágenes con orígenes de dispositivos móviles.

7.2. DESCRIPCIÓN PARA IDENTIFICACIÓN DE LA IMAGEN FUENTE

Para la identificación de una imagen escaneada a la de una imagen de fuente un dispositivo móvil, es la aplicabilidad de la detección de ruido[16]. La técnica ELA influye específicamente en el estudio de imágenes con formato de compresión JPEG ya que este es el formato que es manejado casi universalmente por cualquier dispositivo móvil. Para fines de comprensión el estudio de identificación de la imagen fuente está llevada claramente por una imagen original es cual se denominará "S", una imagen con ruido "S_{ruido}" y una imagen sin ruido "$S_{\sin ruido}$" en donde la ecuación 8 describe la solución para la obtención de una imagen con ruido.

$$S_{ruido} = S - S_{\sin ruido} \qquad (8)$$

El resultado es la imagen original con ruido descompuesta en los 3 componentes RGB, el cual dará el ruido en cada uno de los 3 componentes de colores. En forma concluyente el ruido de una imagen escaneada debe ser uniforme con respecto a una imagen proveniente de un dispositivo móvil ya que el ruido no es uniforme. Se pueden evaluar las similitudes de ambas imágenes pen tal caso de que a simple vista no se identifique cual sea la fuente de la imagen, el cual es buscar la correlación de la misma este cálculo permitirá la identificación de la fuente en filas y columnas de la imagen aprovechando de que la imagen escaneada utiliza un patrón lineal ya en X o en Y el cual dependerá de la posición en que es colocada la imagen en el dispositivo versus el patrón matricial de una cámara de un dispositivo móvil el cual varia la distribución del ruido en el subespacio vectorial, la ecuación 9 describe lo anterior.

[16] EZQUEDA, José. Fundamentos de procesamientos de imágenes. Baja California: Editorial Universitaria, 2005. P16

$$Correlacion\ (X,Y) = \frac{(X-\overline{X})\cdot(Y-\overline{Y})}{\|X-\overline{X}\|\cdot\|Y-\overline{Y}\|} \quad (9)$$

La ecuación anterior describe el sometimiento de la imagen en formato matricial en caso de que por el primer método denominado en la ecuación 8 no permite la diferenciación de la imagen como fuente original de un dispositivo móvil.

7.3. COMPROBACIÓN DE AUTENTICIDAD DE LA IMAGEN

Una vez identificada la imagen de dispositivo móvil hace necesario hacer una comprobación exhaustiva que compruebe que la imagen es original, es decir que no tenga modificaciones o manipulaciones realizadas por algún tercero. Esta etapa es la más importante porque es donde se usa la técnica ELA para validación y comprobación de modificaciones en el objeto de estudio de este análisis de autenticidad se tendrán respuestas definitivas que permitirán concluir si es necesario seguir con la identificación del dispositivo móvil o no, ya que al no ser autentica, se desvalida las pruebas.

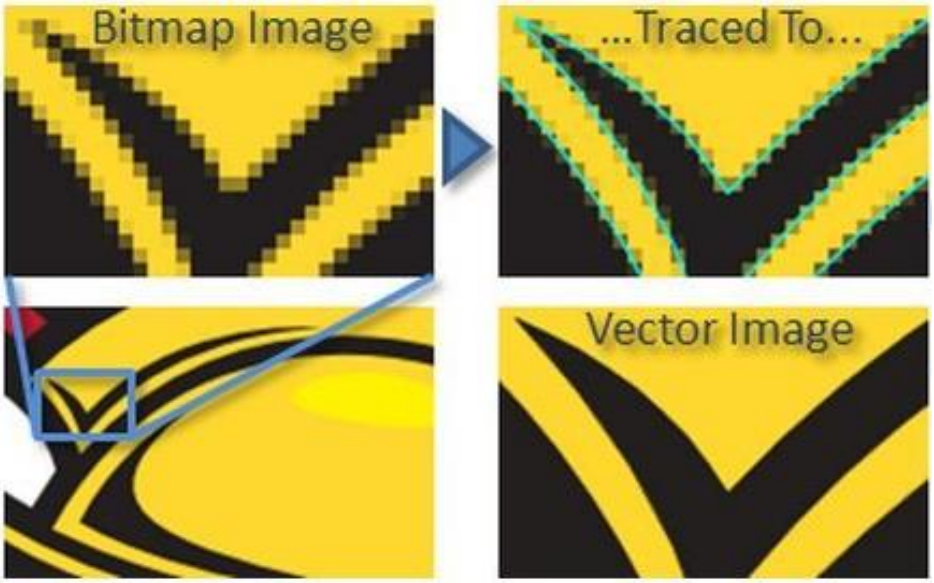
El análisis de nivel de error estudia las características de color, el procesamiento, la saturación en donde muestra indicios de modificación y cambio en las características de la imagen, esto hace necesario saber cada uno de las características del color como lo es:

7.3.1. Valor medio de los pixeles. Representa el valor medido de los pixeles totales de una imagen al momento de clasificarse por cada uno de los componentes RGB, con el fin de obtener un color resultante que en este caso es el gris, esto sucede con la condición de que la imagen tenga suficientes valores medios en las variaciones de color.

7.3.2. Perturbaciones de las imágenes. Las perturbaciones es el parámetro que más se analiza, ya que por medio de estos es posible identificar franjas, ruido, interferencias o alteraciones en los tonos de las imágenes ayuda a identificar el ruido original de la imagen del ruido que tienen las alteraciones realizada en ella. Las perturbaciones más encontradas son el aliasing y la pixelación.

7.3.3. Pixelación y contorneado. Tanto la pixelación como el contorneado pertenecen a las perturbaciones de una imagen cada uno infiere en que la imagen no tiene resolución e insuficiencia del mismo para cada uno de ellos correspondiente a la definición y tonalidad de una imagen. Esta característica es bastante importante en la técnica ELA ya que por lo general son sobresaliente en el estudio de una imagen digital, son las perturbaciones y la pixelación que más sobresalen en una modificación, en la figura 12 se muestra un ejemplo de lo indicado anteriormente.

Figura 13. Pixelación y contorneado



Fuente: http://vectormagic.com/home

7.4. DEFINICIÓN DE LA TÉCNICA ELA (ERROR LEVEL ANALYSIS)

ELA es una técnica bastante útil para encontrar o detectar manipulación en las imágenes el cual son elementos de investigación, dicha técnica trabaja con la compresión de una imagen del 95% y esta misma evalúa la terminación de la misma partiendo de la figura original, por lo tanto se identifican las diferentes áreas modificadas el cual serán vistos con facilidad debido a los aspectos de caracterización de ELA.

ELA usa varios métodos para identificación de las modificaciones el cual sus principales son:

Sombras: Análisis de las diferentes sombras que tiene una imagen digital el cual son relacionados a objetos diferente de la imagen a analizar y la correspondiente evaluación de ellos en relación de la luz fuente.

Ojos: la evaluación y diferenciación del color en los ojos, la reflexión de la luz sobre la imagen para permitir encontrar puntos negros en los ojos, el resultado debe ser una forma oscura o sombra para descartar alguna modificación.

EXIF: Análisis de los metadatos tipo Exif en donde se incluye posicionamiento global GPS, zonas horarias e informa RGB, la variación de estos datos depende del fabricante del dispositivo móvil.

Reflexiones: validación de la reflexión en la imagen debe ser coherente, si la persona que realiza alguna modificación en la imagen y no tuvo en cuenta la coherencia de la reflexión en la figura, este análisis indicará las modificaciones realizadas

7.4.1. Compresión de la imagen usado en ELA. Cada imagen del ordenador se compone de píxeles hechas de tres colores: rojo, verde y azul (RGB). El valor de color de un píxel se representa con un byte (0-255). El mapeador (también conocido como decodificador) modifica el espacio de color RGB al espacio de color YCbCr, Y es la luminiscencia, Cb y Cr son las porciones de color de crominancia-azul-rojo y crominancia. En el espacio de color YCbCr, la mayor parte de los datos de la imagen se encuentra disponible en el componente Y, Cb y Cr tienen información de color.

Figura 14. Representación YCbCr

Fuente: https://msdn.microsoft.com/enus/library/windows/desktop/dn424131(v=vs.85).aspx

El mapeador divide las imágenes en una red de sub-imagen de 8X8, mientras que JPEG siempre se codifica en luminancia con una cuadrícula de 8X8. La crominancia puede ser codificado usando 8X8, 8X16, 16X8, o 16X16. Para la visualización, el decodificador JPEG convierte la imagen de YCbCr a RGB.

7.4.2. Principio de ELA. Error Level Analysis evalúa el nivel de calidad de la red de cuadrados dentro de las imágenes. Presentan un mayor grado de error durante las operaciones sucesivas volver a guardar. El fenómeno es evidente si las imágenes no están optimizadas para un nivel de calidad de la cámara especificada. Por lo tanto, esta vuelve a guardar los recuadros posteriores que reducen el Error Level potencial ni, produciendo una ELA de imagen más oscura. Después de una serie se vuelve a guardar, la cuadrícula alcanza su nivel mínimo error.

7.5. CARACTERÍSTICAS PARA IDENTIFICACIÓN DE LA MARCA Y MODELO

Este punto es importante para el algoritmo ya que por medio de esta se puede extraer las características para la identificación de la marca y modelo del dispositivo móvil el cual fue la fuente para la producción de la imagen objeto de estudio. Para el desarrollo de este hace necesario el estudio de los metadatos el cual el dispositivo

móvil introduce en la imagen en donde es un proceso sencillo con el único punto débil es que los metadatos dependen del fabricante del dispositivo estos datos son los más sensibles ya que pueden ser adulterados por personas malintencionadas para lograr algún objetivo. Es importante recalcar que el proceso de identificación del dispositivo móvil se realiza si y solo si, la imagen de objeto de estudio pasa el análisis de la técnica ELA para la detección de modificaciones en una imagen.

Las características presentes en una imagen tomada de un dispositivo móvil, se observa en la determinación de colores RGB lo cual se llamará el procesamiento del color, en donde se destacan las siguientes características:

- **Correlación RGB**

Es una medida que se expresa en la distancia de las barras de colores RGB, en donde dependiendo las características del dispositivo móvil, estas se modifican, matemáticamente hablando una de las formas para medir dicha correlación es usando el método de coeficientes de Pearson para confirmar la correlación existente de cada una de las bandas.

- **Distribución vectorial del centro de masa**

Es la medida el cual es calculada para cada una de las bandas RGB por separado el cual resultan 256 componentes por cada banda calculada es decir la suma de los pixeles, una vez calculado la vectorización, se suman los vecinos resultantes en un vector i o j por lo tanto para cada uno de los valores vectoriales se le suma o se resta $j+1, j-1$ y como resultante de estas sumas se calcula por último el centro de masa, en donde el total debe ser una valor en el rango de 0 a 255 componentes. Son 3 características que difieren del fabricante.

- **Corrección entre pares RGB**

Es el proceso de corrección que tiene el dispositivo móvil para quitar ruido a la imagen de forma automática, el cual difiere de la marca del dispositivo. Esto se puede representar independientemente para cada una de las bandas RGB.

$$A_1 = \frac{|G|^2}{|B|^2} \; ; \; A_2 = \frac{|G|^2}{|R|^2} \; ; \; A_3 = \frac{|B|^2}{|R|^2} \tag{10}$$

Existen varios métodos para el tratamiento de la imagen para encontrar las características necesarias para la identificación de la marca y modelo como lo son el estudio de lentes en aberración, validación de imperfecciones en el sensor de la cámara, técnica de la interpolación de matriz en banda de colores, la correlación de Pearson, entre otros. La razón de esta monografía no es describir todos los métodos, solo son nombrados para partir de la relación de hay otros métodos para sacar las características esenciales. Para el desarrollo de la identificación del dispositivo móvil se va usar el método de metadatos en la imagen.

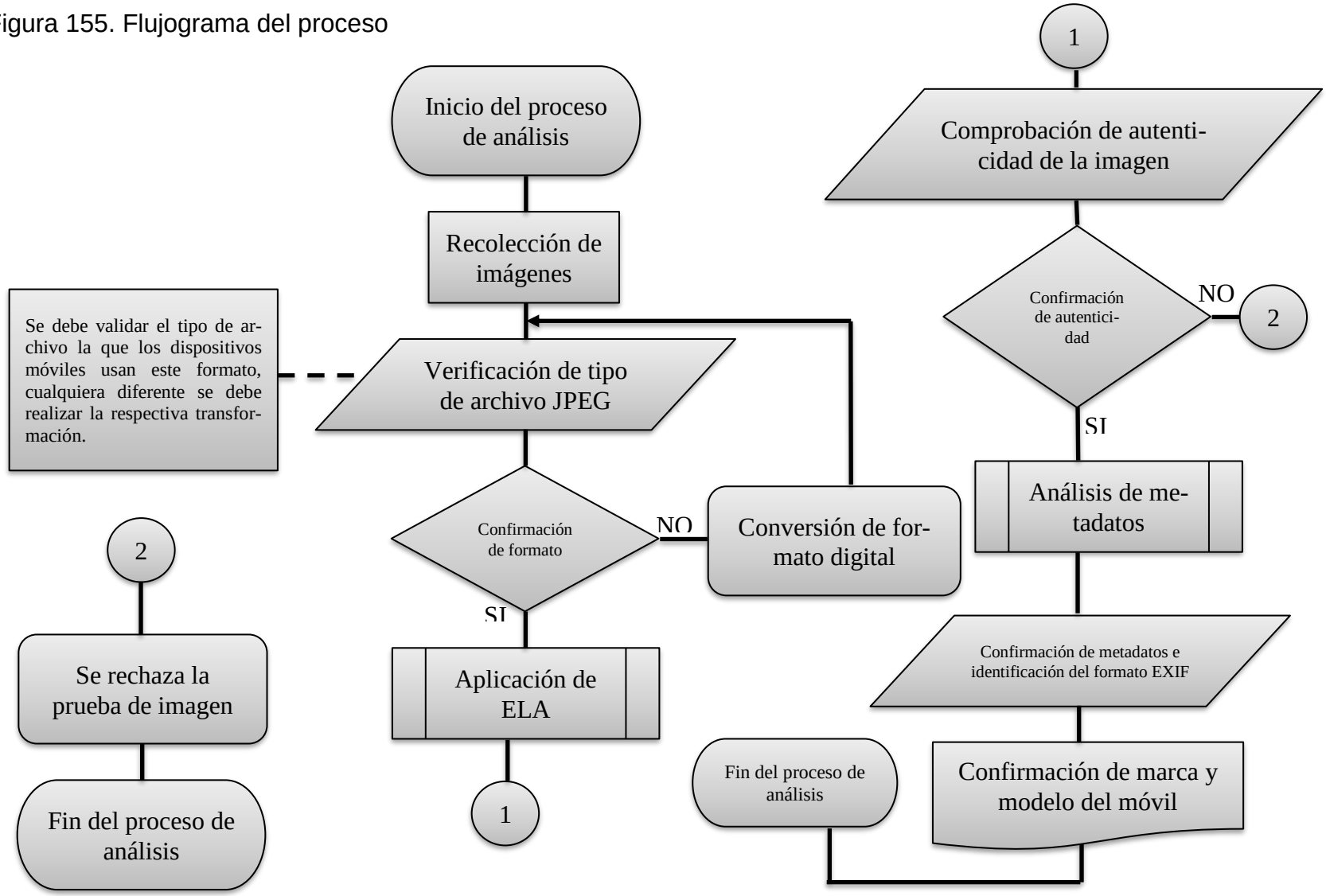
7.5.1. Método de los metadatos. Los metadatos son aquellos datos que son introducidos por los fabricantes en los dispositivos móviles, vienen al momento de realizar una toma fotográfica, existen varios tipos de metadatos, por ejemplo, la fecha y hora, tamaño, resolución, etc. Este tipo de datos varia por parte del fabricante. La desventaja de los metadatos es que son sensibles a la modificación, es decir que si alguien tiene algunas pretensiones diferentes a la sociedad, puede realizar modificaciones de estos datos introduciendo información errónea y borrándolos, para no dejar evidencia cabe recalcar que los metadatos no se ven a simple vista, basta el uso de algún software especial que realice la identificación de este tipo de archivos que se encuentran ocultos.

