



INSTITUTO POLITÉCNICO NACIONAL



**ESCUELA SUPERIOR DE INGENIERÍA
MECÁNICA Y ELÉCTRICA**

**SECCIÓN DE ESTUDIOS DE POSGRADO E
INVESTIGACIÓN**

UNIDAD CULHUACAN

Análisis forense en imágenes digitales

T E S I S

QUE PARA OBTENER EL GRADO ACADÉMICO DE

**MAESTRO EN CIENCIAS DE INGENIERÍA EN
MICROELECTRÓNICA**

PRESENTA

Marcos Arturo Rosales García

ASESOR: M. en C. Rubén Vázquez Medina

MÉXICO D.F.

Junio 2008



SIP-14

INSTITUTO POLITECNICO NACIONAL
SECRETARIA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México D. F., siendo las 18:30 horas del día 20 del mes de JUNIO del 2008 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULHUACAN para examinar la tesis de grado titulada:

"ANÁLISIS FORENSE EN IMÁGENES DIGITALES"

Presentada por el alumno:

ROSALES

Apellido paterno

GARCÍA

materno

MARCOS ARTURO

nombre(s)

Con registro:

B	0	5	1	3	7	5
---	---	---	---	---	---	---

aspirante al grado de:

MAESTRÍA EN CIENCIAS DE INGENIERÍA EN MICROELECTRÓNICA

Después de intercambiar opiniones los miembros de la Comisión manifestaron **SU APROBACIÓN DE LA TESIS**, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director de tesis

M. EN C. RUBÉN VÁZQUEZ MEDINA

DRA. MARIKO NAKANO MIYATAKE

DR. GONZALO ISAAC DUCHEN SÁNCHEZ

DR. JUAN CARLOS SÁNCHEZ GARCÍA

DR. GABRIEL SÁNCHEZ PÉREZ

S. E. P.
SECCIÓN DE ESTUDIOS DE
POSGRADO E INVESTIGACIÓN
EL PRESIDENTE DEL COLEGIO

DR. HÉCTOR MANUEL PÉREZ MEANA



INSTITUTO POLITECNICO NACIONAL
SECRETARIA DE INVESTIGACION Y POSGRADO

CARTA DE CESIÓN DE DERECHOS

En la Ciudad de México D. F., el día 20 del mes de junio del año 2008, el (la) que suscribe Marcos Arturo Rosales García alumno (a) del Programa de MAESTRÍA EN CIENCIAS DE INGENIERÍA EN MICROELECTRÓNICA, con número de registro B051375, adscrito a SEPI-ESIME-CULHUACAN, manifiesta que es autor (a) intelectual del presente trabajo bajo la dirección del M. en C. Rubén Vázquez Medina y cede los derechos del trabajo titulado ANÁLISIS FORENSE EN IMÁGENES DIGITALES, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y / o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección marcosrosales@gmail.com .

Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Marcos Arturo Rosales García

Agradecimientos:

Quiero dedicar este trabajo a mis padres porque siempre han sido un ejemplo para mí, porque siempre me han brindado su apoyo incondicional y porque los quiero con todo mi corazón. También quiero dedicar este trabajo a mi abuelita a quien quiero, respeto y admiro mucho, te amo mamá. A mis hermanos por siempre alentarme y apoyarme. A todos ustedes éste logro también es suyo.

Quiero agradecer al Instituto Politécnico Nacional, particularmente a la Sección de Estudios de Posgrado e Investigación de la ESIME Culhuacan, al Consejo Nacional de Ciencia y Tecnología.

Doy gracias a todos mis amigos y compañeros con los que he compartido muy buenos momentos en el transcurso de estos años, gracias Susana por siempre alentarme a seguir adelante.

Un agradecimiento a todos los profesores del posgrado especialmente a mi asesor M. en C. Rubén Vázquez Medina.

Índice

Resumen

Abstract

Presentación

Objetivo

Definición del problema

Justificación

Estado del arte

Capítulo I: Introducción al análisis forense de imágenes digitales

1.1 Introducción	1
1.2 Falsificación	2
1.3 Marcas de agua	5
1.4 Análisis forense	7
1.5 Contribución	10

Capítulo II: Mejores prácticas recomendadas internacionalmente

2.1 Introducción	12
2.2 Entidades internacionales	12
2.3 Recomendaciones SWGIT	13
2.4 Mejorar la imagen	15
2.5 Restauración de la imagen	17
2.6 Compresión de una imagen	17
2.7 Análisis sobre imágenes digitales	18
2.8 Tipos específicos de análisis forense en imágenes	19
2.9 Guía de procedimientos para el procesamiento de imágenes digitales	21
2.10 Recomendaciones INTERPOL	22
2.11 Comentarios del capítulo	23

Capítulo III: Análisis de zonas clonadas en una imagen digital

3.1 Introducción	25
3.2 Adquisición de la imagen con la cámara digital	25
3.3 Composición de la imagen	28
3.4 Falsificación mediante clonación de zonas	29
3.5 Identificar falsificación en imagen	31
3.6 Resultados	33

Capítulo IV: Análisis de la imagen mediante la dirección de la luz

4.1 Introducción	36
4.2 Manipulación de la imagen	36
4.3 Efecto de la luz en la fotografía digital	37

4.4 ¿Por qué un objeto puede ser más o menos transparente?	38
4.5 Generación de sombra	38
4.6 Metodología	39
4.7 Desarrollo de la metodología propuesta	40
4.7 Conclusiones	45
Bibliografía	48
Lista de tablas y figuras	50
Anexo	
Publicaciones y ponencias.	51

Resumen

En esta tesis se presentan herramientas y un procedimiento para el análisis forense en imágenes digitales, capaces de identificar falsificaciones y manipulaciones en ausencia de marcas de agua o hardware especializado. Estas herramientas funcionan asumiendo que las imágenes contienen propiedades y características específicas de una gran variedad de fuentes, como el ambiente del cual la imagen es capturada, y el proceso de formación de la imagen en la cámara. Estas propiedades pueden ser alteradas al falsificar una imagen y al estimar éstas se puede determinar la autenticidad o no de una imagen. En este contexto se presenta una herramienta forense y procedimientos que explotan dichas debilidades en las imágenes falsificadas.

Abstract

In this work we present the tool and a procedure for forensic analysis on digital images, capable to identify forgeries and manipulations in the absence of water marks or specialised hardware. This tool works assuming that the images contain properties and specific characteristics of a variety of sources, such as the environment from which the picture was taken, or the process of formation of the image in the camera. These properties can be altered while forging an image, but they can also establish if the image is authentic or not. In this context the forensic tools and the procedures that exploit those weaknesses in the forged images are presented.

Presentación

En esta tesis se presenta una herramienta forense basada en un algoritmo desarrollado en este trabajo y procedimientos capaces de detectar rastros de falsificación en imágenes digitales, aun sin el uso de marcas de agua o hardware especializado. Estas herramientas trabajan asumiendo que las imágenes contienen propiedades o características que pueden ser extraídas y cuantificadas de diversas fuentes, como el lente de la cámara, el ambiente en que fue capturada la imagen y el sensor. Estas propiedades se pueden corromper cuando se busca falsificar una imagen con algún software de edición. En este contexto se analizan las recomendaciones hechas por grupos especializados en el análisis de imágenes y se hacen las consideraciones pertinentes para aplicarlas en un proceso forense. Con base en ello, se propone un algoritmo que permite hacer un análisis por clonación de zonas y un procedimiento de análisis geométrico que permite determinar la autenticidad/integridad de una imagen considerando como referencia la dirección de la luz en la imagen. Tanto las técnicas como la herramienta presentada en esta tesis, trabajan en imágenes con ciertas características y no se aplican a cualquier imagen, para el caso del análisis geométrico en la imagen se requiere que la imagen a analizar presente sombras que puedan ser delimitadas para su medición y diferentes objetos que puedan ser usados¹. Para poder usar el algoritmo de detección de zonas clonadas, es necesario que al menos existan bloques de 4x4 pixeles que sean idénticos dentro de la imagen, en caso contrario el algoritmo no detectará nada. Al combinar la técnica de análisis geométrico con la herramienta de detección de zonas clonadas se pueden obtener mejores resultados y robustecer la identificación si una imagen es auténtica/integra o no.