Para el desarrollo de este análisis se basara en el metadato principal EXIF (Exchangeable image file format) el cual todos los fabricantes de dispositivos móviles se basan en este metadato introductorio ya que tiene las etiquetas “make” y “model” uno que dirá la marca y el otro el modelo respectivamente del dispositivo si se obtienen estas etiquetas se dirá que se tiene el cien por ciento de confirmación de del dispositivo móvil, partiendo de que no se ha realizado alguna modificación malintencionada, es por eso que establece la técnica ELA, con el fin de identificar las modificaciones y adulteraciones realizadas en una imagen.

7.6. FLUJOGRAMA DEL PROCESO

A continuación, se definirá el flujograma del proceso para la aplicación de la técnica ELA y metadatos para el estudio forense de imágenes producidas por dispositivos móviles, el cual por medio de esta dará un mejor entendimiento del proceso que debe llevar una imagen digital donde es presentada en algún proceso como elemento probatorio.

Figura 155. Flujograma del proceso



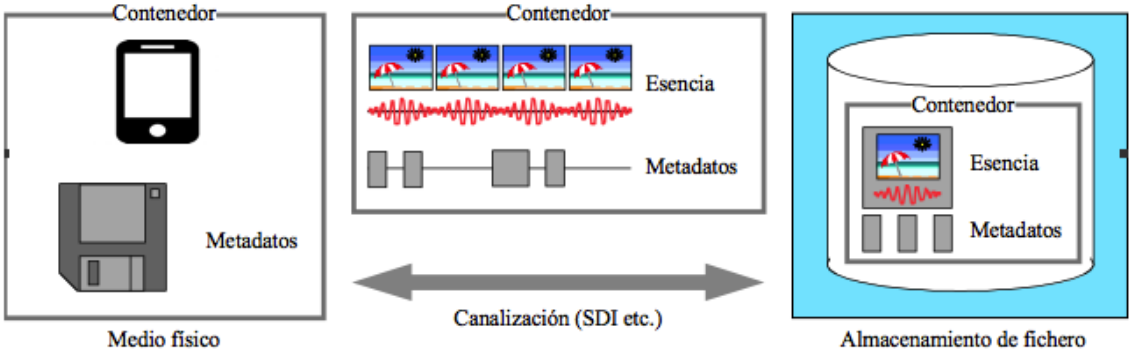
Fuente: Autor

8. LOS METADATOS

Son llamados así porque son datos que están dentro de otros datos, el cual dicha información viene compartida, en este caso son las imágenes. Este tipo de archivos vienen ocultos dentro de las imágenes con el fin de guardar información, tales como la ubicación, el fabricante, el modelo para dejar una marca en ella en caso de ser necesitarse.

A través de los dispositivos móviles se realiza la captura de una imagen digital en donde mientras no se le haga alguna modificación mantendrá sus metadatos, por lo general existen varias extensiones para salvaguardar los metadatos dentro de una imagen como lo son JPG, TIFF, PNG, PGF, MIFF, HDP, PSP en donde cada uno de estos formatos tienen estándares y normas para establecer metadatos dentro de los contenedores el cual dentro de ellos se realiza la organización de los datos referentes a un dispositivos para la identificación de las piezas de la información para así realizar una búsqueda puntual al momento de usarlas

Figura 16. Representación esquemática de los contenedores



Fuente: https://www.itu.int/dms_pubrec/itu-r/.../R-REC-BR.1357-0-199802-W!!MSW-S.doc

El contenido en la cual se representan los metadatos tiene en si una forma que estos elementos se encuentran codificados siempre tendrán un bloque de contenido el cual es una colección de metadatos en un bloque y un paquete de contenido en donde están relacionados un conjunto de imágenes digitales. Algunos de estos metadatos pueden ser cambiados para diferentes fines, pero las únicas personas que realizan cambios en este tipo de archivos es porque están realizando algo fuera de la ley que no quieren que alguien conozca datos de indicios para poder encontrar a esa persona. Por más diferentes que sean los formatos, todos comparten un archivo principal el cual es comúnmente llamado “copyright” el cual son cadenas que son guardados por varios contenedores de metadatos. Lo anteriormente descrito es una

problemática para los fabricantes principales ya que produce desconfianza al momento de realizar una imagen y que esta se puede modificar sus metadatos, por lo que esta creado una sociedad para tratar de mitigar estos hechos llamada “Metadata working Group”, pero aun así la existencia de los metadatos es de gran ayuda para diferentes procesos para reconocimientos de lugares u hechos.

Para un mayor entendimiento de los metadatos hace necesario realizar el estudio de algunos de los formatos que se usan para el manejo de los mismos.

8.1. EXIF (EXCHANGEABLE IMAGE FILE FORMAT)

Es un estándar el cual fue creado para guardar metadatos en imágenes digitales, fue creado por la Japan Electronic Industry Development Association en octubre de 1995, los datos EXIF contienen información propia de la imagen en donde son incrustados como fichero en la imagen digital por lo que en cierto modo se podrá saber los datos del dispositivo el dónde fue tomada la imagen. La información que por lo general indica el fichero son las siguiente:

- Información del dispositivo móvil (marca, modelo, firmware)
- Parámetros de apertura
- Medición de luz
- Características de fecha
- Características comunes del dispositivo como nombre del propietario

Figura 17. Metadatos de una imagen

Image		
Image description		Descripcion de la imagen (editable)
Artist		Artista (editable)
Copyright		Información del copyright (editable)
Exposure time	1/1600 s	Tiempo de obturación
F-number	f/5	Apertura de diafragma
Exposure program	Aperture priority	Modo de disparo (Av)
ISO speed ratings	100	Sensibilidad
Date/time original	07/04/2007 14:42:17	Fecha y hora del disparo
Exposure bias value	0.00 EV	Nivel de exposición
Metering mode	Pattern	Método de medición de luz (matricial)
Flash	Flash did not fire, compulsory flash mode	Flash
Focal length	50 mm	Distancia focal
User comment		
Colorspace	sRGB	Espacio de color
Pixel X dimension	3888	Ancho de la imagen
Pixel Y dimension	2592	Alto de la imagen
White balance	Manual white balance	Ajuste de blancos
Scene capture type	Standard	Modo del disparo (estandar)

Fuente: http://www.thewebfoto.com/2-hacer-fotos/218-datos-exif

La especificación EXIF, ha lanzado varias versiones, pero la última versión que actualmente se está usando, fue lanzada en abril del 2010 la versión 2.3, los dispositivos móviles y cámara usan el formato JPEG, en donde cabe recalcar que este formato es que se debe definir en proceso de identificación de la imagen.

8.1.1. Estructura del formato JPEG. Dentro de la estructura del formato JPEG, se encuentra dos ficheros el cual son los denominados EXIF y JFIF. Este tipo de ficheros son fáciles de identificar ya que se diferencian por el uso de cuarto bit que identifica que fichero se está usando además el uso de los bits en el rango del 6 al 11 el cual especifica el código ASCII. Como se ha dicho con anterioridad el formato EXIF está creado para guardar las características de la imagen y el formato JFIF es más usado para la edición de las imágenes digitales es donde están guardados los datos de copyright. En la tabla 4 se muestra la asignación de bits para cada uno de los formatos y su traducción en hexadecimal.

Tabla 3. Bytes de identificación del formato JPEG

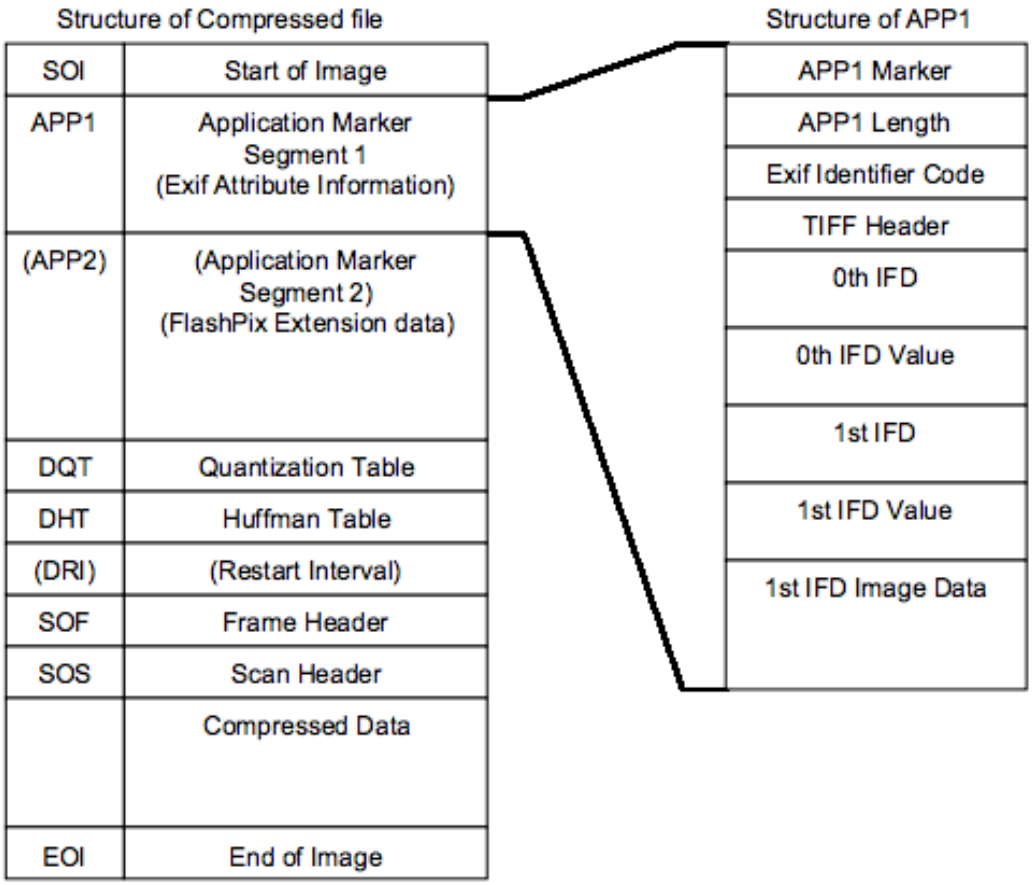
	JFIF	*EXIF*
Posición	Bytes	Bytes
0	FF	FF
1	D8	D8
2	FF	FF
3	E0	E1

Fuente: http://searchsoa.techtarget.com/definition/JPEG

La estructura para el fichero JFIF, no hace necesario implementarla ya que no se realizará el enfoque en este tipo de fichero.

La estructuración de la compresión del formato JPEG, según la versión 2.3 está dada por el formato ISO/IEC 1918-1, en donde la conversión empieza con los ficheros en el segmento de aplicaciones (APP1), en donde esta es aplicada en el segmento SOI (Start Of Image) indicando el inicio del archivo (ver figura 18) precedida del APP2 como aplicación del segmento, esto sucede después de establecer la aplicación del segmento 1 APP1. Los demás ficheros que se involucran en esta compresión no se incluye el formato EXIF, el cual se encuentra ubicado en el fichero APP1. La Interoperabilidad del APP1 consiste en el marcador APP1, el código de identificación Exif, y la información de atributos en sí.

Figura 18. Estructura básica de compresión del formato



Fuente: http://jmbigas.blogspot.com.co/2011/09/editores-fotograficos-gimp-y-datos-exif.html

El tamaño del fichero APP1 incluyendo todos esos elementos no deberá superar los 64 Kbyte especificados en el estándar JPEG. La información de los atributos se almacena en la estructura de TIFF que incluye un encabezado de archivo, con un máximo de dos, los registros IFD atribuyen la información relativa a la imagen comprimida (imagen principal). El primero de los IFD se puede utilizar para grabar una imagen en miniatura.

APP2 consiste en el marcador APP2, FPXR (Flashpix Ready) código de identificación, y la lista de contenidos para la extensión de Flashpix de grabación, o flujo de datos. Una cadena de múltiples segmentos marcadores APP2 se puede utilizar para registrar datos superiores a 64 Kbyte.

8.1.2. Datos thumbnail. Este tipo de datos se encuentran en la APP1 de compresión del formato JPEG, el cual son imágenes en miniatura de manera similar a las imágenes primarias, utilizando dos formatos de imagen existentes.

Para este tipo de imágenes no hay límite sobre el tamaño de las imágenes en miniatura más sin embargo no son obligatorias, pero se recomienda que sea registrado de ser posible, a menos que el hardware, el mismo dispositivo u otras restricciones se opongan a esto.

datos thumbnail no necesariamente tienen que adoptar la misma estructura de datos que el utilizado para las imágenes primarias. sin embargo, las imágenes primarias se registran como datos RGB sin comprimir o datos YCbCr como no comprimido,

los thumbnail no se pueden grabar como datos comprimidos JPEG (ver Tabla 4).

Tabla 4. combinaciones de imágenes primarias y estructuras de datos en miniatura

		Imagen Primaria	
		Sin compresión	Compresión
Thumbnail	Sin compresión	Posible	Posible
	Compresión	No es posible	Posible

Fuente: http://jmbigas.blogspot.com.co/2011/09/editores-fotograficos-gimp-y-datos-exif.html

Cuando los thumbnail se graban en formato sin comprimir, que deben ser registradas en el 1er IFD en conformidad con la línea de base TIFF Rev. 6.0 Imágenes RGB a todo color o TIFF Rev. 6.0 Imágenes Extensiones YCbCr.

8.1.3. Especificaciones Exif-ifd. EXIF IFD es un conjunto de etiquetas de registro de información Exif-específico como atributo. Se apunta el desplazamiento desde el TIFF cabecera (valor Offset) en donde indica un valor de etiqueta privada EXIF. A continuación, en la tabla 5 se muestra un ejemplo de etiqueta EXIF-IFD el cual muestra un registro de la imagen.

Tabla 5. Especificación EXIF-IFD

Exif IFD Pointer	
Tag	34665 (8769.H)
Type	LONG
Count	1
Default	none

Fuente: http://www.exif.org/Exif2-2.PDF

8.1.4. Gps ifd. GPS IFD es un conjunto de etiquetas de información de registro GPS. Se apunta el desplazamiento desde la cabecera TIFF (valor Offset) indicado por un valor de etiqueta privada GPS.

Tabla 6. Especificación GPS IFD

GPS Info IFD Pointer	
Tag	34853 (8825.H)
Type	LONG
Count	1
Default	none

Fuente: http://www.exif.org/Exif2-2.PDF

8.1.5. Interoperabilidad del apuntador IFD. Interoperabilidad IFD se compone de etiquetas que almacena la información para garantizar la interoperabilidad y señalado por la siguiente etiqueta situada en Exif IFD.

Tabla 7. Interoperabilidad IFD

GPS Info IFD Pointer	
Tag	40965 (A005.H)
Type	LONG
Count	1
Default	none

Fuente: http://www.exif.org/Exif2-2.PDF

La estructura de Interoperabilidad de Interoperabilidad IFD es la misma que define TIFF estructura IFD, pero no contiene los datos de imagen característicamente en comparación con IFD TIFF normal.

8.1.6. Datetime. La fecha y hora de creación de la imagen. En esta norma indica la fecha y hora del archivo. En donde se muestra el formato como "AAAA: MM: DD HH: MM: SS" con el tiempo se muestra en formato de 24 horas, y la fecha y hora separados por un carácter en blanco [20.H]. Cuando se desconoce la fecha y la hora, todos los espacios de caracteres, excepto dos puntos (":") pueden rellenarse con caracteres en blanco, o de lo contrario el campo de interoperabilidad pueden rellenarse con caracteres en blanco. La longitud de cadena de caracteres es de 20 bytes, incluyendo NULL para la terminación. Cuando el campo se deja en blanco, se trata como desconocido. Cabe recalcar que este es un metadato sensible al cambio cualquier modificación en el entorno de la imagen guardaría una fecha diferente a la establecida originalmente.