¹ Para hacer comparación entre el ángulo de cada uno de ellos.

Objetivo

Aplicar el proceso forense y las mejores prácticas recomendadas internacionalmente para encontrar las evidencias que permitan determinar si una imagen digital es o no auténtica, usando para ello técnicas de correlación de patrones y técnicas geométricas de análisis sobre la imagen que se analiza.

Definición del problema

Las cámaras digitales, cada día más potentes y económicas, y el software de edición de imágenes disponible brindan la facilidad para manipular una imagen de forma casi imperceptible.

En la actualidad las imágenes son una fuente de información sumamente importante, existe un dicho que dice “Una imagen dice más que mil palabras”. Una imagen es mucho más representativa que las palabras o la descripción que se pueda hacer referente a un suceso. La mayoría de la información que manejamos a lo largo del día tiene una imagen representativa. Las imágenes que vemos cotidianamente van desde imágenes con fines publicitarios, investigación, tecnología, hasta imágenes que representan la noticia del día. Habrá algunas imágenes que por el tipo de información que representan no importará si han sido retocadas o no. Sin embargo, en otras imágenes es necesario garantizar su autenticidad². Imagine una imagen publicitaria cuya intención es vender un producto de consumo general, dicha imagen es muy probable que haya sido retocada para hacerla más atractiva a la vista de los potenciales clientes. Este tipo de imágenes no requieren ser analizadas buscando garantizar que sean auténticas/integras. Por otro lado, existen imágenes que representan información sumamente sensible y que se tiene que garantizar que dicha imagen se encuentra en un estado auténtico e íntegro, por ejemplo, la imagen que se publicó en diferentes medios de comunicación, en la cual se podía ver la silueta de un hombre sentado sobre unas rocas y se decía que era un hombre en Marte³, Figura 1.1, imágenes como esta influyen en la percepción de la mayoría de la gente y contribuyen a formar la opinión de diferentes tópicos en la vida diaria. Es entonces cuando surge la necesidad de contar con herramientas, metodologías y procedimientos que auxilien en la identificación de imágenes manipuladas.

² En lo sucesivo se entenderá que la autenticación de imágenes por medio de análisis forense es la aplicación de ciencias de la imagen y el dominio de expertos para discernir si la imagen presentada está en su formato original, esto con base en algunos criterios predefinidos como la fotogrametría, colorimetría, etc.

³ http://news.cnet.com/2300-11397_3-6227262-1.html

Justificación

Las imágenes digitales se pueden observar en cualquier medio de comunicación, revistas, diarios, televisión, etc. Es una forma visual de representar sucesos o eventos que acontecen diariamente. Existen algunas imágenes que por el tipo de información que representan será necesario garantizar su autenticidad e integridad y de no ser por el uso de marcas de agua actualmente no existe en el mercado una herramienta que permita determinar la autenticidad de una imagen.

Imagine la creación de una imagen en la cual se muestra a dos rivales políticos conviviendo de forma muy amigable entre ellos; o imagine una imagen donde se pretenda inculpar a una persona de haber estado en un lugar donde nunca estuvo y en el que se llevó acabo un crimen. Las consecuencias para los inculpados podrían ser muy serias, es por ello que se requiere de mecanismos que permitan determinar si una imagen es o no auténtica. El presente trabajo ayuda en esa labor, proponiendo herramientas y mecanismos que ayuden a garantizar la autenticidad de una imagen.

Estado del Arte

Existen algunos trabajos al respecto del análisis forense en imágenes digitales. A continuación se mencionan algunos de los más destacados:

- Hany Farid, **Digital Image Forensics**, American Academy of Forensic Sciences, Washington, DC, 2008

En este artículo se trata de forma genérica la falsificación de imágenes digitales, haciendo énfasis en las consecuencias de estos actos, y se trata el uso de marcas de agua como sistema de identificación en la autenticidad de una imagen.

- Micah K. Johnson, **Lighting and Optical Tools for Image Forensics**, (advisor: H. Farid), Ph.D. Dissertation, Department of Computer Science, Dartmouth College, 2007

En este trabajo se presenta una herramienta de análisis forense en imágenes digitales, la cual funciona en ausencia de marcas de agua. Dicha herramienta explota las propiedades ópticas y de luz contenidas en la imagen.

- M.K. Johnson and H. Farid, **Exposing Digital Forgeries in Complex Lighting Environments**, IEEE Transactions on Information Forensics and Security, 2(3):450-461, 2007

Se describe una técnica para demostrar que una imagen es falsa con base en la detección de inconsistencias en la luz. Se demuestra como acercarse a un ambiente complejo de luz mediante modelado en 3D y dicho modelo es usado para determinar las inconsistencias de luz en una imagen, como los diferentes niveles de luminosidad en una misma imagen.

- M.K. Johnson and H. Farid, **Exposing Digital Forgeries Through Specular Highlights on the Eye**, 9th International Workshop on Information Hiding, Saint Malo, France, 2007

Este trabajo presenta una técnica de análisis que explota las condiciones de luz, así como la reflexión de la luz en el ojo, cuando se trata de ambientes cerrados y se usó flash para capturar la imagen. Se analiza si dos ó más personas que aparecen en una foto siempre estuvieron juntas, y dicho análisis se hace con base en las condiciones de luz presentada en cada una de las personas, así como el ángulo de reflexión de la fuente de luz en los ojos de cada una de las personas fotografiadas.

- H. Farid, **Digital Doctoring: can we trust photographs?**, In *Deception: Methods, Motives, Contexts and Consequences*, 2007

El artículo aborda el tema de la credibilidad que se le puede tener a una imagen. Muestra como las fotografías han sido manipuladas desde los primeros días de las mismas, y como las técnicas de falsificación han evolucionado hasta nuestros días.

- Lukas, J., J. Fridrich, and M. Goljan . **Digital camera identification from sensor noise**. IEEE Transactions on Information Security and Forensics 1(2), 205–214. 2006

Se presenta una forma de detección de alteraciones en imágenes digitales asumiendo que se poseen imágenes tomadas de la misma cámara con la que se tomó la imagen que se está analizando. Este método se basa en detectar patrones de ruido en algunas regiones de la imagen, creados por la cámara, única característica estocástica presentada por el sensor Charged Couple Device (CCD).

- Jessica Fridrich, David Soukal, and Jan Lukáš, **Detection of Copy-Move Forgery in Digital Images**, Department of Electrical and Computer Engineering, Department of Computer Science SUNY Binghamton, Binghamton, NY 13902-6000

Se analiza una forma específica de falsificar una imagen, mediante el análisis de porciones copiadas y pegadas en la misma imagen con la intención de eliminar información de la imagen. Se analiza el problema de copiar y pegar segmentos de una misma imagen, y se describe un método para la identificación de este fenómeno.

- **Best Practices for image authentication⁴**, Scientific Working Group on Imaging Technology (SWGIT). 2007

Este trabajo trata sobre las recomendaciones para hacer un análisis de las imágenes digitales en busca de errores que demuestren su autenticidad o no. Su propósito es proveer recomendaciones y guías para el uso de imágenes digitales en un proceso judicial, las cuales se han elaborado a partir de las mejores prácticas recomendadas internacionalmente. El objetivo de estas

⁴ http://www.theiai.org/guidelines/swgit/guidelines/section_14_v1-0.pdf

recomendaciones es asegurar el éxito de una imagen al ser presentada como evidencia en un proceso judicial ante una corte.