Tabla 8. Fecha y Hora

GPS Info IFD Pointer	
Tag	306 (132.H)
Type	ASCII
Count	1
Default	none

Fuente: http://www.exif.org/Exif2-2.PDF

8.1.7. Modelo. Es el nombre del modelo del dispositivo móvil. El cual también puede ser el modelo de serie de un escáner, digitalizador de vídeo u otro equipo que genera imágenes. Cuando el campo se deja en blanco, se trata como desconocido.

9. HERRAMIENTAS PARA APLICACIÓN DE ELA Y METADATOS

Para la aplicabilidad de la técnica y realizando seguimiento del proceso del algoritmo hace necesario definir el software que se usará para validación de las modificaciones en las imágenes por medio del Error Level Analysis y extracción de los metadatos EXIF en una imagen a analizar.

Para el análisis de la técnica ELA se usará el software GIMP (software libre) en su versión 2.8 para Ubuntu para encontrar modificaciones realizadas en las imágenes, además se realizará las respectivas comparaciones con los softwares WEB para confirmar la efectividad de las modificaciones encontradas como lo es fotoforensics o Forensically.

Para el estudio de los metadatos se utilizará el entorno virtual Linux EXIFTOOL el cual está diseñado para los metadatos EXIF y el análisis de los mismos además soporta varias extensiones de imágenes, es una herramienta de software libre.

9.1. GIMP 2.8 (UBUNTU)

GIMP es un programa libre de licencia gratuita el cual proviene del proyecto GNU que significa (GNU Image Manipulation Program), el cual es usado para realizar modificaciones en imágenes, realizar retoques, edición de imágenes, cambiar tamaño de imágenes, formatos y otras tareas. Se escoge este software ya que permite la instalación de plugins, mediante la programación de código Python.Con el uso de esta herramienta se puede realizar la verificación de error level analysis en imágenes de formato JPEG, en donde el objetivo de este es encontrar si una fotografía tiene alguna clase de modificación.

9.2. FOTOFORENSICS

Es una herramienta de uso web creada para el análisis de imágenes para encontrar anomalías en ellas. Dicha herramienta encuentra metadatos, saturación y errores en imágenes digitales, además tiene la forma de realizar ELA en imágenes directamente encontrando las modificaciones realizadas.

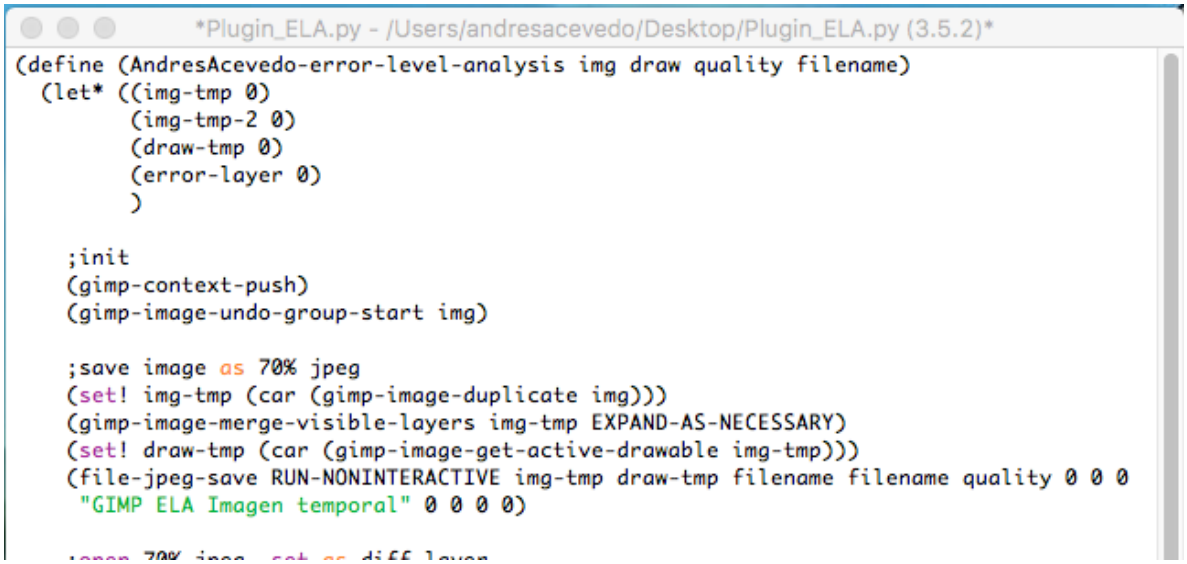
9.3. EXIFTOOL

Es una herramienta multiplaforma, el cual para el análisis de las imágenes se usará la instalación en Ubuntu. Es una herramienta usada para tratar, validar y editar metadatos de las imágenes, en especial da una posibilidad de validación de los Exif en las imágenes con el fin de verificar que información se puede extraer de ella

10. IMPLEMENTACIÓN DEL ALGORITMO ELA

Para la implementación del algoritmo del método error level analysis se implementa un plugins desarrollado en Python con el fin de facilitar el análisis de las modificaciones de una imagen, dicho algoritmo está basado en la resta diferencial de la imagen con ruido y la imagen fuente para encontrar la imagen original y resaltar las modificaciones que estén en la imagen. Para realizar tal proceso se debe realizar copia de la imagen fuente en un archivo temporal del directorio de la herramienta GIMP y seguido de esto hacer el respectivo tratamiento de la imagen a tratar. En la figura 19 se observa la introducción de un archivo en directorio temporal para análisis de la imagen.

Figura 19. Generación de archivo temporal



Fuente: El Autor

Se escoge como valor default el 70% de saturación de la imagen duplicada y tratada como formato JPEG esta es llevada a la carpeta activa de temporales del software GIMP. Dicho valor de default se puede variar dependiendo del análisis que se requiera para la corrección de saturación de la imagen.

El siguiente paso en el algoritmo de implementación es la superposición diferencial de la imagen fuente con ruido (Saturación) contra la imagen fuente, con el uso de las funciones ya creadas en la herramienta GIMP, esta función llamará al archivo duplicado y la función “DIFF” realizará la resta de las imágenes haciendo el modo de diferenciación. Al realizar dicha operación hace necesario borrar el archivo duplicado del directorio de temporales ya que se genera un nuevo temporal el cual es el resultante del diferencial, tal como se muestra en la figura 20. La última línea del programa borra el archivo generado de forma automática.

Figura 20. Estructurado diferencial del nuevo archivo de imagen

```
;open 70% jpeg, set as diff layer
(set! draw-tmp (car(gimp-file-load-layer RUN-NONINTERACTIVE img-tmp filename)))
(gimp-image-add-layer img-tmp draw-tmp -1)
(gimp-layer-set-mode draw-tmp DIFFERENCE-MODE)
(file-delete filename)
```

Fuente: El Autor

En la programación del algoritmo en código después de realizar el momentum diferenciado, se debe hacer visible el archivo del nuevo generado en el directorio temporal y adjuntar un set point de error en la imagen, dicho margen de error significará las modificaciones realizadas en la imagen digital y dejará la saturación por default en la imagen resultante.

Figura 21. Set point de ELA

```
;error layer on top
(gimp-edit-copy-visible img-tmp)
(set! error-layer (car (gimp-layer-new-from-visible img-tmp img-tmp
"Niveles de error") ))
(gimp-image-add-layer img-tmp error-layer -1)
(gimp-levels-stretch error-layer)
;(gimp-display-new img-tmp)
```

Fuente: El Autor

La digitalización resultante del código debe ser reemplazada por la imagen original y por ultimo ser mostrada como archivo digital que muestra saturaciones en las modificaciones.

Figura 22. Imagen resultante

```
;add error levels as layer on orig image
(gimp-edit-copy-visible img-tmp)
(set! error-layer (car (gimp-layer-new-from-visible img-tmp img
"Niveles de error") ))
(gimp-image-add-layer img error-layer -1)
(gimp-drawable-set-name error-layer "Niveles de error)
```

Fuente: El Autor

Para finalización del algoritmo, se debe borrar el archivo temporal generado, establecer el archivo resultante realizar el registro del script generado dentro de los directorios internos de GIMP y se realiza el registro del script como firma del plugins creado.

Figura 23. Fin del algoritmo ELA

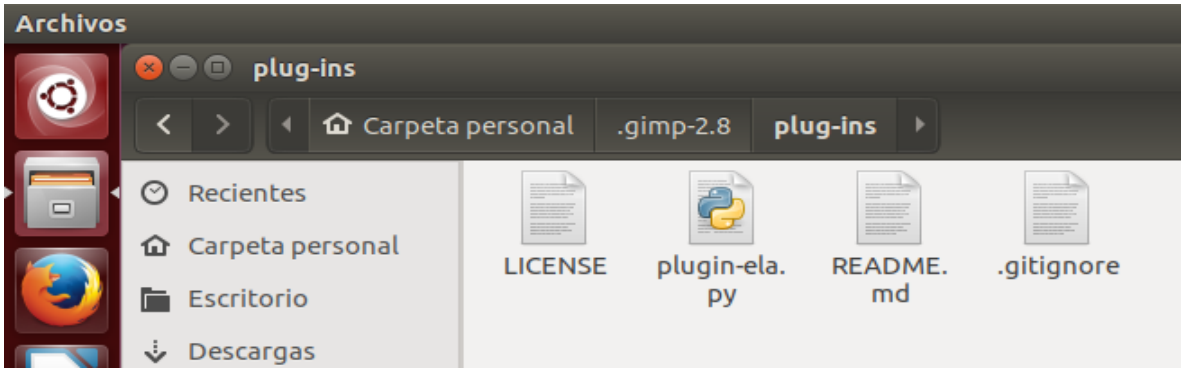
```
    ; tidy up
    (gimp-image-delete img-tmp)
    (gimp-image-undo-group-end img)
    (gimp-displays-flush)
    (gimp-context-pop)
    )
  )

(script-fu-register "AndresAcevedo-error-level-analysis"
                    _"_Error Level Analysis"
                    "El análisis a nivel de error muestra diferentes niveles de error
                    "a lo largo de esta imagen,sugiriendo fuertemente algún tipo de
                    "manipulación digital"
                    "Andres Acevedo <ing_andresacev1@hotmail.com>"
                    "Andres Acevedo"
                    "*"
                    SF-IMAGE       "Imagen de entrada"           0
                    SF-DRAWABLE    "modificacion de entrada"        0
                    SF-ADJUSTMENT _"Calidad"               '(0.7 0 1 0.1 1 1 0)
                    SF-STRING      "Nombre de archivo tempora   "error-level-analysis-temporal.jpg"
                    )
```

Fuente: El Autor

10.1. IMPLEMENTACIÓN DE PLUGINS EN GIMP 2.8

La herramienta GIMP en su versión 2.8 es multiplataforma, para el desarrollo de la técnica ELA se realiza la instalación del software en el SO Ubuntu en su versión más reciente, esto con el fin de que el algoritmo en código realizado funcione correctamente, en el Anexo A, se puede consultar el manual de instalación de la herramienta GIMP, desde consola. En el desarrollo del plugins en Python, se guarda el script en la extensión .py en el directorio del programa GIMP 2.8 en la carpeta Plug-ins, en la figura 24 se observa el directorio de instalación de complementos en donde solo basta con pegar el archivo realizado en Python.

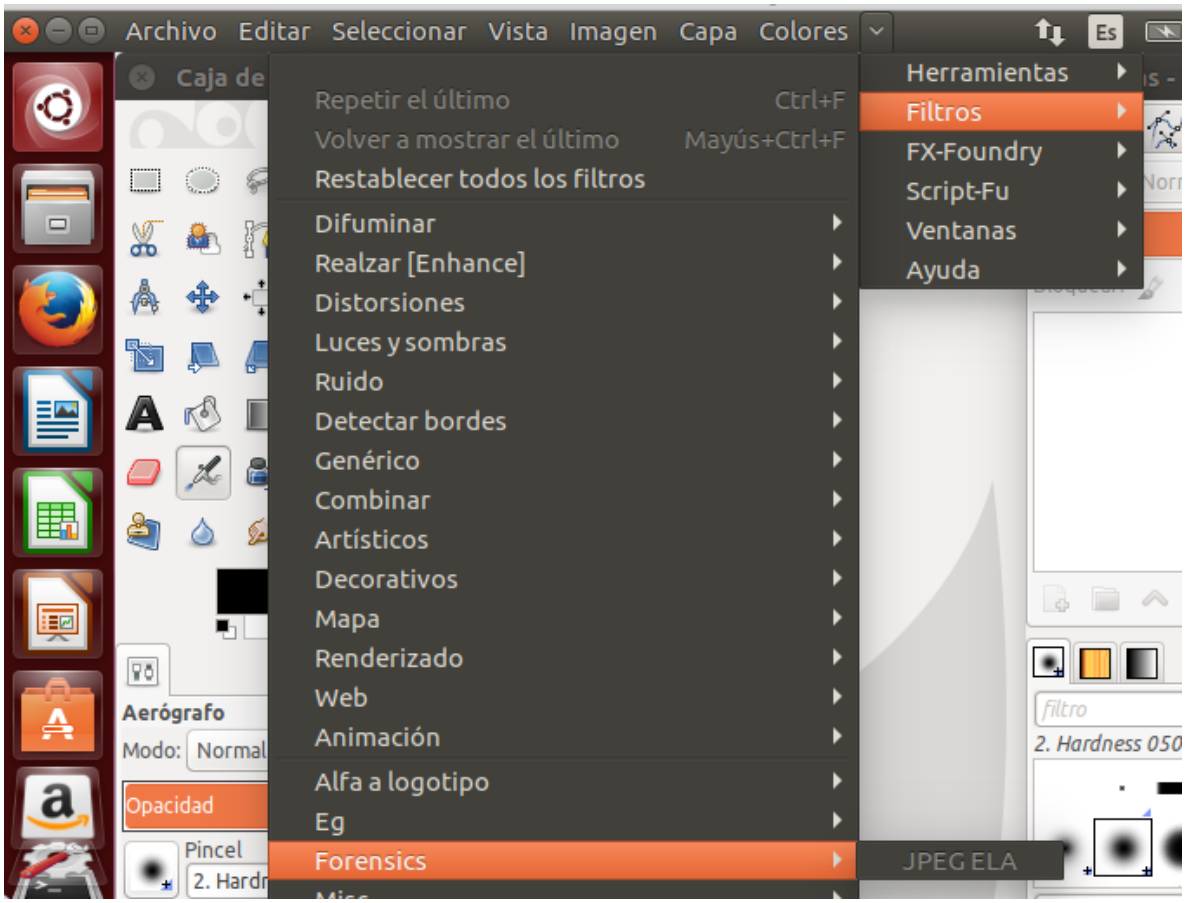
Figura 24. Instalación del Plug-ins



Fuente: El Autor

Al momento de ejecutar el programa se puede observar el complemento de la aplicación de la técnica error level analisys.

Figura 25. Validación de la herramienta

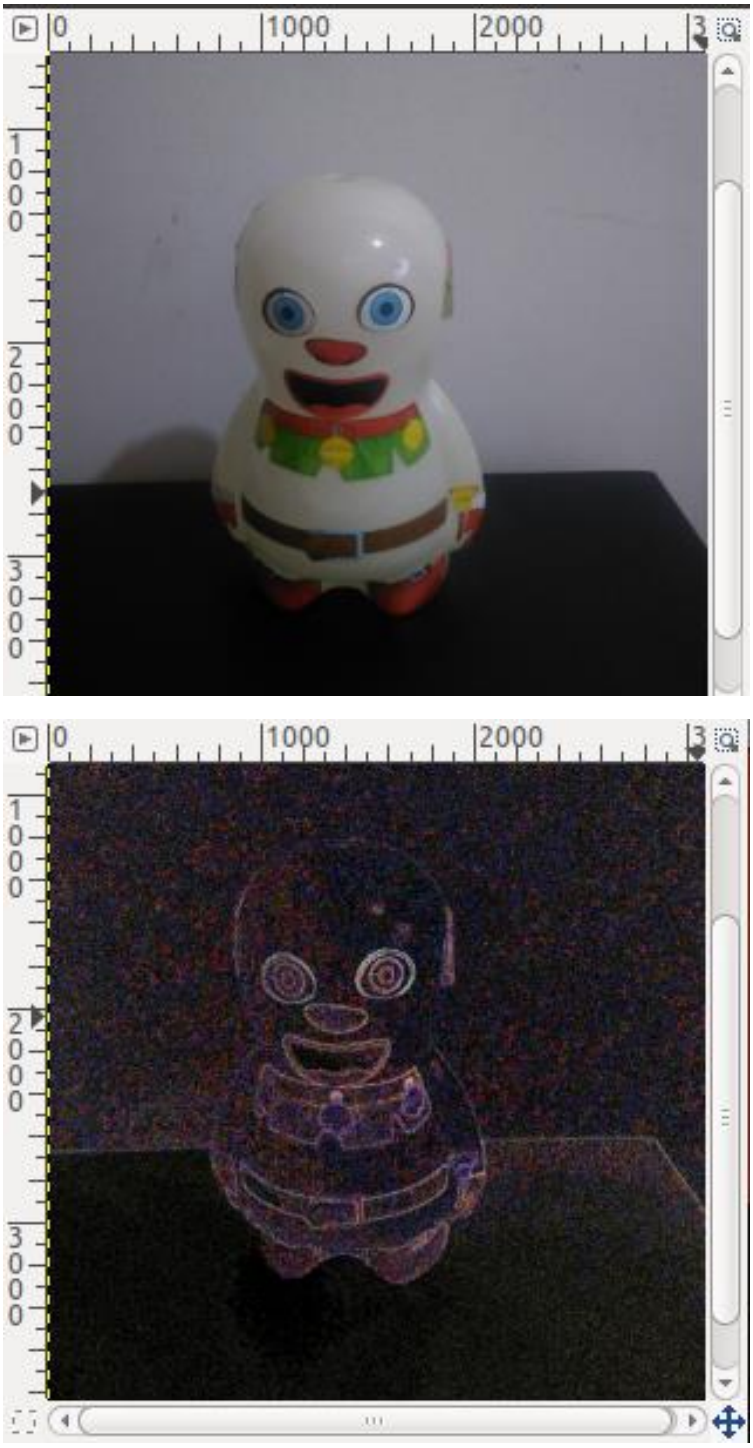


Fuente: El Autor

10.2. ANÁLISIS DE IMAGEN DIGITAL CON GIMP

Para el análisis de Error Level Analysis (ELA) en GIMP hace necesario cargar la imagen desde el entorno gráfico. La imagen debe ser de origen JPG o JPEG ya que es el tipo de formato que relacionan los dispositivos móviles, el siguiente ejemplo se tomó de un dispositivo móvil marca Lenovo en donde se quiere demostrar la eficiencia del algoritmo creado y por ende el correspondiente análisis. La figura 26 muestra el resultado del algoritmo ELA, en donde se observa que al momento de realizar el cargue de la imagen original sin modificaciones no se detecta alguna iluminación resaltante en la imagen, es decir debe arrojar un resultado de uniformidad al momento de la resultante realice el diferencial entre la imagen original y la imagen guardada en buffer y saturada al 70%, cabe recalcar que el algoritmo aunque tenga el setpoint por default, este se puede modificar al porcentaje que se quiera analizar.

Figura 26. Análisis de ELA imagen fuente original



Fuente: El Autor

Al momento de usar ELA esta identifica las áreas dentro de una imagen que se encuentran en diferentes niveles de compresión. Con las imágenes JPEG, toda la

imagen debe ser más o menos al mismo nivel de error. Si una sección de la imagen está en un nivel de error significativamente diferentes, entonces es probable que se observe una modificación digital. Como referencia se toma la imagen de la figura 26 y se realiza una modificación en ella para el correspondiente análisis con el algoritmo ELA.

Figura 27. Análisis de ELA de imagen modificada

Fuente: El Autor

Como se observa en la figura 27, al momento de realizar el análisis ELA a la imagen modificada se observan elementos que se resaltan más del error uniforme que se encuentra en la imagen. Las imágenes JPEG utilizan un sistema de compresión con pérdida. Cada re-codificación (Volver a guardar) de la imagen añade más pérdida de calidad a la imagen. Específicamente, el algoritmo JPEG opera en una cuadrícula de 8x8 por píxel. Cada cuadrado de 8x8 se comprime de forma independiente. Si la imagen es completamente sin modificar, a continuación, todos los cuadrados de 8x8 deben tener errónea similares. Si la imagen es sin modificar y volver a guardar, a continuación, todas las plazas deberán deteriorarse aproximadamente a la misma velocidad. ELA guarda la imagen en un nivel de calidad de JPEG especificado. Por lo tanto, volver a guardar introduce una cantidad conocida de error a través de toda la imagen. Si la imagen se vuelve a guardar se compara entonces con la imagen original. Si se modifica una imagen, entonces cada cuadrado de 8x8 que fue afectado por la modificación debe estar a un potencial de error más alto que el resto de la imagen. Las áreas modificadas aparecerán con un nivel de error potencial más alto.

10.3. COMPARACIÓN DEL ALGORITMO CON SOFTWARE WEB

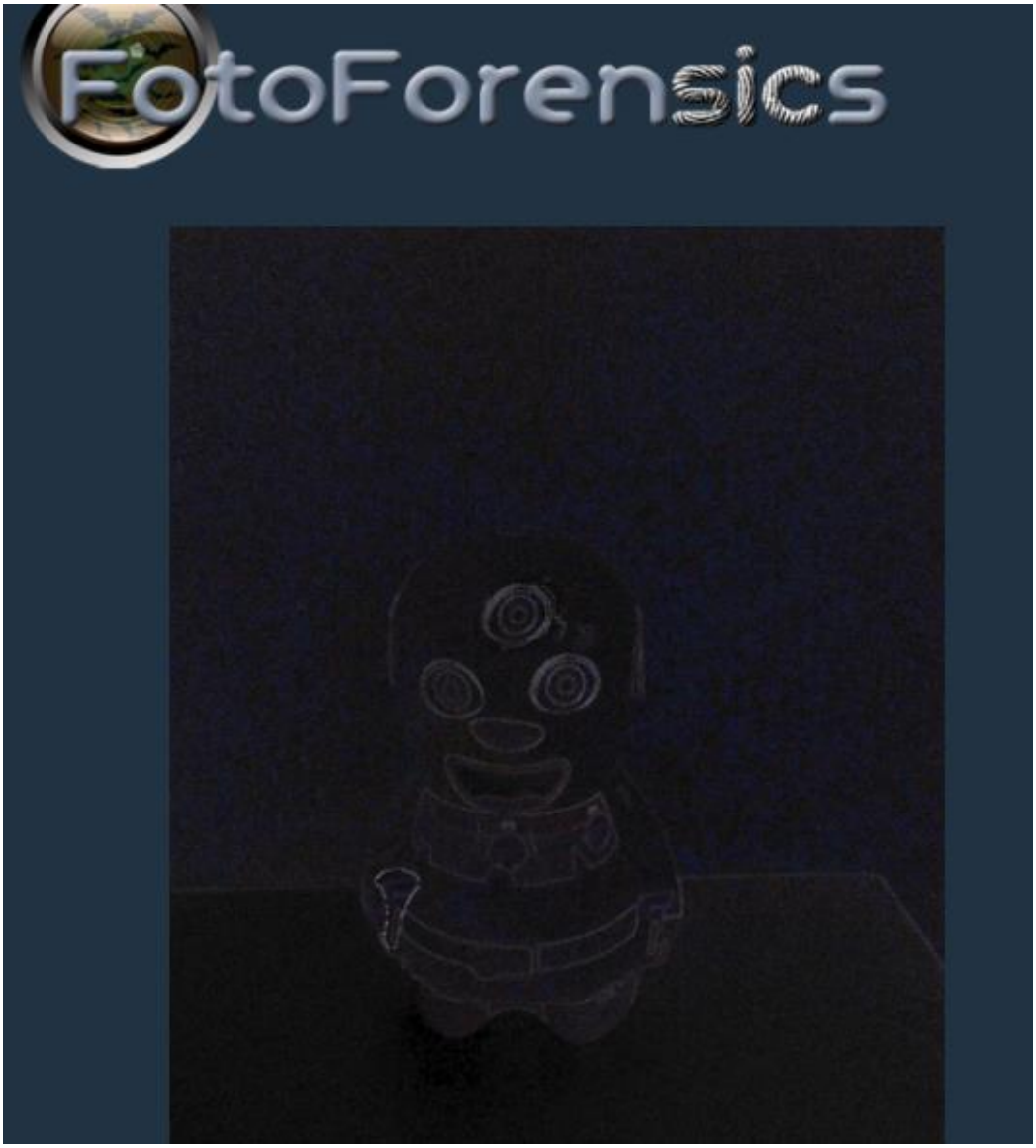
Para validar que tan efectivo fue el análisis anterior, hace necesario que se compare el algoritmo realizado con otras aplicaciones que hagan el análisis de saturación para verificar la uniformidad del error y encontrar las modificaciones en una imagen digital, por lo tanto, se empezará con la aplicación Fotoforensics. La figura 29 muestra el análisis de la imagen de ejemplo con modificaciones, para acceder a la aplicación, muestra la siguiente interface, en donde debe cargarse la imagen a analizar.

Figura 28. Aplicación Web Fotoforensics

Fuente: http://fotoforensics.com/

Se observa que la resultante tiene partes más saturadas que en la fotografía original, por lo tanto, aunque arroja el mismo resultado esperado del algoritmo, pero como resultante una imagen más oscura y menos nítida al momento de realizar el deferencial de la imagen fuente vs la imagen saturada.

Figura 29. Resultante ELA Fotoforensics

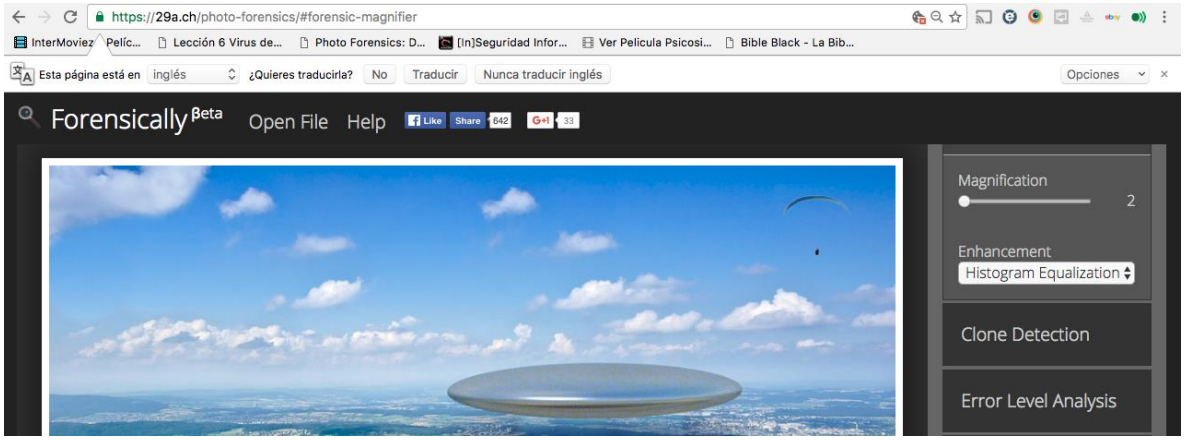


Fuente: http://fotoforensics.com/analysis.php?id=8a052372ffd8d3c2ef2ca613d2c3a63f77a878d2.1948064

También se encuentra la herramienta Forensically el cual realiza el mismo análisis de error de nivel para encontrar modificaciones en las imágenes digitales en la figura

30, se puede observar la interface de la herramienta online el cual además de realizar el análisis ELA, puede verificar el ruido en las imágenes, metadatos, thumbnail entre otros.

Figura 30. Aplicación web Forensically



Fuente: https://29a.ch/photo-forensics/#forensic-magnifier

Al momento de realizar ELA, se observa más claridad en la imagen, aunque con el resultado esperado, hace un poco más difícil encontrar las modificaciones, por la claridad de las imágenes, tal como se muestra en la figura 31.

Figura 31. Resultante ELA Forensically

Fuente: https://29a.ch/photo-forensics/#error-level-analysis

Con los resultados anteriores, se puede observar que el algoritmo desarrollado en Python está programado de forma correcta el cual mediante el script diseñado se obtiene mejores resultados para el método de Error Level Analysis, por lo tanto, es más confiable en el análisis de evidencias en casos delicados en donde se puede estar comprometiendo alguna violación de los derechos humanos, como el derecho a la vida, el derecho a la libertar entre otros.

11. ANÁLISIS DE METADATOS CON EXIFTOOL

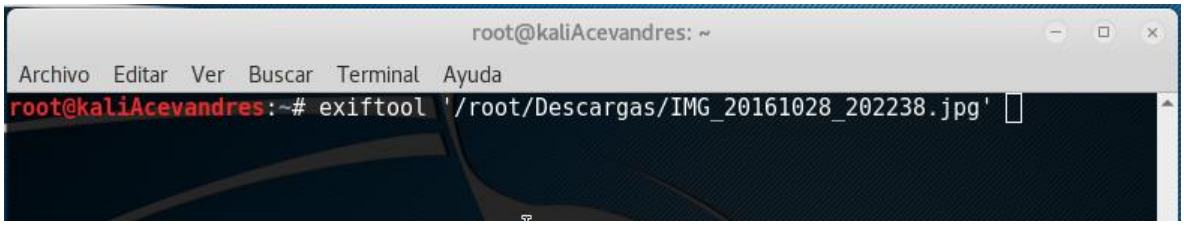
Para completar el análisis de la imagen hace necesario realizar un estudio de sus metadatos, cabe decir que según el flujograma del proceso de selección de una imagen valida como evidencia de la figura 15, este análisis solo se realiza cuando al momento de aplicar el algoritmo de ELA los resultados deben ser de una imagen original, es decir que no tenga modificaciones ya que al momento de que una imagen se somete a una modificación estarían cambiando en si los metadatos internos, el cual no sería favorable para la investigación.

A continuación, se presenta el análisis de una imagen tomada con origen de un dispositivo móvil, en donde se podrán observar diferentes datos de la cabecera Exif de la imagen. Cabe recalcar que para este análisis existen un sinnúmero de herramientas para validación de los metadatos, pero para el desarrollo de esta investigación se usa la herramienta Kali Linux ya que se consideró como una herramienta apropiada para realizar el respectivo análisis, además de que es un SO de software libre por lo que no tiene ningún costo. La instalación de la herramienta Exiftool se podrá ver en el anexo B, para cualquier consulta de cómo se debe realizar dicha instalación.