- **2004 Digital Image Integrity (Imaging Forensics INC.)⁵.**

Este trabajo hace una recomendación de políticas o reglas que proveen una guía de procedimientos en este caso para mantener la integridad⁶ de las imágenes digitales, un punto a considerar dentro de las mejores prácticas recomendado en este trabajo es lo siguiente: Archivar la imagen o generar la cadena de custodia de dicho archivo, control de procesos aplicados a la imagen, poder repetir los procesos que le fueron aplicados a la imagen.

⁵ <http://forensicimaging.com/v1.3>

⁶ La integridad en los sistemas de información se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc.

Capítulo I

Introducción al análisis forense de imágenes digitales.

1.1 Introducción.

Las imágenes digitales están en todos lados, en las portadas de las revistas, en periódicos, en los medios de comunicación, Internet, etc. Todos los días tenemos contacto con estas imágenes, la mayoría de las imágenes que vemos a diario son manipuladas para tener un mejor aspecto; dichas imágenes son creadas con fines publicitarios, pero hay algunas imágenes que por lo importante de la información que representan se tiene que garantizar su autenticidad. Dada la facilidad con que las imágenes digitales pueden ser manipuladas muchas de las veces no podemos tener la certeza de que lo que estamos viendo es real o se trata de una imagen que ha sido manipulada.

En los últimos años, la falsificación de imágenes ha afectado la ciencia, la política, los medios de comunicación y algunos negocios. Cada vez está más cercano el día en que todas las imágenes que se tengan como evidencia en un proceso judicial sean digitales y esto a causa de la facilidad de adquirir una cámara digital o los mismos teléfonos celulares que cuentan con cámaras integradas, hacen fácil la captura de imágenes digitales. La percepción que la gente pueda tener de algunas imágenes será extremadamente sensible, ya que muchas imágenes podrán servir como prueba de algunos sucesos o eventos importantes; por ejemplo, la figura 1.1 muestra la polémica imagen de una silueta de hombre en el planeta Marte, dicha imagen fue foco de muchos noticieros a principios del año 2008, esta imagen fue captada por una sonda espacial de la National Aeronautics and Space Administration (NASA), pero la autenticidad de dicha imagen aun está en duda.



Figura 1.1 Foto captada por una sonda espacial enviada a Marte por la National Aeronautics and Space Administration, en ella se puede ver una silueta con forma de humano.

Aun cuando la falsificación de imágenes no es un problema nuevo, las herramientas que actualmente se usan para hacer dichas falsificaciones si lo son, tal es el caso de cámaras digitales, computadoras, software de edición de

imágenes, escáner y todos los dispositivos de tratamiento de imágenes que se han sofisticado de forma exponencial en los últimos años, esto ha traído consigo la facilidad para que casi cualquier persona pueda realizar una falsificación de buena calidad sin necesidad de ser un especialista en la manipulación de imágenes digitales. Por otro lado las herramientas para detectar que una imagen ha sido alterada de su estado original son prácticamente inexistentes en el mercado, y no hay muchas opciones para autenticar la originalidad o no de una imagen digital.

1.2 Falsificación

El arte de crear una imagen falsa es tan viejo como la fotografía misma. En los primeros años la fotografía rápidamente se convirtió en el método que la mayoría escogía para tener un retrato, así los fotógrafos de la época aprendieron que podían mejorar sus ventas si conseguían manipular de forma adecuada dichas fotografías.



Figura 1.2 se muestra (a) la fotografía original de Lenin y Trotsky, y (b) muestra la imagen alterada en donde Trotsky y otro individuo fueron removidos.

En la figura 1.2 se muestra un claro ejemplo de la falsificación de fotografías desde el principio de la fotografía misma. En el ejemplo de la Figura 1.2 se ve a un par de personajes de la Unión Soviética, pero al ser un personaje no grato para la vida política de dicho país, Trotsky es removido de muchas de las imágenes que se tenían en los archivos como lo muestra nuestro ejemplo.

La figura 1.3 (a) es una imagen propuesta como una de las imágenes más impactantes del año 2005, fue tomada en las costas africanas en una maniobra del ejercito Ingles, aunque después se descubrió la imagen original¹, en la cual no existe ningún tiburón, y se descubrió la imagen donde aparece el tiburón que fue usado para el fotomontaje figura 1.3 (b).

¹ <http://bl06.net/blog/fake/>



(a)



(b)

(c)

Figura 1.3 es una imagen propuesta como una de las imágenes más impactantes del año 2005, fue tomada en las costas africanas en una maniobra de rescate del ejercito Ingles.

Recientemente se pueden ver numerosos ejemplos de imágenes falsas en periódicos y portadas de revistas. En la figura 1.4 y 1.5 se muestran las portadas de diferentes diarios y revistas donde pueden apreciarse imágenes que fueron manipuladas.

En la figura 1.4 (a) se puede ver una imagen de la guerra de Irak, fue la portada del diario Times de los Angeles CA. Marzo del 2003², y se descubrió que dicha imagen está compuesta por la fusión de dos imágenes³ mostradas en la misma figura 1.4 (b) y (c). El fotógrafo que capturó estas imágenes se llama Brian Walsky. Poco tiempo después de ser publicada su foto envió todas las imágenes a su editor en jefe quien descubrió que Walsky había manipulado las imágenes para crear una imagen de mayor impacto visual, pero en el mundo periodístico alterar la información tiene un costo muy caro ya que se pierde la credibilidad del medio que la difunde, en este caso le costó a Walsky el ser despedido del diario Los Angeles Times.

² <http://www.washingtonpost.com/wp-srv/photo/essays/vanRiper/030409.htm>
³ http://www.poynter.org/content/content_view.asp?id=28082



(a)



(b)

(c)

Figura 1.4 imagen de la guerra de Irak, fue la portada del diario Times de los Angeles CA. Marzo del 2003

En la figura 1.5 (a) se pueden ver la portada de la revista Star Mayo del 2005, en la que se muestra al actor Brad Pit y Angelina Jolie tomados de la mano caminando por la playa, esto cuando Brad Pit recientemente había terminado su compromiso con la actriz Jennifer Aniston, poco tiempo después se dijo que dicha imagen se trataba de un fotomontaje. En la figura 1.5 (b) se ve la portada de la revista New York del mes julio del 2005, en la que se muestra al actor Tom Cruise junto con su esposa Katie Holmes, dicha imagen fue manipulada con el fin de hacerlos ver como un par de psicopatas.



Figura 1.5 portadas de revistas en la que se muestra a artistas en situaciones comprometedoras o embarazosas.

En todos los ejemplos anteriores la autenticidad de las imágenes se pone en entredicho, ¿Cómo se puede decir entonces que una imagen es original, ó como podemos probar que esas imágenes fueron modificadas o tal vez

generadas por computadora?, para dar solución a esta problemática existen básicamente dos opciones: Marcas de agua y análisis forense.

1.3 Marcas de Agua

Una solución que se ha propuesto para autenticar las imágenes digitales son las marcas de agua. La idea consiste en incrustar información dentro de una imagen que puede ser extraída después para verificar su autenticidad. Estas técnicas están siendo implementadas por algunas compañías fabricantes de cámaras digitales, tal es el caso de Epson con su Image Authentication System⁴ y Canon EOS 5D Data Verification Kit DVK-E1⁵. Las dos cámaras generan una marca de agua que se incrusta en la imagen en el momento mismo de ser capturada, así cuando la imagen llega a ser manipulada la información de la marca de agua insertada originalmente cambia. Cuando se requiere autenticar la originalidad de la imagen, esta es analizada con un software especial DVK-E1 que verifica la marca de agua original con la que actualmente tiene la imagen si dicha marca se ha modificado es sinónimo de que la imagen ha sido manipulada.