Una vez realizada la instalación de forma correcta de la herramienta, se podrá ejecutar la herramienta desde el CLI del sistema operativo Kali Linux con el siguiente comando:

Exiftool "directorio de la imagen"

Figura 32. Llamado de Exiftool para análisis de imagen



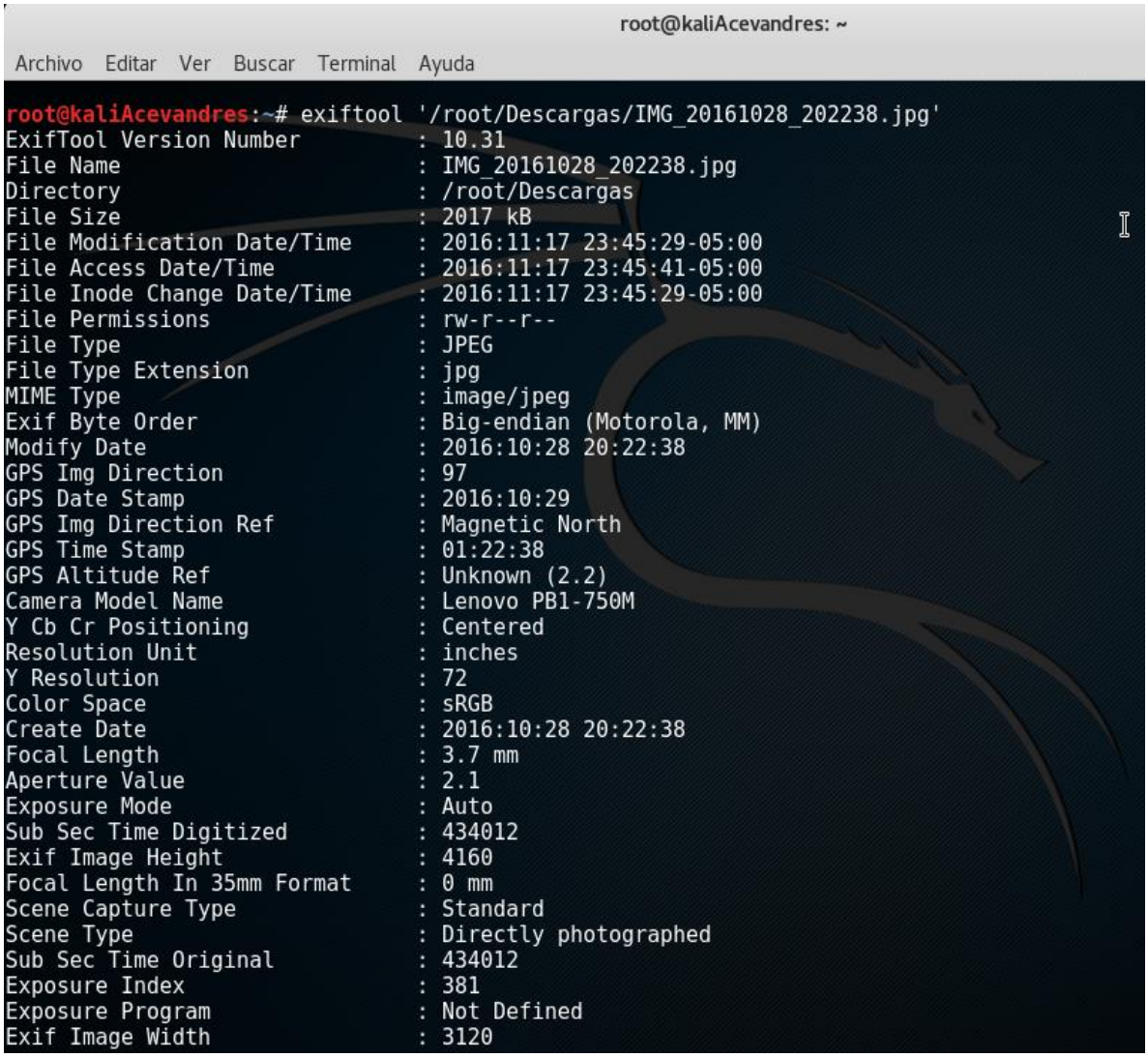
Fuente: El Autor

Una vez realizado el llamado del directorio de la imagen este empezará a realizar el análisis de la imagen con el fin de extraer los datos de cabecera Exif en donde arrojará la información de los metadatos encontrados en la imagen, en dicho resultado se puede observar, desde la versión usada por el dispositivo de forma Exif hasta los valores de la longitud focal del lente de la cámara del dispositivo móvil.

Cabe recalcar que, dependiendo del dispositivo móvil, también del fabricante los metadatos pueden variar en su cabecera. Como se muestra en la figura 33, el resultado del análisis de la imagen que anteriormente fue tratada en el algoritmo ELA

allí se puede apreciar la cantidad de datos significativos que se pueden sacar de una imagen.

Figura 33. Metadatos de la imagen



Fuente: El Autor

Como se puede observar en la figura 33, es el resultado de los elementos de cabecera Exif, en donde se puede apreciar datos importantes de la imagen al momento de certificar la valides de la misma, a continuación, en la tabla 9 se muestra el significado de los datos más relevantes

Tabla 9. Significado de los datos de cabecera Exif

Cabecera EXIF	Significado	Observación
Exiftool Version Number	Versión de cabecera Exif	10.31
File Name	Nombre del Archivo	IMG_20161028_202238.jpg
Directory	directorio de la imagen en el pc	root/Descargas
File Size	Peso del archivo	2017 Kb
File Modification Date	Fecha de modificación del archivo	2016:11:17 23:45:29-05:00
File Permissions	Permisos de archivo	rw-r--r--, lectura y escritura
File Type	Tipo de archivo	JPEG
File Type Extension	Tipo de extensión de archivo	jpg
Modify Date	Fecha de modificación	2016:10:28 20:22:38
GPS Img Direction	Indica la dirección de la imagen cuando fue capturada. El intervalo de valores es de 0,00 a 359,99.	97
GPS Time Stamp	Indica el tiempo del UTC (Tiempo Universal Coordinado). TimeStamp se expresa con tres valores racionales que dan la hora, minuto y segundo	2016:10:29
GPS Img Direction Ref	Indica la referencia para dar la dirección de la imagen cuando se captura. 'T' denota dirección verdadera y 'M' es Dirección magnética.	Magnetic North
GPS Time Stamp	Indica el tiempo como UTC (Tiempo Universal Coordinado). TimeStamp se expresa como tres valores RACIONALES que dan la hora, minuto y segundo.	01:22:38
GPS Altitude Ref	Indica la altitud utilizada como altitud de referencia. En esta versión la altitud de referencia es el nivel del mar, por lo que esta etiqueta debe estar en 0 desconocida. La unidad de referencia es metros.	Unknown (2.2)
Camera Model Name	Nombre y modelo de la cámara	Lenovo PB1 - 750M
Y Cb Cr Positioning	Es la posición de la Crominancia versus los componentes de la luminancia, se manejas dos estados: 1 = centered; 2 = co-sited	Centered
Resolution Unit	Es la unidad usada para la resolución horizontal y vertical. Los valores están dados en pulgadas o centímetros	inches
Create Date	Fecha de creación	2016:10:28 20:22:38
Focal Length	Longitud focal del lente de la cámara	3.7 mm
Scene type	se confirma que la fotografía no tiene agregados por el software de la cámara	Directly photographed

Tabla 9. (Continuación)

Cabecera EXIF	Significado	Observación
Exif Image Width	Es el número de columnas de datos de imagen, igual al número de píxeles por fila.	3120

Fuente: El Autor

El análisis arroja más resultados el cual se omitieron ya que no son relevantes para la investigación. Este es el proceso final del procesamiento de la imagen y el análisis de la misma con el fin de concluir un proceso acusatorio ya sea en contra o en pro de la víctima en donde se puede demostrar mediante una imagen sin modificaciones datos importantes como la fecha en que se tomó la foto, el modelo del dispositivo móvil, la posición de geográfica (GPS), formato de la imagen entre otras.

Este último proceso solo se realiza, si la aplicación del algoritmo ELA sale negativo, es decir sin modificaciones realizadas, comprobando la originalidad de la imagen.

11.1. METADATOS CON OTRAS APLICACIONES

Existen diferentes herramientas para realizar verificación de los metadatos existentes en imágenes digitales el cual mostraran diferentes visualizaciones de los metadatos dependiendo de la lectura que realicen de las cabecera Exif.

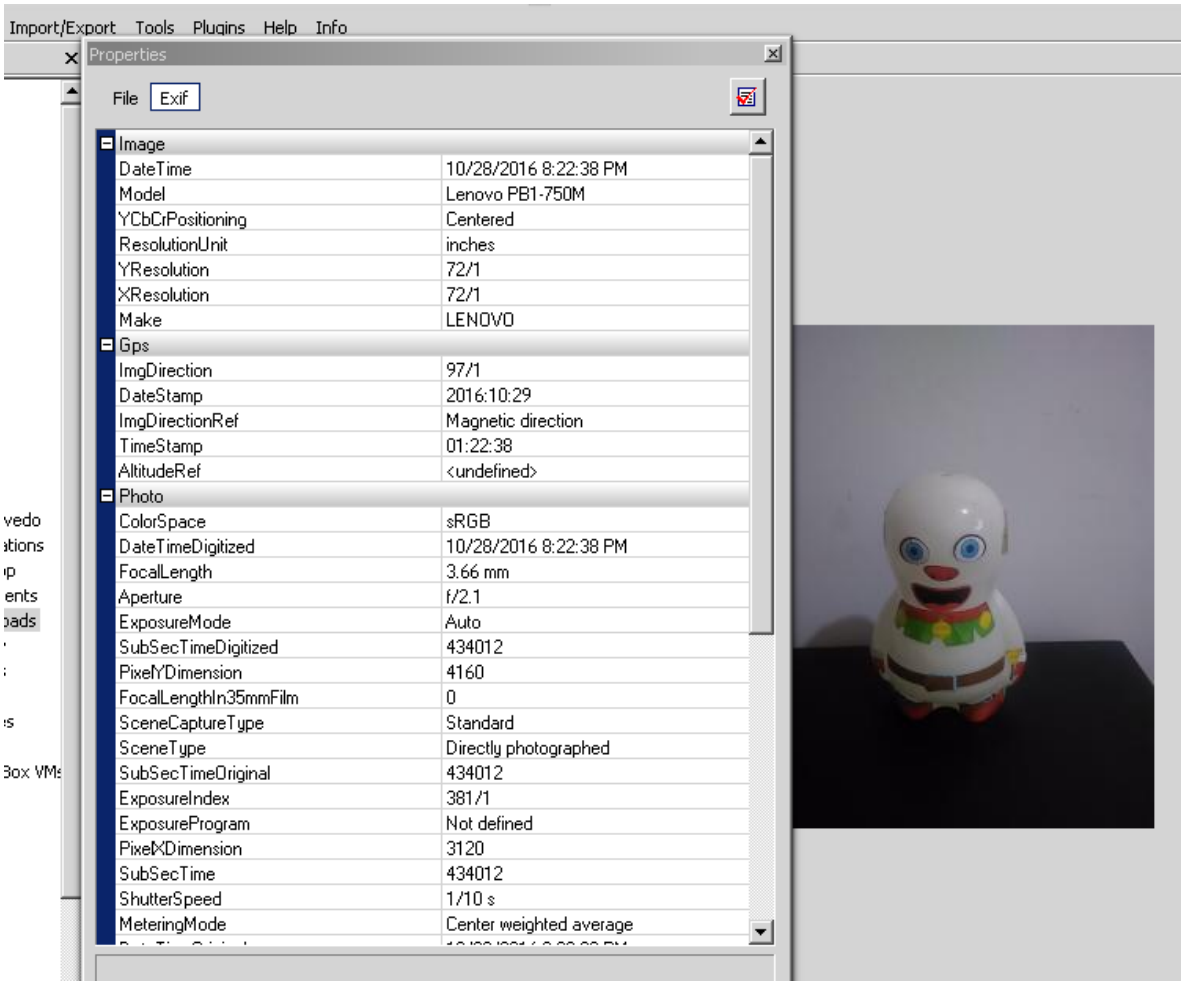
Como se muestra en la figura 35, la resultante son los datos de la cabecera Exif usando la herramienta Exif Pilot, dicha herramienta también puede ser usada para limpiar los metadatos y cambiarlos si es necesario. Ofrece la visibilidad de una imagen en miniatura del archivo analizado además de poder exportar en formato CSV los metadatos encontrados en la imagen. La versión de Exif Pilot se puede descargar desde la página principal y puede ser usada en dos sistemas operativos Windows y versiones MAC. Se encuentra la versión 4.12.1.

Figura 34. Exif Pilot

Fuente: El Autor

Tal como se puede observar en la figura 35 la herramienta realiza la clasificación de los datos de cabecera como Imagen, GPS, Photo entre otras.

Figura 35. Cabeceras Exif con Exif Pilot



Fuente: El Autor

Exif Pilot también ofrece realizar la validación de la imágenes thumbnail y también de poder modificar dicha parte de la cabecera de la imagen. Cabe recalcar que la versión 4.12.1 es gratuita y de libre distribución.

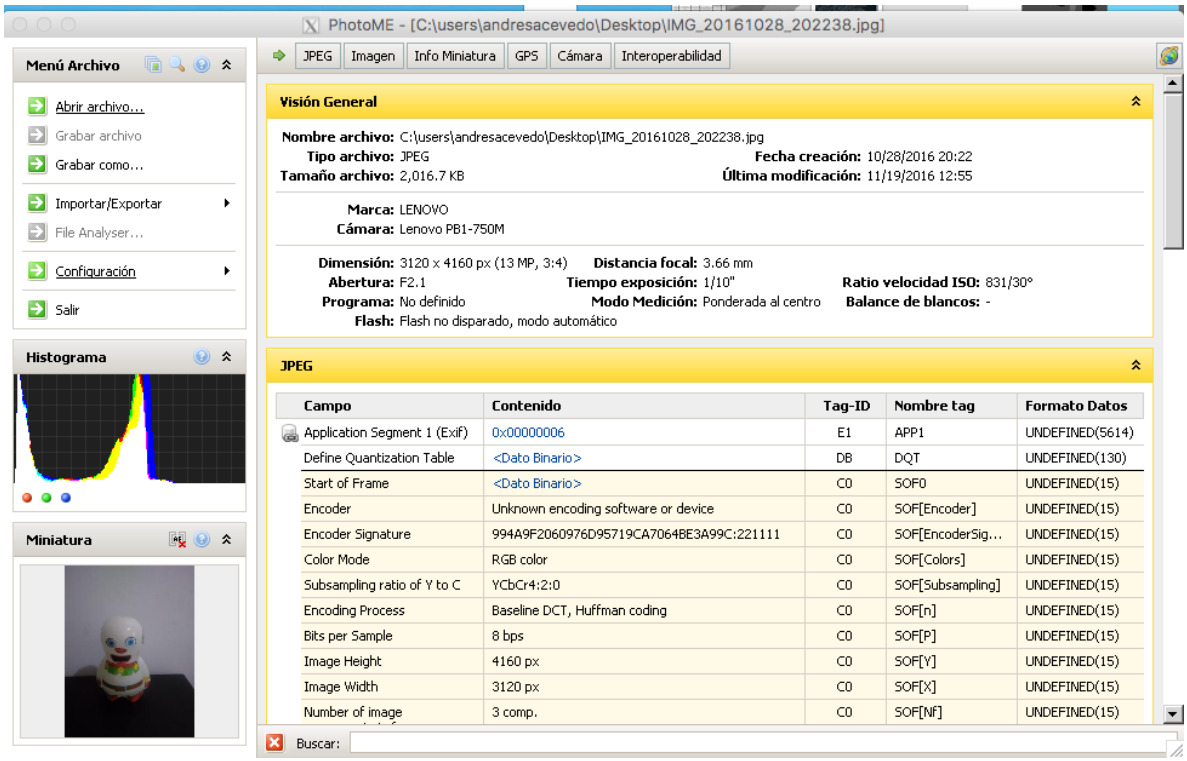
También se realiza la comparación del análisis de metadatos con la herramienta PhotoME, el cual realiza una validación general de la imagen, la versión 0.8 ofrece inspeccionar los datos Exif además de realizar una breve grafica en forma de histograma en donde muestra la exposición de los colores (RGB) para determinar la extra posición del brillo en la imagen digital. Se puede descargar una versión beta de forma gratuita en la página del fabricante, tal como se muestra en las especificaciones de PhotoME en la figura 36.