En la figura 1.6 se puede observar de forma gráfica el proceso que se lleva a cabo para validar la autenticidad de una imagen usando el software Data Verification Kit DVK-E1, desarrollado por la compañía CANON® y que se incluye con algunos modelos de cámaras digitales. El proceso de evaluación es muy simple, primeramente en el momento justo en que es capturada la imagen la cámara genera un código (Marca de agua) que se incrusta en la imagen y posteriormente cuando la imagen requiera ser autenticada será evaluada en una computadora por el Data Verification Kit DVK-E1 y con esto se verificará el código de evaluación, si la marca de agua ha sido corrompida es prueba de que la imagen ha sido alterada de su estado original.

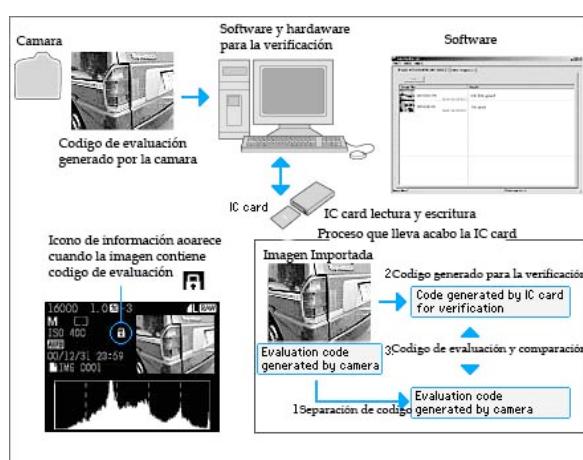


Figura 1.6 Proceso de evaluación de la imagen con el Data Verification Kit DVK-E1.

⁴ http://www.epson.com/cgi-bin/Store/support/supDetail.jsp?BV_UseBVCookie=yes&infoType=Overview&oid=14594

⁵ <http://www.canon.com/camera-museum/tech/report/200211/report.html>

El uso de marcas de agua se ha establecido como sistema de protección de los derechos de propiedad casi desde la invención del papel. Durante muchos años, cualquiera que fabricara un documento u obra de arte valioso lo podía marcar con un sello de identificación o marca de agua (visible o no), para establecer su propiedad, origen y/o autenticidad.

La posibilidad de digitalización de cualquier tipo de información (imágenes, vídeo, audio, texto, etc.) permite realizar copias perfectas de la información digitalizada. Las propias características de la información digital (facilidad de réplica, facilidad de transmisión, facilidad de tratamiento y modificación, etc.) facilitan la falsificación de cualquier archivo digital, incluyendo imágenes, video y audio.

Las técnicas de marcas de agua son utilizadas para la autenticación tanto del distribuidor como del propietario legal, como se explicó anteriormente el DVK-1 la usa para determinar que el original no ha sido alterado de su estado íntegro, en nuestro país se usan marcas de agua en billetes para garantizar su autenticidad.

Esta técnica de protección requiere básicamente dos herramientas:

- Introducción de la firma o marca en la información a proteger (Algunas cámaras Canon® lo hacen al momento de tomar la foto).
- Extracción e identificación de la marca (con el Data Verification Kit DVK-E1, se carga la imagen en una computadora y se analiza)⁶.

Una marca de agua es un código de identificación imperceptible que puede extraerse para verse o escucharse, que puede contener información acerca del propietario, de los derechos de autor, el creador, el usuario autorizado, el número de copias o reproducciones autorizadas, etc⁷.

Los sistemas de marcas de agua digitales para imágenes se basan en introducir la marca en las componentes espectrales perceptiblemente significativas de una imagen, que son las bajas frecuencias. Ahora bien, la modificación de dichas componentes a de ser lo suficientemente pequeña como para que no se pueda percibir a simple vista (característica de invisibilidad de la "marca de agua"), pero al ser extraída y analizada dicha marca de agua debe ser identificable la manipulación de la imagen.

La robustez⁸ de una marca de agua se refiere a que debe ser difícil de eliminar o de ser distorsionada hasta el punto de hacerse indetectable. En particular, una marca de agua debe ser robusta frente a: Análisis estadísticos como, por ejemplo, un filtro de Kalman (para imágenes); procesamientos comunes de la señal, como por ejemplo conversiones A/D, D/A, remuestreo, recuantificación, compresión, etc.; distorsiones geométricas: rotación,

⁶ <http://www.canon.com/camera-museum/tech/report/200211/report.html>

⁷ <http://www.iec.csic.es/cryptonomicon/articulos/expertos64.html>

⁸ <http://www.iec.csic.es/cryptonomicon/articulos/expertos64.html>

traslación, recortes y cambios de escala (para imágenes); y falsificación, esto es, ante la combinación de copias de un mismo documento. La clave fundamental para hacer que una "marca de agua" sea robusta es introducirla en las componentes perceptiblemente más significativas de la señal o de su espectro. Para hacer análisis de integridad en una imagen es recomendable usar marcas de agua frágiles⁹, ya que si la imagen ha sido alterada, la marca de agua se alterará y al extraerla se verificará que dicha imagen fue manipulada. Una marca de agua frágil que tiene que probar la autenticidad de los datos de una imagen no tiene que ser robusta contra técnicas de procesamiento o alteraciones intencionadas de los datos de la imagen, ya que el fallo para detectar la marca de agua prueba que los datos del archivo imagen han sido modificados y consecuentemente no es auténtico. La ambigüedad se refiere a que la probabilidad de un falso positivo en la detección de la marca ha de ser muy baja. La imperceptibilidad dependerá del sentido receptor (vista, oído), y se referirá siempre a la comparación con la original.

1.4 Análisis Forense

En el sub índice 1.2 del presente se ha visto como las marcas de agua, aún cuando no fueron diseñadas para ello pueden ayudar a garantizar la autenticidad de una imagen. El problema es que muy pocas cámaras digitales cuentan con el sistema de marcado de agua, y normalmente son las cámaras más costosas del mercado¹⁰ por lo tanto no son de uso popular. En ausencia de las marcas de agua y hardware especializado que permitan identificar si una imagen digital ha sido alterada de su estado original, deben existir opciones alternas para identificar la integridad de una imagen digital, la informática forense ha venido trabajando desde hace ya algunos años en la identificación y prosecución de delitos informáticos, el análisis forense a imágenes digitales es entonces la forma existente de identificar si una imagen digital ha sido manipulada. Este análisis consiste en identificar las irregularidades presentadas en la imagen tanto a nivel visual, como de la información que compone a la imagen como es el caso del valor de los píxeles. Es preciso señalar que de no ser por la implementación de marcas de agua, no existe una herramienta ni procedimiento único que permita determinar que una imagen digital ha sido alterada. Mediante un conjunto de técnicas estadísticas y análisis en la imagen se pueden detectar rastros de que una imagen digital ha sido alterada. Estas técnicas sirven para cuando no hay una marca de agua ó firma que pueda ayudar a determinar de una forma más rápida si la imagen ha sido modificada. El trabajo de estas técnicas consiste primeramente en identificar los cambios estadísticos asociados a la manipulación de imágenes, así pues las técnicas estadísticas que se pretenden usar estarán diseñadas para estimar estos cambios. A continuación se definen

⁹ Una marca de agua frágil es aquella que al ser insertada en un fichero y este ser manipulado la marca de agua frágil se alterará fácilmente al momento de extraer dicha marca de agua se nota fácilmente que el fichero fue manipulado.

¹⁰ <http://www.pixmania-pro.com/es/es/canon/eos-5d/135923/accessoire.html>

el tipo de cambios que sufre una imagen al ser alterada y qué tipo de rastro puede dejar.

- **Falsificaciones de Imágenes.** Considerando una falsificación de imagen mediante la unión de dos imágenes. Para crear una imagen convincente de este tipo es necesario hacer las siguientes o alguna de las siguientes modificaciones: cambiar el tamaño, rotar o estrechar las imágenes originales, cualquiera que sea el caso el retoque será necesario en diferentes secciones de la imagen.
- **Manipulación del Arreglo de Filtros de Color (CFA) de imágenes interpoladas.** La mayoría de las cámaras digitales están equipadas con un Charge-couple device (CCD) o un sensor Complementary Metal Oxide Semiconductor (CMOS) y capturan la imagen usando un arreglo de filtros de color. Para cada píxel solo se asigna un color (de tres que son capturados), los colores que no se obtienen al momento de tomar la foto son asignados por los valores entre los pixels vecinos. Este proceso se conoce como CFA interpolación, se introduce una correlación específica entre las muestras tomadas a una imagen de color. Así cuando una imagen es manipulada insertándole información de otra imagen se presentará un fenómeno que se conoce como aberración cromática, y es que el contorno de una figura no tendrá la suavidad que presenta la imagen sobre la que fue pegada, en este objeto será muy marcado el límite dentro de la imagen. En la figura 1.7 se puede observar el proceso por el que pasa una imagen en una cámara digital, así como la información que se procesa en cada una de estas etapas y qué tipo de información puede ser analizada en la imagen una vez capturada en busca de información, que permita identificar irregularidades. Por ejemplo el sensor de la cámara, un CCD típico solo captura uno de los tres canales de color en cada uno de los pixels. Para crear los valores faltantes en la imagen se pasa la información obtenida por un filtro de Bayer o algoritmo de mosaico, que asigna valores dependiendo de la intensidad que envía el sensor a este último. Una vez obtenida esta información se genera una interpolación para llenar los pixels faltantes de la imagen, es aquí donde se genera una correlación en la información contenida en la imagen y puede ser explotada al ser analizada mediante su formato JPEG. Cuando una imagen se manipula esta correlación tiende a perderse, este proceso se lleva a cabo en la zona de cámara presentada en la figura 1.7, esto se verá a detalle en el capítulo tres.

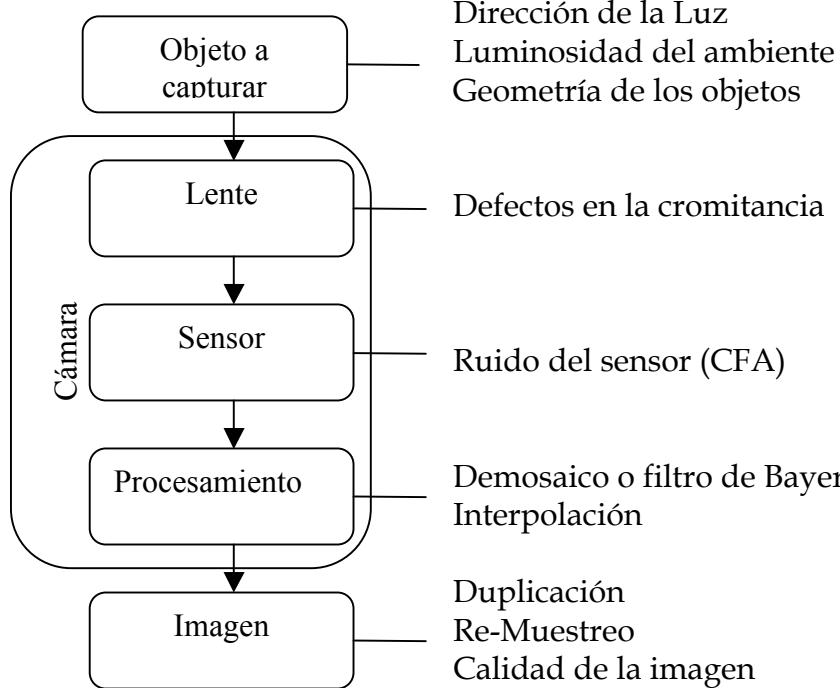


Figura 1.7

- **Doble compresión.** Cuando se quiere retocar una imagen lo primero por hacer es descargar la imagen en algún software de edición de imágenes (Ej. Adobe Photoshop®) después de hacer algunos procesos en el programa se necesita guardar nuevamente para que tome los cambios que se le han hecho a la imagen. Si se usa el formato JPEG, el resultado de la imagen alterada será una doble compresión, la doble compresión de JPEG altera la información estadística de la imagen, por el uso nuevamente de las tablas de cuantización con las que será nuevamente comprimido y esto puede ser identificable.
- **Duplicar Regiones de la imagen.** Una manipulación común es remover a una persona o algún objeto dentro de la imagen, esto requiere un procedimiento de copiar y pegar porciones de la misma imagen, sobre la parte que se desea ocultar, esto es prácticamente imperceptible a simple vista. En el capítulo 3 se estudiará un algoritmo que permite comparar cada uno de los bloques de la imagen para detectar la presencia de regiones duplicadas en la imagen.
- **Patrones de ruido inconsistentes.** Las imágenes digitales contienen un valor inherente de ruido introducido por el sensor con el que la imagen es capturada, este es distribuido uniformemente a través de toda la imagen. Cuando se crean falsificaciones usando información de diferentes imágenes es común que se adjunten pequeñas cantidades de ruido en las zonas editadas esto para mantener ocultos los rastros de la falsificación a simple vista. El resultado de esto será que los niveles de ruido local a través de la imagen podrían ser inconsistentes.

El ruido son aquellos electrones presentes en la señal que no corresponden a las luminosidades de la escena. Siempre existe un porcentaje de ruido parásito, originado en distintas fuentes. Los tipos más importantes de ruido en una imagen son los siguientes:

Ruido fotónico: ningún flujo de luz es uniforme, por muy estable que sea la fuente y homogéneas las superficies en que se refleja o el medio en que se propaga. Su desviación es puramente aleatoria, por lo que se cuantifica según la distribución de Poisson, es decir: el ruido fotónico vale la raíz cuadrada del total de la señal, en términos de electrones presentes. Sus efectos sólo se aprecian en zonas muy oscuras o poco expuestas.

Corriente oscura: son los electrones de origen térmico que genera el silicio a cualquier temperatura mayor que el cero absoluto. No es significativo a velocidades normales y rápidas, pero las exposiciones largas aumentan la temperatura del sensor, y el ruido se duplica cada 6 ó 7 grados. Este ruido aportado a la señal es la raíz cuadrada de la corriente oscura total.

Ruido de lectura: Se genera principalmente en el preamplificador que lee las cargas a la salida del sensor (de tipo CCD) o de cada fotodiodo (CMOS), y también en la medición sobre el voltaje que hace el conversor analógico-digital. Es la principal fuente de ruido, especialmente a velocidades cortas.

En la figura 1.8 se puede ver de forma gráfica las zonas donde se adhiere ruido en el momento de capturar la imagen.

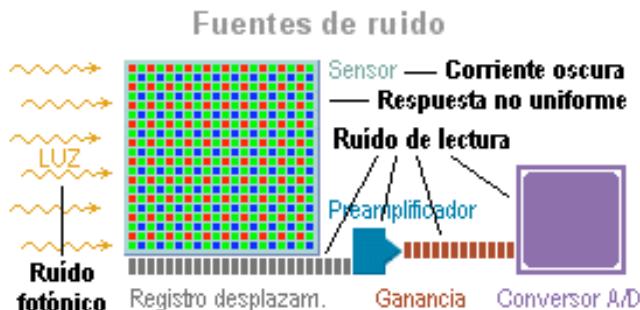


Figura 1.8 factores que influyen en la calidad que presentara una imagen digital en el momento de ser procesada.