Figura 36. PhotoMe

Fuente: El Autor

La imagen 37 muestra el análisis realizado por la herramienta PhotoMe en donde esta muestra una vista general de los Datos Exif

Figura 37. Cabeceras Exif con PhotoME



Fuente: El Autor

Como se puede observar en la figura anterior PhotoMe, muestra un histograma RGB para confirmar la exposición del brillo en la imagen, con el resultado arrojado se puede observar que el histograma está indicando la distribución de los colores básicos (rojo, azul y verde). Según el análisis del histograma se puede observar que la distribución de colores está mayormente en la parte derecha del histograma, por lo que significa que la imagen es sobreexpuesta.

12. ANÁLISIS DE UN BANCO DE IMÁGENES USANDO LA TÉCNICA ELA

De acuerdo a la técnica ya establecida anteriormente Error Level Analysis, permite hallar las modificaciones que se han realizado a una imagen proveniente de un dispositivo móvil. Por consiguiente, hace necesario hacer el respectivo análisis por medio de un banco de imágenes provenientes de celulares de diferentes modelos. Cabe recalcar que a estas imágenes se realizaron modificaciones y/o montajes con el fin de prueba del algoritmo realizado. Para realizar el banco de imágenes, fueron obtenidas de personas cercanas o conocidas que facilitaron la evidencia digital con modificaciones, esto seguido de la marca y modelo del móvil. Dicho banco de imágenes comprende de 150 imágenes provenientes de 6 marcas y diferentes modelos de referencia del fabricante.

Tabla 10. Clasificación de móviles por marca y modelo

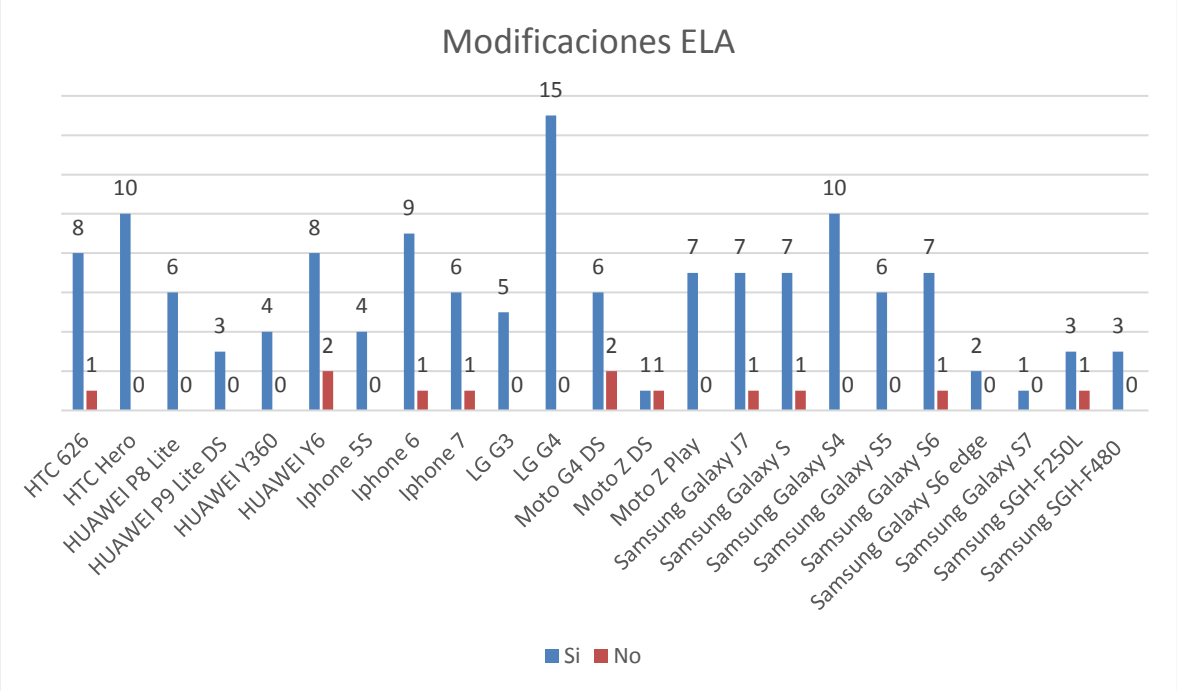
Marca	Modelo	Numero de fotos
Apple	Iphone 5S	4
	Iphone 6	10
	Iphone 7	7
LG	LG G3	5
	LG G4	15
Samsung	Samsung Galaxy S	8
	Samsung SGH-F250L	4
	Samsung SGH-F480	3
	Samsung Galaxy S4	10
	Samsung Galaxy S5	6
	Samsung Galaxy S6	8
	Samsung Galaxy S6 edge	2
	Samsung Galaxy S7	1
	Samsung Galaxy J7	8
HTC	HTC Hero	10
	HTC 626	9
Motorola	Moto G4 DS	8
	Moto Z Play	7
	Moto Z DS	2
Huawei	HUAWEI P8 Lite	6
	HUAWEI P9 Lite DS	3
	HUAWEI Y6	10
	HUAWEI Y360	4

Fuente: El Autor

12.1. ANÁLISIS DE INFORMACIÓN ELA

Al momento de realizar el respectivo análisis con el algoritmo de ELA mediante la herramienta GIMP en el entorno Linux, tal como se observa en la figura 38, el cual se encuentra que casi en la totalidad de las imágenes con modificaciones, se encontró la saturación correspondiente a las modificaciones, en excepción de algunas imágenes en donde la saturación de cada una de la regla de pixeles 3x3 del formato JPG en donde era uniforme por lo que no se notaba el error de nivel.

Figura 38. Modificaciones ELA



Fuente: El Autor

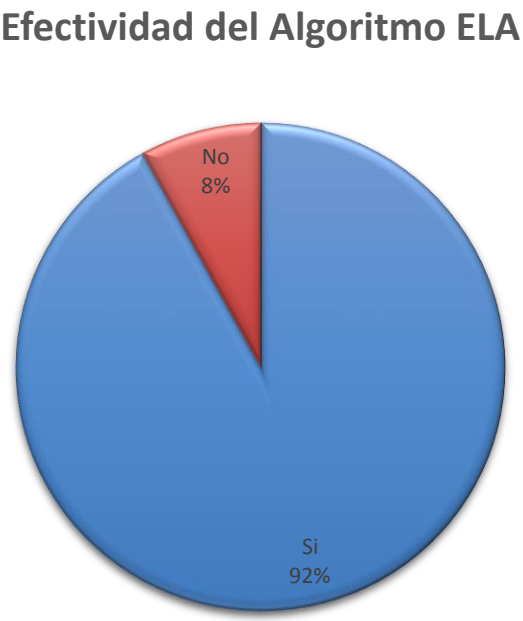
En las siguientes figuras se puede evidenciar que en algunos modelos no se puede diferenciar la saturación que producen las modificaciones realizadas debido al nivel de uniformidad tomada del mismo segmento de imagen, a continuación se muestra en la figura 39, el resultado de ELA para el modelo HTC 626. Se puede apreciar que el resultado del análisis no da un indicio de alguna conclusión, puesto tal como se ha mencionado con anterioridad, debido a la regla 3 x3 pixeles del formato JPEG, las modificaciones realizadas a la imagen no se apreciaran.

Figura 39. Imagen Modelo HTC 626

Fuente: El autor

La formación de nuevos pixeles en cada uno de los factores del acomodamiento de la imagen permite saturar los pixeles y realizar un nuevo factor de hasta 10x10 pixeles en el nuevo espacio de color RGB, es ahí donde la crominancia actúa en la imagen digital y expone el color haciendo un realce de la información lumínica de los pixeles, y a la vez mostrando un tinte de negativo de color blanco en cada de una de las imágenes analizadas mediante el algoritmo del Error Level Analysis. En la figura 39 se puede observar la efectividad de la técnica respecto a las modificaciones encontradas de un 92%, haciéndola efectiva al momento de usarla para análisis de una evidencia.

Figura 40. Efectividad del Algoritmo

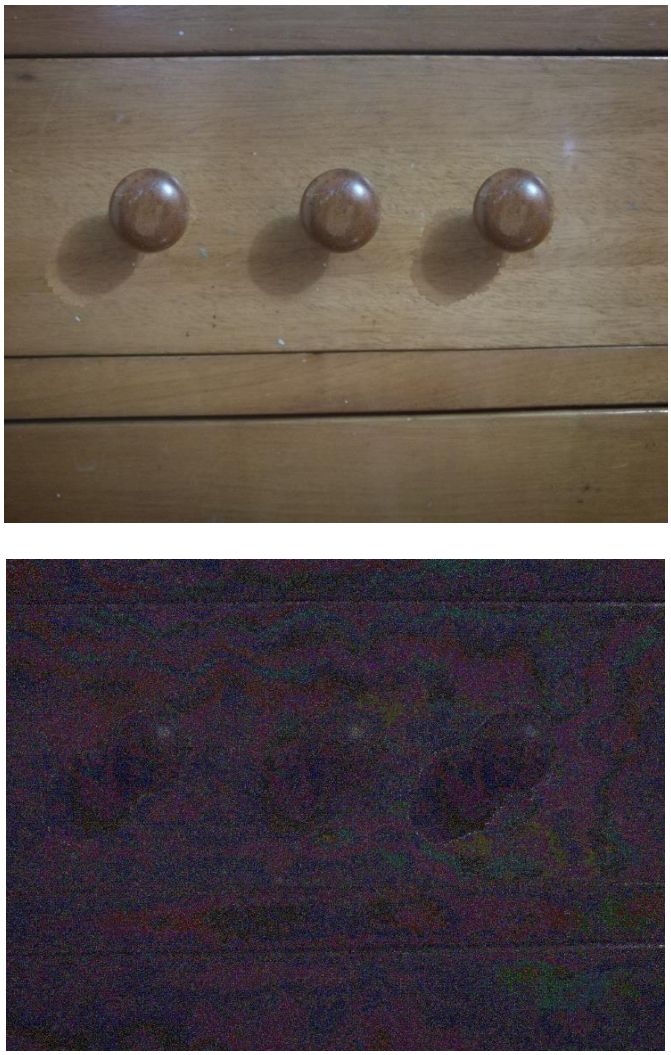


Modificaciones	Total
Si	138
No	12

Fuente: El Autor

El análisis de las imágenes arrojó un excepcional resultado, ya que se demuestra la efectividad del algoritmo realizado para la aplicación de la técnica, es por eso que es necesario realizar el respectivo análisis de los archivos de cabecera Exif o metadatos del conjunto de imágenes con el fin de validar que tan eficiente es la validación de las cabeceras. Tal como se muestra en la figura 41, se evidencia el resultado de ELA para una de las imágenes tomadas por un Huawei P9, en la imagen se puede apreciar las modificaciones realizadas en la parte iluminada de sobresaturación en donde se demuestra que dichos sectores “iluminados” están en un diferente factor de acomodamiento de los pixeles del formato JPEG. En la imagen se puede analizar que solo la esfera del centro es la real, y que la de los extremos fueron modificaciones realizadas a partir de la esfera real por lo que las sombras se ven más pronunciadas.

Figura 41. Resultado ELA del Huawei P9



Fuente: El Autor

12.2. ANÁLISIS DE METADATOS DEL BANCO DE IMÁGENES

El análisis de los metadatos se debe medir por la lectura estadística del banco de imágenes realizados, ya que por medio de esto hace posible medir que tan efectivo puede ser la lectura de los datos de cabecera. En la tabla 12 se puede observar el análisis realizado de las imágenes propuestas de acuerdo al porcentaje de seguimiento que realizan los fabricantes al incluir los metadatos en las imágenes.

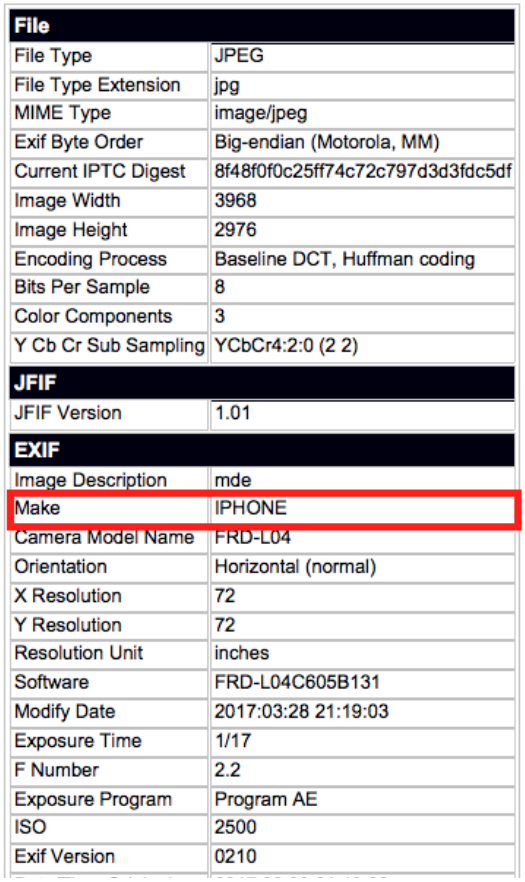
Tabla 11. Resultado análisis de metadatos de cabecera Exif

Marca	Modelo	Numero de fotos	Número de Fotos Datos Exif	Porcentaje de Seguimiento
Apple	Iphone 5S	4	4	100%
	Iphone 6	10	10	100%
	Iphone 7	7	0	-
LG	LG G3	5	5	100%
	LG G4	15	15	100%
Samsung	Samsung Galaxy S	8	8	100%
	Samsung SGH-F250L	4	4	100%
	Samsung SGH-F480	3	3	100%
	Samsung Galaxy S4	10	10	100%
	Samsung Galaxy S5	6	0	-
	Samsung Galaxy S6	8	8	100%
	Samsung Galaxy S6 edge	2	2	100%
	Samsung Galaxy S7	1	1	100%
	Samsung Galaxy J7	8	8	100%
HTC	HTC Hero	10	10	100%
	HTC 626	9	0	-
Motorola	Moto G4 DS	8	8	100%
	Moto Z Play	7	7	100%
	Moto Z DS	2	2	100%
Huawei	HUAWEI P8 Lite	6	6	100%
	HUAWEI P9 Lite DS	3	3	100%
	HUAWEI Y6	10	10	100%
	HUAWEI Y360	4	4	100%

Fuente: El Autor

Según la tabla 11, se puede observar el porcentaje de seguimiento de los fabricantes en donde las marcas Apple, Samsung, HTC en algunos de sus modelos se incluye el nombre de la marca del móvil mas no del modelo, en la figura 42 se puede observar los metadatos extraídos del modelo Iphone, en donde se puede observar en el recuadro en rojo que el resultado para este tipo de fabricante solo señala el dato exif de la marca mas no del modelo.

Figura 42. Metadatos de imagen de Iphone 6



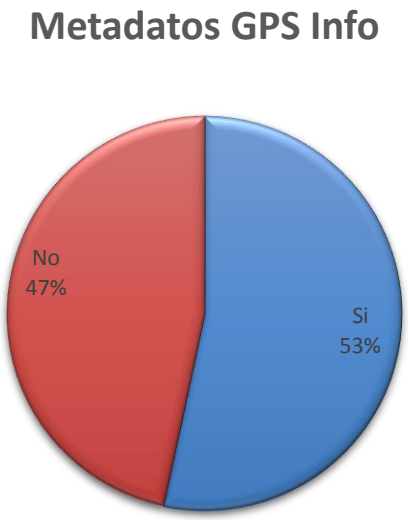
File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Current IPTC Digest	8f48f0f0c25ff74c72c797d3d3fdc5df
Image Width	3968
Image Height	2976
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
JFIF	
JFIF Version	1.01
EXIF	
Image Description	mde
Make	IPHONE
Camera Model Name	FRD-L04
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	FRD-L04C605B131
Modify Date	2017:03:28 21:19:03
Exposure Time	1/17
F Number	2.2
Exposure Program	Program AE
ISO	2500
Exif Version	0210

Fuente: El autor

12.3. ANÁLISIS DE AGREGACIÓN DE POSICIONAMIENTO (GPS)

Del banco de imágenes se realiza el análisis de la data del sector *GPS info* el cual depende de que el usuario final tenga activado el GPS del dispositivo y de que el fabricante incluya este objetivo en su metadato. La figura 40 representa el porcentaje encontrado equivalente al 53% en la cual cada uno de los dispositivos móviles incluyen los datos del GPS

Figura 43. Metadatos GPS Info

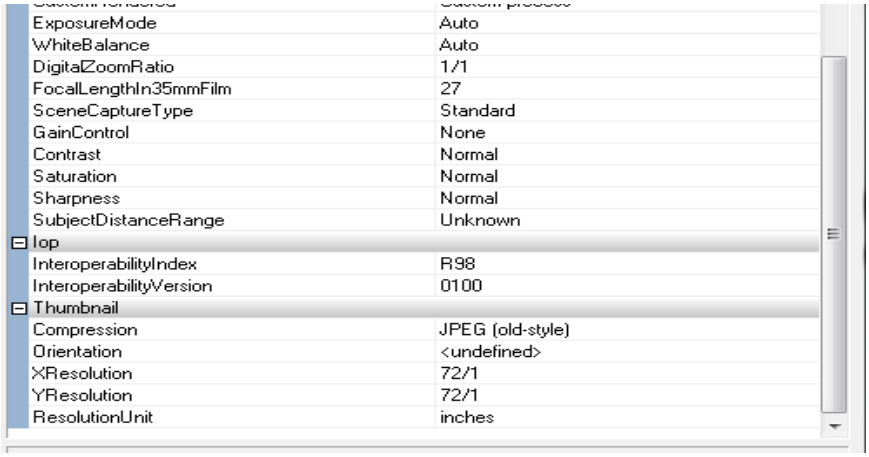


Metadatos GPS Info	Total
Si	80
No	70

Fuente: El Autor

De acuerdo al resultado obtenido de la estadística se puede observar que el 47% de las imágenes de los diferentes modelos de celular no incluye en su cabecera Exif el contenido GPS Info esto es debido a que el fabricante no lo cree relevante o que por alguna razón el usuario tiene deshabilitado la opción del GPS en alguna de sus opciones por default. En la figura 44, metadatos de la imagen tomada desde un Huawei P9, en este modelo el fabricante no incluye el dato GPS.

Figura 44. Metadatos GPS Info Huawei P9

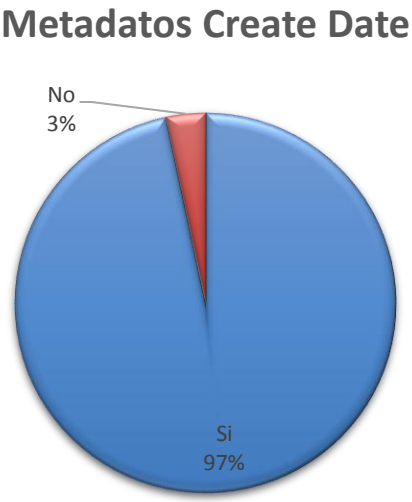


Fuente: El Autor

12.4. ANÁLISIS DE AGREGACIÓN DE FECHA DE CREACIÓN (CREATE DATE)

Para completar el análisis estadístico era necesario realizar el estudio “create date” ya que es un dato fundamental en el estudio de la evidencia digital, en cualquier caso. En la figura 41 se puede observar que la mayoría de los fabricantes incluye este dato en los móviles para agregación de los metadatos de cabecera Exif, se concluye que el 97% de las imágenes estudiadas contiene estos datos.

Figura 45. Metadatos Create Date

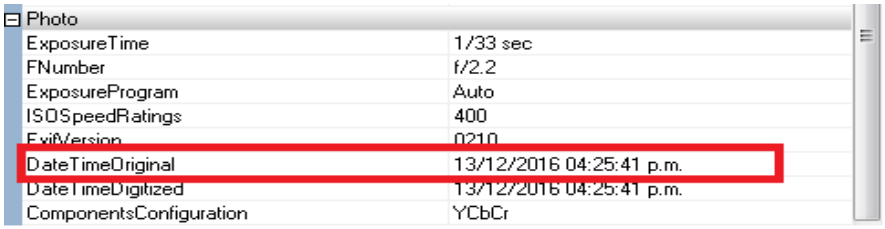


Metadatos Create Date	Total
Si	145
No	5

Fuente: El Autor

Es tipo de metadato informa la fecha y hora de creación de la imagen, lastimosamente es un dato vulnerable ya que se puede modificar con los mismos programas de visualización de metadatos. En la figura 46 se puede observar el metadato de la cabecera Exif “Create Date” para el modelo Huawei P9.

Figura 46. Metadatos Create Date Huawei P9



Fuente: El Autor

13. RECOMENDACIONES

Para que la técnica Error Level Analysis funcione correctamente hace necesario que la evidencia digital esté en formato JPG o JPEG el cual dicho formato por defecto lo utilizan los dispositivos móviles, es por eso que en el flujograma de proceso de análisis de la figura 15 recomienda, convertir o cambiar el formato de la evidencia presentada, si y solo si, la imagen se encuentra en otro tipo de extensión.

Se recomienda guardar un backup de la imagen original, ya que por temas del formato JPG, cada vez que se abra la imagen, el efecto de las pixelación 6X6, termina degradando las imágenes y realizando en cierto momento un cambio en las modificaciones que se encuentren en tal caso que las tuviera.

Se recomienda que la herramienta GIMP con el plugin del algoritmo ELA, debe estar instalado en equipos autorizados, por lo que cualquier modificación en el código de la programación de ELA, puede causar errores en el análisis, además de hacer saturaciones incorrectas en las modificaciones, permitiendo dar un resultado erróneo.

El resultado de la saturación impuesta por el algoritmo ELA, arroja un tinte distinto en las modificaciones, por lo que se puede observar una luminosidad diferente a los subespacios de la fuente original, debido a esto el archivo que resulta del algoritmo puede aumentar de peso significativamente, debido a que se debe manejar una calidad mayor al del archivo original, por lo que se recomienda que la herramienta GIMP esté instalada en un equipo con característica óptimas para el desarrollo de este tipo de análisis.

El análisis de los metadatos en las imágenes es el siguiente proceso para confirmar finalmente la información que se necesita para concluir el documento forense como evidencia de alguna eventualidad que este siendo juzgada ante la ley. Este tipo de datos son muy sensible al cambio por lo que se recomienda que cada vez que se haga el análisis de cabecera Exif, sea guardado en un documento aparte.

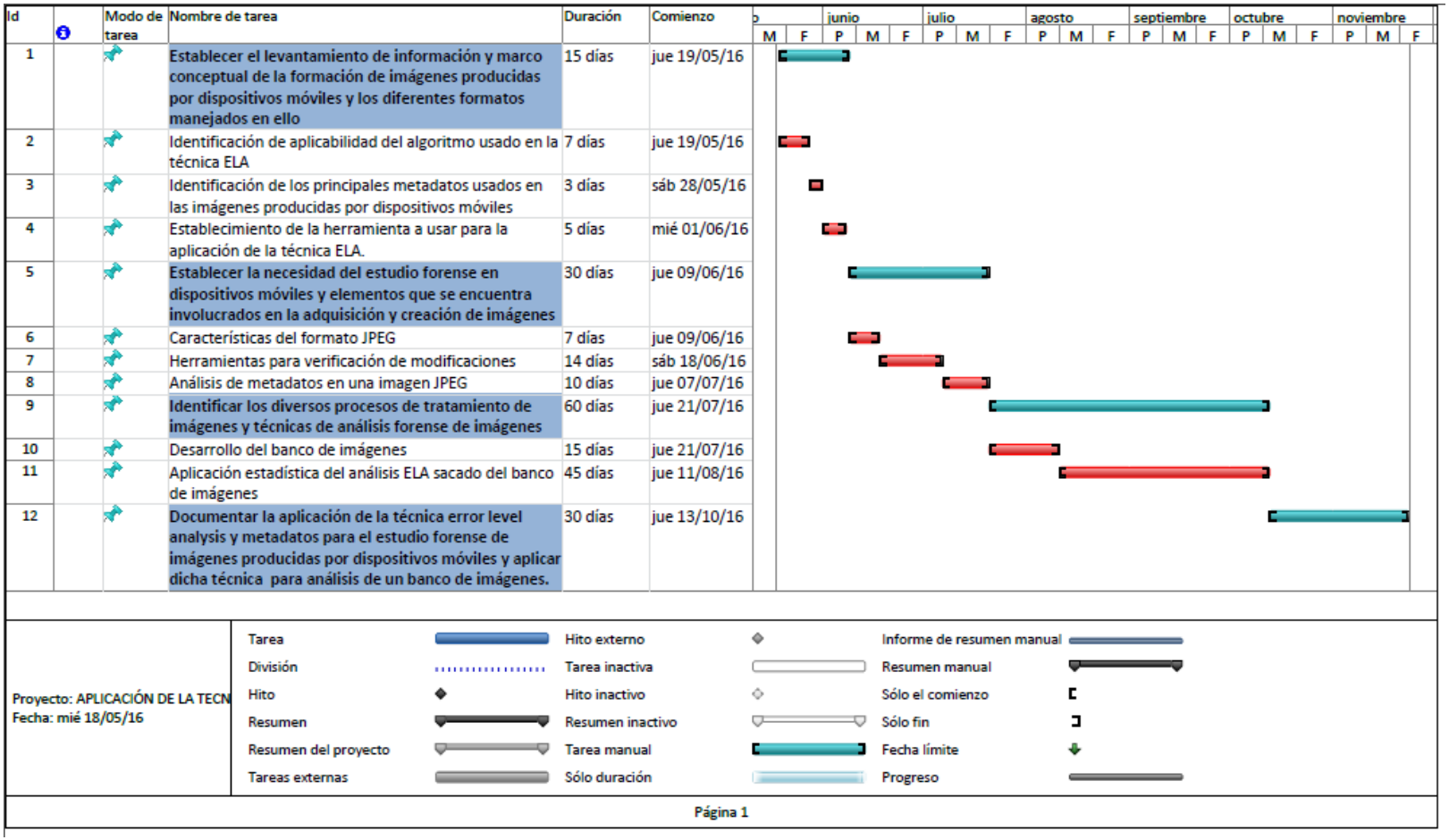
14. DIVULGACIÓN

Para la aplicación respectiva de la técnica Error Level Analysis y metadatos hace necesario divulgarla para así hacerla conocer, puesto que está dentro del campo de la investigación y el desarrollo el cual está abierta a la inclusión de nuevas características dentro de su programación, por lo tanto dicha técnica hace necesario publicarla dentro de los repositorios de la biblioteca de la Universidad Nacional Abierta y a Distancia en donde la información estará abierta a la lectura investigativa para dar la aplicabilidad de las técnica aquí propuesta, dando inicio al desarrollo activo de otras metodologías de estudio y técnicas en visión del desarrollo del análisis de las imágenes partiendo de la saturación de una versión JPG modificada, permitiendo el amplio desarrollo de la investigación.

15. CRONOGRAMA DE ACTIVIDADES

Tabla 12. Cronograma de actividades

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
1		Establecer el levantamiento de información y marco conceptual de la formación de imágenes producidas por dispositivos móviles y los diferentes formatos manejados en ello	15 días	jue 19/05/16
2		Identificación de aplicabilidad del algoritmo usado en la técnica ELA	7 días	jue 19/05/16
3		Identificación de los principales metadatos usados en las imágenes producidas por dispositivos móviles	3 días	sáb 28/05/16
4		Establecimiento de la herramienta a usar para la aplicación de la técnica ELA.	5 días	mié 01/06/16
5		Establecer la necesidad del estudio forense en dispositivos móviles y elementos que se encuentra involucrados en la adquisición y creación de imágenes	30 días	jue 09/06/16
6		Características del formato JPEG	7 días	jue 09/06/16
7		Herramientas para verificación de modificaciones	14 días	sáb 18/06/16
8		Análisis de metadatos en una imagen JPEG	10 días	jue 07/07/16
9		Identificar los diversos procesos de tratamiento de imágenes y técnicas de análisis forense de imágenes	60 días	jue 21/07/16
10		Desarrollo del banco de imágenes	15 días	jue 21/07/16
11		Aplicación estadística del análisis ELA sacado del banco de imágenes	45 días	jue 11/08/16
12		Documentar la aplicación de la técnica error level analysis y metadatos para el estudio forense de imágenes producidas por dispositivos móviles y aplicar dicha técnica para análisis de un banco de imágenes.	30 días	jue 13/10/16



Fuente: Autor

CONCLUSIONES

La aplicación de la técnica Error Level Analysis (ELA) es de gran importancia para la validación de evidencia digital el cual da solución al análisis de la imagen para encontrar modificaciones en ella por lo que se puede incluir en la resolución de problemas digitales para dar con la originalidad de la misma.

ELA es de gran ayuda para comprobar la originalidad de una imagen proveniente de un dispositivo móvil, cabe recalcar que dicha técnica solo fue diseñada para el formato JPG o JPEG, por lo que no resulta ser tan eficiente realizar el análisis fuera de una extensión diferente a las mencionadas con anterioridad.

El análisis de los resultados de los metadatos encontrados en el formato JPG, puede variar al momento de encontrar las cabeceras Exif, es decir este tipo de información depende de la implementación del fabricante de cada dispositivo móvil, por lo tanto, se concluye que si la imagen proviene de un móvil marca Iphone de última generación o HTC es posible que los datos de generación Exif se encuentren incompletos, lo que es un excluyente al momento de realizar un análisis de metadatos.

La implementación del algoritmo ELA en la herramienta GIMP de libre distribución permite realizar un desarrollo limpio y libre de imposiciones que implica usar otro tipo de software por lo que, al momento de implementarlo, se debe tener un equipo avalado para correr este tipo de pruebas ya que puede consumir significantes recursos del computador, se debe implementar en máquinas que optimicen el funcionamiento de la herramienta. Los resultados de imagen que arroja la herramienta GIMP por medio del algoritmo son de muy buena calidad, es por eso que el tamaño de la imagen resultante puede ser hasta 6 veces mayor que la imagen original, esto se da por que la imagen que se guarda en el buffer de GIMP debe ser tratada con saturación de luminancias, esto aumenta la calidad de la imagen para que al final se pueda observar las modificaciones a partir de un brillo con saturación diferente a la uniformidad de la imagen original.

El tratamiento de los metadatos en una imagen es de vital importancia para la conclusión de los resultados finales del análisis forense, es por eso que hace necesario saber e interpretar el resultado que puede dar la herramienta propuestas Exiftool, el cual se concluye que este tipo de información es muy sensible al momento de manipularlo, ya que se puede borrar muy fácilmente.

BIBLIOGRAFÍA

OROS ESCUSOL, David. Lightroom 3 Edición de fotografía digital: La importación. Bogotá: RC Libros, 2010. 23p

KRISS, Michael. Handbook of Digital Imaging. Stanford: John Wiley & Sons, 2015. 31p

BERNAL TORRES, Cesar Augusto. Metodología de la investigación.México: Pearson Educación, 2006. 110p.

CERON. Metodologías de investigación social. Chile: LOM Ediciones,2006

FONG KWONG, Weng "Captura de imagen en una cámara digital". {En línea} { 25 de Sep. de 2011} disponible en: (http://www.chw.net/2011/05/captura-de-imagen-en-una-camara-digital-chwonders/).

GONZÁLEZ, Woods. Tratamiento digital de imágenes. USA: Addison-Wesley.

NICK, "Image Compression: How JPEG Works". {En línea} {11 de Mayo de 2013} disponible en: (http://nboddula.blogspot.com.co/2013/05/image-compression-how-jpeg-works.html).

KRAWETZ, Neal "Full Coverage". {En línea} disponible en: (http://www.hackerfactor.com/blog/index.php)

"Guide To Photo Metadata Fields". {En línea} disponible en: (http://www.photometadata.org/meta-resources-field-guide-to-metadata#Image Supplier ID).