1.5 Contribución

En esta tesis, se presentan diferentes métodos de análisis en las imágenes digitales, así como las mejores prácticas de análisis. Estos métodos estiman las regularidades e irregularidades presentadas por la imagen, para cada una de las metodologías presentadas se describe bajo qué condiciones puede ser usada. En el capítulo II se presentan las mejores prácticas recomendadas internacionalmente para el análisis de imágenes digitales, emitidas por autoridades en el campo, como lo es el Scientific Working Group on Imaging Technology. En el capítulo III se presenta una herramienta que detecta la manipulación de una imagen mediante la técnica de clonación de zonas. En el capítulo IV se muestra un método de análisis por estimación del ángulo de incidencia de la fuente de luz en los objetos contenidos en una imagen digital.

Se usarán imágenes originales y falsificadas para demostrar cómo es que funciona cada uno de estos métodos que se presentan a continuación y que son los tópicos tratados en la presente tesis, es importante señalar que existen muchas otras técnicas de manipulación de imágenes pero para el caso de esta tesis los tópicos de interés son los siguientes.

- **Mejores prácticas recomendadas internacionalmente.** Toda metodología tiene un proceso y puntos importantes que se deben tomar en cuenta para garantizar que dicha metodología se ha desarrollado de manera óptima. En el capítulo dos se definirán cuales son las recomendaciones más importantes para poder llevar a cabo un análisis forense de imágenes digitales.
- **Zonas duplicadas.** Suponga que en una imagen aparecen dos personajes de la vida pública, y que uno de ellos no quiere ser visto en la misma fotografía con el otro. El proceso para quitar algo o alguien de una imagen consiste en clonar algunas zonas de la imagen y sobre exponerlas en la parte que queremos que desaparezca. Esta clonación puede ser cuantificada e identificada por una herramienta que se ha desarrollado en la investigación para la elaboración de este trabajo de tesis y se presenta a detalle en el capítulo 3 del presente trabajo.
- **Inconsistencias en la luz.** Cuando se captura una imagen en la que solo existe una fuente de luz, esta siempre tiene un ángulo y una dirección que afecta a todos los objetos contenidos en la imagen. Por ejemplo, imagine que se quiere crear una imagen en la que aparezcan dos individuos uno al lado del otro, esta composición se realizará usando dos fotografías diferentes; al unir a las dos personas, será muy complicado hacer coincidir la intensidad y dirección de la luz en los dos individuos. Es aquí donde se puede hacer un análisis en la inconsistencia de la luz en una imagen.

La alteración de imágenes no es un fenómeno nuevo, la accesibilidad a equipo para producción y tratamiento de imágenes digitales hace muy fácil que cualquier persona con conocimientos básicos pueda manipular y alterar una imagen. La falsificación de imágenes va desde revistas, noticias, medios publicitarios, etc., estas imágenes pueden tener un gran impacto en nuestra sociedad. Aun cuando cada uno de los métodos y herramientas presentados en esta tesis atacan un tipo específico de manipulación, el uso en conjunto de ellos puede ayudar a reforzar y robustecer la autenticación de imágenes digitales.

Capítulo II

Mejores prácticas recomendadas internacionalmente

2.1 Introducción

El propósito de este capítulo es proveer recomendaciones y guías para el uso de imágenes digitales en un proceso judicial, las cuales se han elaborado a partir de las mejores prácticas recomendadas internacionalmente. El objetivo de estas recomendaciones es asegurar el éxito de una imagen al ser presentada como evidencia en un proceso judicial ante una corte. Este capítulo incluye algunas descripciones de los retos que se presentan en el momento en que se analiza una imagen digital y las limitaciones que se presentan en dicho análisis.

El proceso de autenticación puede envolver muchas dificultades. Estas dificultades incluyen, evaluación de la estructura y contenido de la imagen. La estructura de la imagen incluye descubrimiento de objetos consistentes con la manipulación o degradación de la imagen, análisis de meta datos y el origen de la imagen. El contenido de la imagen incluye evidencia de manipulación.

La integridad de una imagen digital es muy importante en el campo forense, imágenes médicas, militares y fotografía industrial. Ya que ayudan a tomar decisiones en las Cortes afectando la libertad de individuos. Algunas veces, por la presencia de imágenes que son presentadas como evidencia, ocurre que podrían ser falsas. Médicos e investigadores generan diagnósticos basándose en lo que las imágenes les muestran sobre los pacientes. Las fotografías digitales pueden determinar locaciones de objetivos basándose en su contenido y la interpretación. Las fotografías industriales evidencian defectos en los materiales que pueden terminar en productos peligrosos o defectuosos para el consumidor.

2.2 Entidades internacionales

En Estados Unidos de Norteamérica existe el Scientific Working Group on Imaging Technology (SWGIT), el cual está formado por fotógrafos, científicos, instructores e investigadores de agencias federales, estatales y locales encargados de la lucha contra el crimen, así como de algunas universidades y grupos de investigadores. Todos los documentos emitidos por el SWGIT representan la opinión emitida por los miembros que lo conforman.

La misión del SWIGT es facilitar la integración de las tecnologías en imágenes y sistemas, con el sistema de justicia criminal de los Estados Unidos de Norteamérica, proveyendo definiciones y recomendaciones para la captura, almacenamiento, procesamiento, análisis, transmisión e impresión de imágenes.

Las imágenes digitales son aceptadas en la práctica de las ciencias forenses, en el sistema judicial y Cortes de los Estados Unidos de Norteamérica. Es necesario autenticar una imagen digital antes de ser presentada como prueba en una corte. Esta autenticación solo puede ser garantizada por personal altamente calificado y especializado en el tema.

La autenticación de imágenes digitales no se debe confundir con el requisito de autenticar evidencia como una condición de admisión en una corte. La autenticidad difiere significativamente de integridad. La integridad asegura que la información presentada es completa y no ha sido alterada desde que fue creada y hasta su disposición final. Por ejemplo, el uso de funciones hash pueden verificar que la copia de un archivo de imagen digital es idéntico al archivo del cual fue copiado, pero esto no puede demostrar la veracidad de la escena contenida en la imagen.

El proceso de autenticación puede envolver muchas dificultades. Estas dificultades incluyen, evaluación de la estructura y contenido de la imagen. La estructura de la imagen incluye descubrimiento de objetos consistentes con la manipulación o degradación de la imagen, análisis de meta datos y el origen de la imagen. El contenido de la imagen incluye evidencia de manipulación.

En la actualidad, se ha planteado una controversia a nivel Iberoamericano referente a la validez o no de las imágenes digitales en diversos tipos de procesos judiciales. El argumento en contra de la nueva tecnología de imágenes digitales, se fundamenta en la supuesta facilidad con la que presuntamente se pueden alterar este tipo de imágenes¹¹.

Para que la fotografía tenga pleno valor probatorio deberá ser obtenida a través de una orden judicial, es decir, que para que la fotografía tenga validez en juicio debe ser tomada por una orden judicial, lo cual en la práctica se hace a través de prácticos, peritos o expertos, por lo que esta fotografía desde el punto de vista subjetivo, goza de una especie de principio de fe pública que se deriva de que el medio probatorio es obtenido por un funcionario público. Pero de ser así casi ninguna fotografía digital sería admitida como prueba en un proceso judicial. Aun cuando la ley en México no contempla el uso de imágenes digitales como medios probatorios, tampoco limita el uso de las mismas en procesos judiciales.

2.3 Recomendaciones SWGIT

El objetivo del documento emitido por el SWGIT titulado “Best Practices for Forensic Image Analysis”, es proveer una guía de las prácticas más apropiadas cuando se hace una gran variedad de procesos relacionados con el tratamiento de imágenes, como puede ser el caso del ajuste de contraste, color, brillo, dimensión, etc. Es necesario saber qué tipo de análisis hacer a las

¹¹ <http://www.criminalistica.net/forense/modules.php?name=News&file=article&sid=691>

imágenes, a continuación se presentan las mejores prácticas para el tratamiento de imágenes digitales.