BEJORK, Gail " Viewing and using EXIF data". {En línea} disponible en: (http://www.digicamhelp.com/glossary/exif-data/).

WAGNER, Richard "Los 12 principales mitos sobre los metadatos incrustados en las fotos". {En línea} {18 de Noviembre de 2010} disponible en: (http://www.controlledvocabulary.com/blog/top-metadata-myths.html)

Exchangeable image file format for digital still cameras:Exif Version 2.2. JEITA CP-3451, 2002

BIGAS. "Editores Fotográficos (GIMP) y datos Exif". {En línea} {11 de Septiembre de 2011} disponible en: (http://jmbigas.blogspot.com.co/2011/09/editores-fotograficos-gimp-y-datos-exif.html).

“Datos EXIF”. {En línea} {2015} disponible en: (http://www.thewebfoto.com/2-hacer-fotos/218-datos-exif).

BERROCAL, Lucia. Software para análisis automático de ficheros de imagen. Madrid. Universidad Politécnica, 2012.

“El tutorial de Python”. {En línea} disponible en: (http://docs.python.org.ar/tutorial/pdfs/TutorialPython2.pdf).

“GPS Attribute Information”. {En Linea} disponible en: (http://www.opanda.com/en/pe/help/gps.html#GPSAltitudeRef).

“Metadata reference tables”. {En Linea} disponible en: (http://www.exiv2.org/tags-xmp-tiff.html).

“http://www.exiv2.org/tags-xmp-tiff.html”. {En Linea} disponible en: (http://superuser.com/questions/994666/what-fields-in-exif-files-provide-image-height-width-information)

ANEXOS

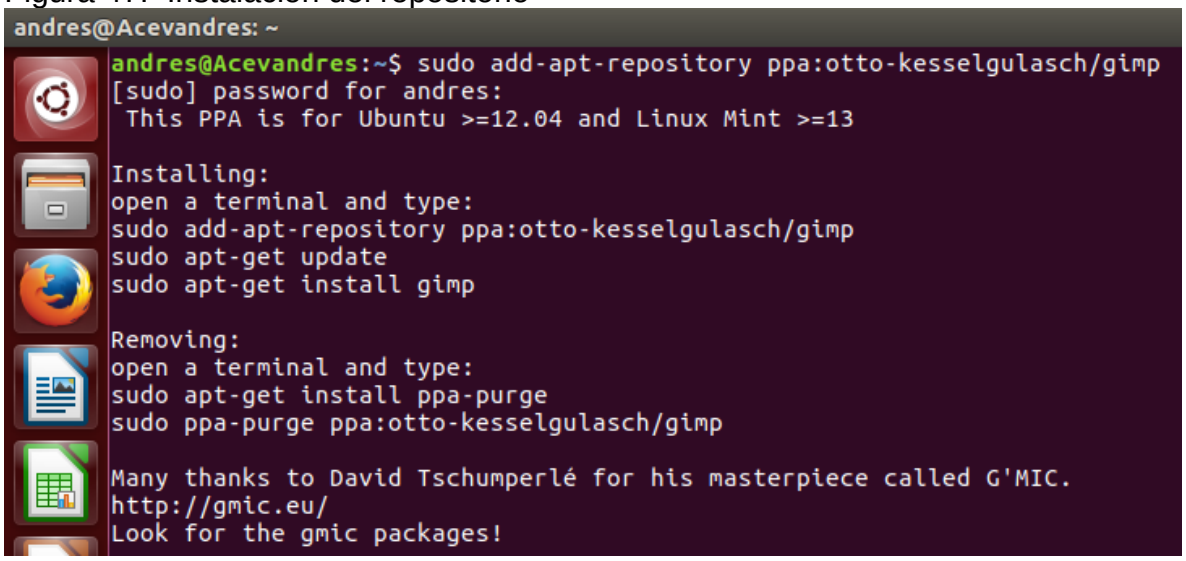
Anexo A. Manual de instalación de GIMP 2.8 en Ubuntu

Para el funcionamiento correcto de la herramienta GIMP, es necesario seguir los siguientes pasos, con el fin de seguir el conducto necesario para el análisis de una imagen digital para poder aplicar la técnica ELA:

1. Se debe abrir la consola de comandos de Ubuntu y colocar el siguiente comando para anexar el repositorio de descarga de la herramienta GIMP.

Sudo add-apt-repository ppa:otto-kesselgulasch/gimp

Figura 47. Instalación del repositorio



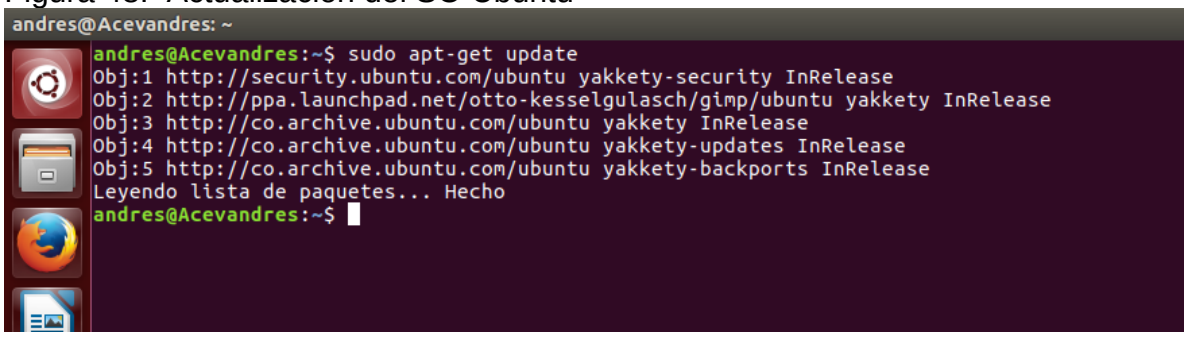
Fuente: El Autor

2. Una vez descargado el repositorio de la herramienta, se debe actualizar el SO ejecutando el comando a continuación

Sudo apt-get update

En la figura a continuación se observa la instalación de los paquetes descargados de los repositorios, el tiempo de instalación de las actualizaciones depende de la versión de Ubuntu que se encuentra instalada.

Figura 48. Actualización del SO Ubuntu

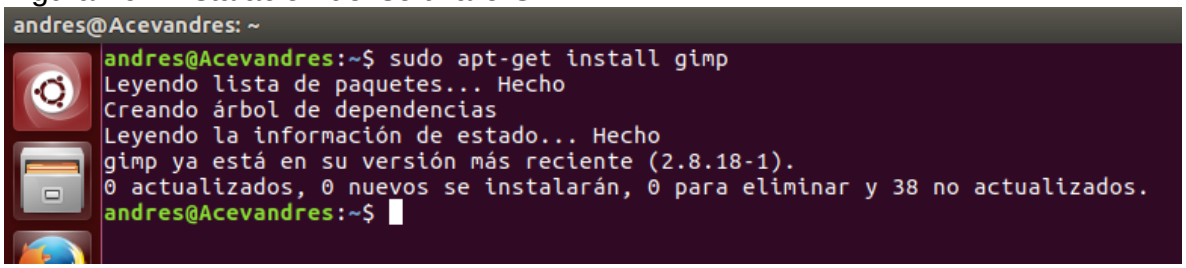


Fuente: El Autor

3. A continuación, después de que se haya realizado la instalación de las actualizaciones, se debe instalar el paquete de instalación de GIMP a partir del siguiente comando.

Sudo apt-get install gimp

Figura 49. Instalación del software GIMP



Fuente: El Autor

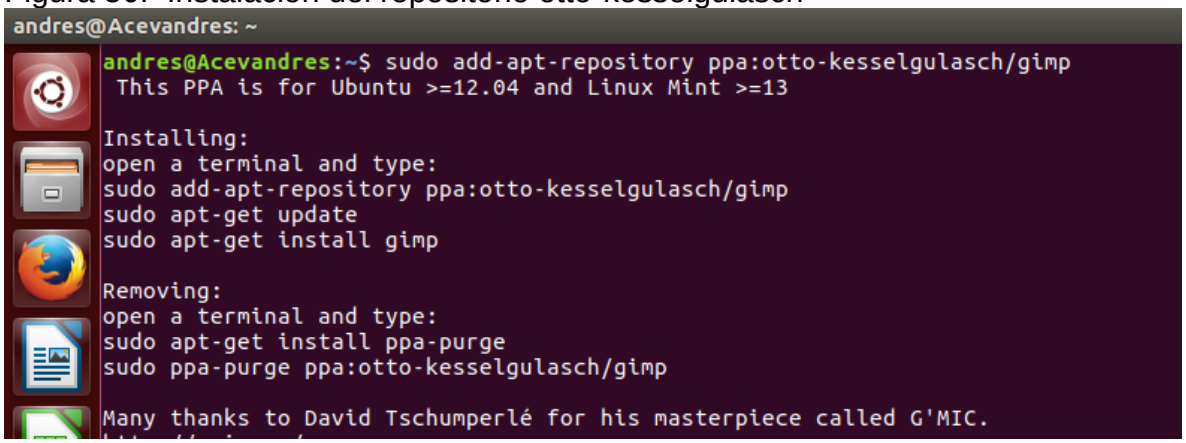
Si se tiene el software instalado, muestra una aviso como el de la imagen “gimp ya está en su versión más reciente …” de lo contrario se cargaran los paquetes de instalación con un tiempo estimado de 5 minutos dependiendo de la velocidad del PC

4. Una vez instalado el software GIMP, es imprescindible realizar el registro de la herramienta ya que sin esta no funcionaría correctamente, por lo tanto se vuelve a incluir el siguiente repositorio

Sudo add-apt-repository ppa:otto-kesselgulasch/gimp

En la siguiente imagen se observa la instalación del repositorio otto-kesselgulasch en los directorios del sistema de Ubuntu.

Figura 50. Instalación del repositorio otto-kesselgulasch

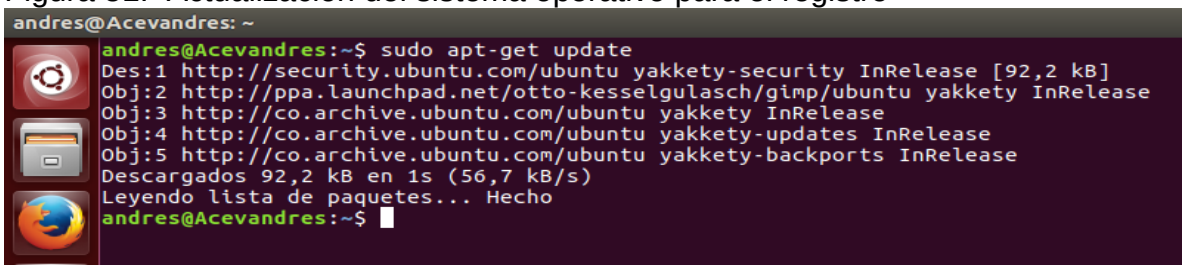


Fuente: El Autor

5. Nuevamente se realiza actualización del SO Ubuntu para bajar los paquetes de registry

Sudo apt-get update

Figura 51. Actualización del sistema operativo para el registro

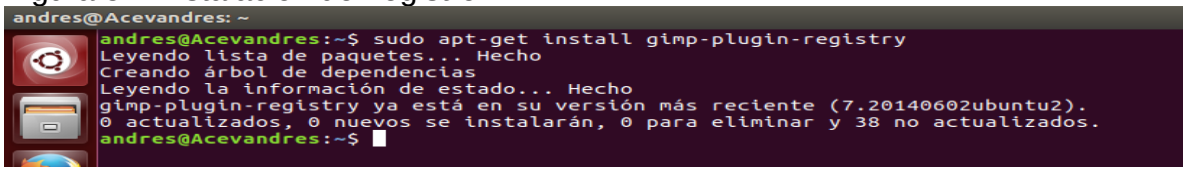


Fuente: El Autor

6. Como último paso se debe instalar los registros con el siguiente comando

Sudo apt-get install gimp-plugin-registry

Figura 52. Instalación del registro



Fuente: El Autor

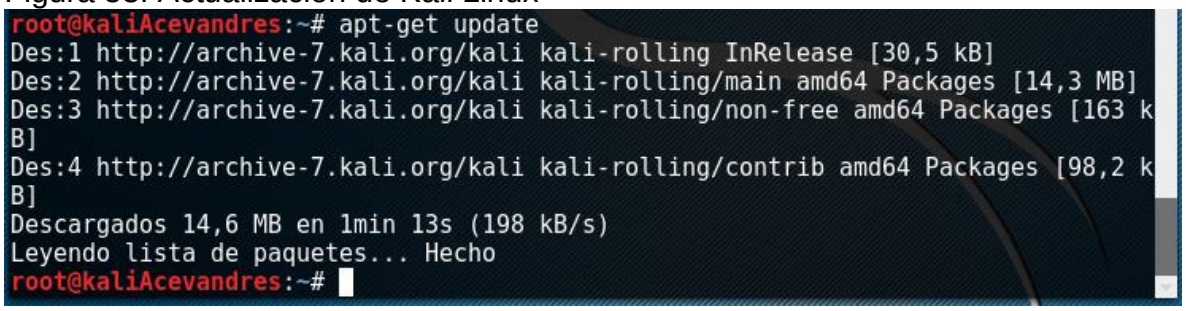
Anexo B. Proceso de instalación de Exiftool en Kali Linux

Para poder llevar a cabo la instalación de la herramienta Exiftool en la herramienta de testing Kali Linux, hace necesario realizar los siguientes pasos:

1. Inicialmente la herramienta aún no está instalada en el sistema operativo, por lo que se debe digitar el siguiente comando en el CLI del SO para realizar la actualización correcta de Kali Linux

Apt-get update

Figura 53. Actualización de Kali Linux

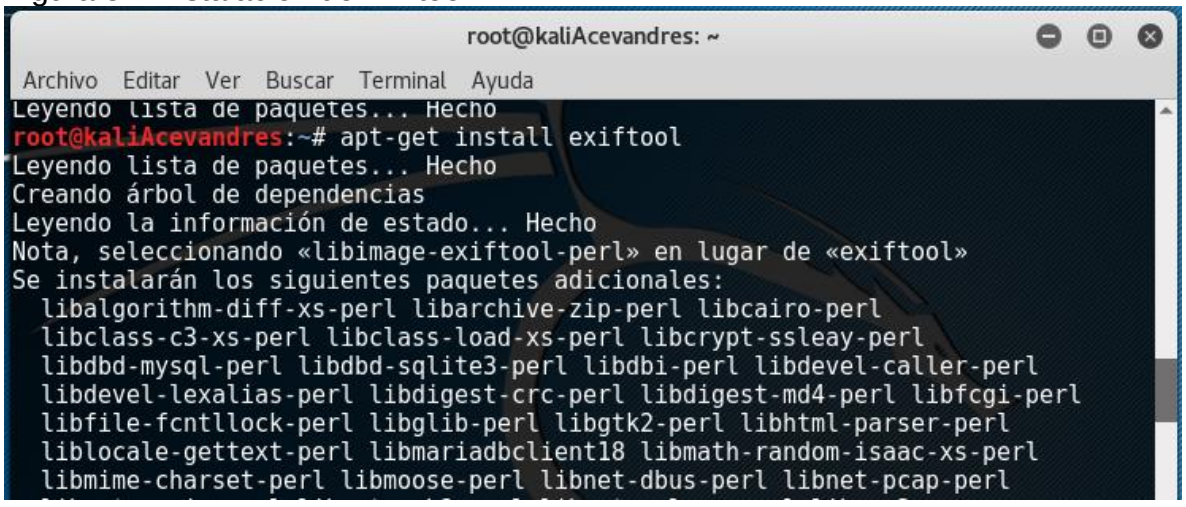


Fuente: El Autor

2. Luego de realizar la correspondiente actualización se debe ejecutar el siguiente comando para instalación de la herramienta Exiftool.

Apt-get install exiftool

Figura 54. Instalación de Exiftool



Fuente: El Autor