La fotografía tradicional, y los procesos asociados a estas han sido usados desde 1839¹². Muchos de los procesos desarrollados para la fotografía tradicional, tienen su equivalente en el procesamiento digital de imágenes. Todas las técnicas usadas en el procesamiento digital de imágenes tienen sus raíces en la fotografía digital y/o las matemáticas. Este precedente histórico ayuda a que el procesamiento de imágenes digitales sea aceptado como una práctica en las ciencias forenses.

El procesamiento digital de imágenes es una práctica aceptada en las ciencias forenses de EUA (Estados Unidos de Norteamérica), pero para que una imagen digital sea aceptada en un proceso judicial después de haber sido sometida a un análisis forense debe sujetarse a los siguientes criterios:

- La imagen digital original debe ser preservada, generando copias exactas del original y trabajar sobre las copias, guardando el original en donde solo personal autorizado pueda tener acceso a él.
- Los pasos en el procesamiento del análisis deben ser documentados.
- El resultado final presentado de la imagen podrá repetirse, con base en los procedimientos documentados en su análisis.
- Los pasos documentados en el proceso de análisis de la imagen deben ser tan claros que permitan a cualquier persona con conocimientos del tema, entender de forma clara como se realizó dicho análisis y le permitan emular el proceso realizado.

Los procedimientos que se llevarán a cabo en el procesamiento de la imagen, para su análisis son los siguientes y se presentarán a detalle más adelante:

- Mejorar la imagen
- Restauración de la imagen
- Compresión de la imagen

Cuando se usan técnicas de procesamiento de imágenes digitales se debe tener precaución con no introducir ruido extra a la imagen, lo cual se vería reflejado en pérdida de información de la imagen, y también perder ciertos detalles de la imagen, que generaría una mala interpretación. Cualquier técnica de procesamiento se realizará sobre la copia de la imagen.

El éxito para que la imagen sea aceptada como evidencia en una corte radica en los siguientes puntos.

- Fiabilidad: que la imagen sea creíble, fidedigna y no presente errores

¹² SWIGT, Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System, Version 2.0 2006.01.09, Pg1.

- Reproducibilidad: Que los procesos por los cuales fue sometida la imagen para su análisis puedan ser repetidos siempre que se requieran.
- Seguridad: Que se garantice que la imagen original permaneció en un lugar seguro y lejos de personal no autorizado a tener acceso a ella.

2.4 Mejorar la imagen

Es cualquier proceso que trata de mejorar la apariencia de una imagen.

Técnicas de mejora. Para mejorar una imagen se tienen que llevar a cabo algunas o todas las siguientes técnicas: ajuste del brillo y contraste, balance de color, cortar, etc. Estas son consideradas técnicas aceptables de forensia en imágenes digitales.

- *Ajuste de brillo:* Es usada cuando la imagen es muy brillante o muy obscura. Si la imagen fue realizada con mucha luz, se correrá el riesgo de perder información valiosa en las zonas de mucha luz y viceversa para las partes oscuras.
- *Balance de color:* Balancear el color sirve para nivelar los contrastes de color en la escena. Un mal balance de color puede poner los colores inadecuadamente y los objetos contenidos se verán con un color irreal.
- *Cortar:* Se usa para eliminar áreas de una imagen que no interesan en el análisis.
- *Pegar.* Se usa para añadir información a una imagen, puede ser de la misma imagen o de otra.

Es preciso señalar que hay que tener cuidado cuando se hace balance de color, ya que la imagen puede perder fidelidad.

Técnicas de filtrado lineal: estas técnicas se usan para incrementar el contraste en pequeños detalles dentro de la imagen, sharpening¹³, deburring¹⁴, cambiar ciertas características de la imagen. Si la imagen tiene una mala calidad el análisis dentro de la misma será mucho más complicado, al no tener una adecuada representación de todo el escenario , pero puede seguir siendo usada interpretando pequeños detalles de la imagen.

¹³ Es el proceso de darle mayor nitidez a una imagen.

¹⁴ Es la degradación en la calidad de una imagen.

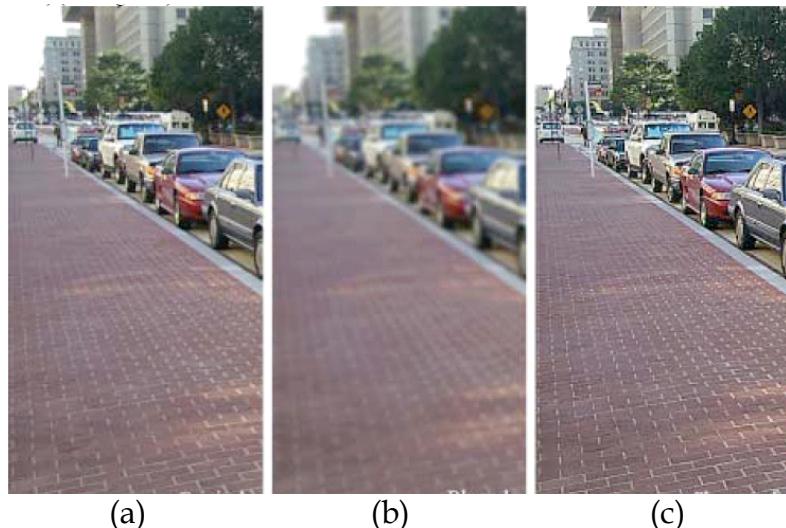


Figura 2.1 muestra el efecto de usar filtrado lineal. (a) la imagen original, (b) imagen con ruido, y (c) con mayor nitidez.

Los ajustes de contraste no lineal incluyen la corrección de gama de color, transformación en escala de grises, ajustes en brillo y contraste. Esto sirve para ajustar los niveles de brillo dentro de la imagen. Por ejemplo, los detalles buscados podrían estar contenidos en las áreas más sombreadas, pero hay que tener en cuenta que al realizar ajustes radicales se puede introducir mucho ruido que alteraría otros segmentos de la imagen.



Figura 2.2 muestra ajustes de contraste no lineal, (a) la imagen original, (b) definición de áreas sombreadas y de luz, (c) son los rangos medios de sombra y luz.

Consideraciones a tomar en cuenta en la aplicación de técnicas de mejora de la imagen.

- Qué tipo de imagen no debe mejorarse. La imagen original no debe ser manipulada, única y exclusivamente será sometida a un proceso de duplicación, pero después de eso tendrá que ser asegurada, para evitar alteraciones a dicha imagen.

La imagen original está representada en el dispositivo donde fue almacenada por primera vez o puede ser una copia fiel de la original, pero para poder hacer mejoras sobre la imagen solo se podrá hacer sobre la imagen de trabajo (Copia de la imagen original).

- Es necesario documentar las mejoras realizadas y los procesos usados para mejorar la imagen.
- La documentación del proceso para mejorar la imagen estará determinada por el proceso usado.

Es importante enfatizar en el hecho de que el documentar las mejoras en imágenes no es necesario cuando se usan técnicas de cuarto oscuro, osea imágenes no digitales.

2.5 Restauración de la imagen

Objetivo: la restauración de imágenes es el proceso de remover parcial o totalmente cualquier efecto de la degradación contenida en una imagen.

Las limitaciones que presenta esta técnica son por un lado la remoción o inclusión de ruido, esto es que la información perdida en la imagen ya no se podrá recuperar. Cuando se hace una restauración parcial es posible recuperar alguna información, pero al realizar una restauración total será prácticamente imposible recuperar dicha información.

Técnicas de restauración

Conversión a escala de grises es el ajustar el brillo relacionado con los objetos contenidos en la imagen. La conversión a escala de grises se usa para evaluar la diferencia de brillo en la escena. Por ejemplo, si se incluye un objeto en la escena que no forma parte de la captura original, es posible identificar ciertas variaciones del brillo en los contenidos adjuntados en la imagen.

Balance de color es el ajuste de los componentes de color de una imagen. El propósito de hacer un balance de color dentro de la imagen sirve para evaluar los componentes u objetos con color dentro de la imagen, haciéndolos más evidentes en la imagen y permitiendo analizar partes muy detalladas.

2.6 Compresión de una imagen.

El objetivo de comprimir una imagen radica en el hecho de que si una imagen es muy grande en tamaño, la manipulación que se tenga sobre la misma será muy costosa en cuanto a consumo de procesador y memoria, y es probable que algunos equipos de cómputo no cuenten con las características que les permitan procesar en forma efectiva toda esta información. Otro problema que se puede presentar es que si la imagen analizada requiere ser transmitida por la internet, y dicha imagen es muy grande ocasionará problemas en su transmisión. Una de las recomendaciones para mitigar este problema es

aplicar algoritmos de compresión de imágenes a la imagen a tratar siempre y cuando la compresión no dañe la información contenida en la imagen.

A continuación se presentan los diferentes formatos de compresión que existen.

JPEG: Es un formato de compresión con pérdida, es muy bueno para hacer compresiones de muy alto nivel aunque la pérdida de calidad es considerable al aumentar la tasa de compresión.

GIF: Es un formato de compresión sin pérdida pero está limitado a 256 colores, limitado para imágenes de muchos colores.

PNG: Formato de compresión sin pérdida excelente para imágenes de muchos colores.

2.7 Análisis sobre imágenes Digitales.

El análisis forense sobre imágenes puede considerarse como una ciencia forense. Esta misma ha sido practicada desde los primeros días de la fotografía, se remonta a finales de 1851 cuando Marcus A. Root documentó el primer ejemplo de autenticación. Además, de que el análisis de imágenes ha sido aceptado como una práctica científica en la comunidad forense, el análisis de imágenes es utilizado en otras disciplinas incluidas la medicina, geología, astronomía, agricultura, etc.

El análisis forense de imágenes digitales es la aplicación de técnicas científicas de la imagen y el dominio experto para interpretar el contenido de una imagen, y si la imagen misma es íntegra para ser admitida en un proceso legal. Las sub-disciplinas del análisis forense sobre imágenes digitales con fines legales incluyen: Fotogrametría, Comparación fotográfica, Análisis de contenido, y la autenticación de la imagen.

El proceso de análisis forense sobre imágenes puede envolver muchas y variadas tareas, aun cuando se ha mejorado el tipo de análisis sobre imágenes. Estas tareas se pueden catalogar en tres categorías: Interpretación, Examinación, y la preparación técnica. Estas tareas se describen a continuación:

Interpretación

Se usa para definir conclusiones por un experto acerca de los sujetos u objetos incluidos dentro de una imagen. Por ejemplo, un experto en huellas de pie definirá si las huellas incluidas en una imagen están correctamente distribuidas dentro de la misma.

Examinar

Es la extracción de información contenida en la imagen por parte de los expertos en ciencias de la imagen, obtener las características de la imagen, y la

interpretación de la estructura de la imagen, esto incluye la detección de marcas de agua dentro de la imagen, análisis esteganográfico, y evaluar la posible alteración de la imagen, otras tareas de examinar la imagen incluyen medidas de la misma, restauración de la imagen, y algunas otras actividades de procesamiento de la imagen que intentaron cambiar el contenido y características de la imagen como se vió en las figuras 2.1 y 2.2.

Preparación Técnica.

Es el desempeño de tareas, así como la preparación de la evidencia o examinar e interpretar imágenes. Aquí existe una gran gama de decisiones técnicas las cuales incluyen muchas responsabilidades que serán cubiertas por las acciones de la preparación técnica. Algunas responsabilidades incluyen tomar decisiones técnicas, como por ejemplo, decidir qué papel usar para imprimir las imágenes o el tipo de impresora a usar (Inyección de tinta, láser, etc.), que dispositivos de almacenamiento usaremos para la imagen (CD, Memorias, Disco Duro, etc.). Algunas otras responsabilidades incluyen decisiones técnicas muy importantes como el software de análisis que usaremos, determinar el color apropiado del balance o la resolución de salida¹⁵.

2.8 Tipos específicos de análisis forense en imágenes.

Análisis de los meta datos: los archivos de imágenes digitales contienen dos tipos diferentes de datos, píxeles e información sobre la estructura y contenido de la imagen, esto último se conoce como meta datos. Los meta datos pueden ser usados en la identificación de la fuente y el histórico del procesamiento del archivo, pero este puede ser alterado o borrado. EXIF es un estándar para almacenar información intercambiable en archivos de imagen. Es el que usan la mayoría de las cámaras digitales para almacenar en las fotos la información técnica sobre la toma y las características de la cámara. La especificación EXIF ha sido desarrollada por JEITA, la Asociación Japonesa de Tecnologías Electrónicas y de la Información. Esta especificación cubre datos como: tiempo de exposición, número frame, distancia focal, fecha, modelo de la cámara, datos del flash, etc. En la figura 2.3 se muestra una imagen y en la figura 2.4 los metadatos de la misma, en los cuales se puede apreciar toda la información que pueden contener estos de la imagen.

¹⁵ Interpretar, examinar y la preparación técnica son tareas, no descripciones de trabajo o roles. Cada una de estas tareas requiere de entrenamiento y capacitación.



Figura 2.3 Imagen de la cual se extraerán los meta datos.

Metadatos	
Palabras clave	
Proveedor	:
Origen	:
Aviso de copyright	:
Términos de uso de derechos:	
Datos de cámara (Exif)	
Exposición	: 1/125 s en f/8
Modo de exposición	: Automático
Programa de exposición	: Normal
Índices de velocidad ISO	: 100
Distancia focal	: 4.9 mm
Distancia focal en película de 35 mm	: 36 mm
Valor máximo de apertura	: f/2.8
Software	: Ver.1.0
Fecha y hora	: 17/02/2008, 05:56:27 p.m.
Fecha y hora originales	: 17/02/2008, 05:56:27 p.m.
Fecha y hora digitalizadas	: 17/02/2008, 05:56:27 p.m.
Flash	: No se disparó, modo automático
Modo de medición	: Motivo
Espacio de color EXIF	: sRGB
Interpretación personalizada	: Proceso normal
Equilibrio de blancos	: Automático
Tipo de captura de escena	: Estándar
Control de ganancia	: 0
Contraste	: 0
Saturación	: 2
Enfoque	: Duro
Método sensorial	: Sensor de un chip
Origen de archivo	: Cámara digital
Marca	: Panasonic
Modelo	: DMC-FX07

Figura 2.4 meta datos de la figura 2.3.

Fotogrametría: la fotogrametría es el arte, ciencia o técnica de obtener información valiosa sobre los objetos físicos y el ambiente a través de la grabación, medida, e interpretación de imágenes y los patrones de energía radiante y otros fenómenos visuales en una imagen. En aplicaciones forenses la fotogrametría es comúnmente usada para extraer información dimensional de las imágenes, tales como la altura de sujetos u objetos en imágenes, muchas veces con el fin de reconstruir la escena donde tuvo lugar un incidente.

La siguiente imagen muestra como por medio de la fotometría se puede realizar un análisis sobre una imagen tomada por una cámara de vigilancia. Este análisis ayuda a determinar la geometría de los objetos dentro de la imagen, para estimar el tamaño y posición de dichos objetos, en el caso de la

figura 2.5, se estima la posición y tamaño que tiene el sujeto que esta asaltando un banco, en base a las dimensiones de otros objetos dentro de la foto y de los cuales se tiene bien identificado su tamaño, como es el caso del mostrador del banco.

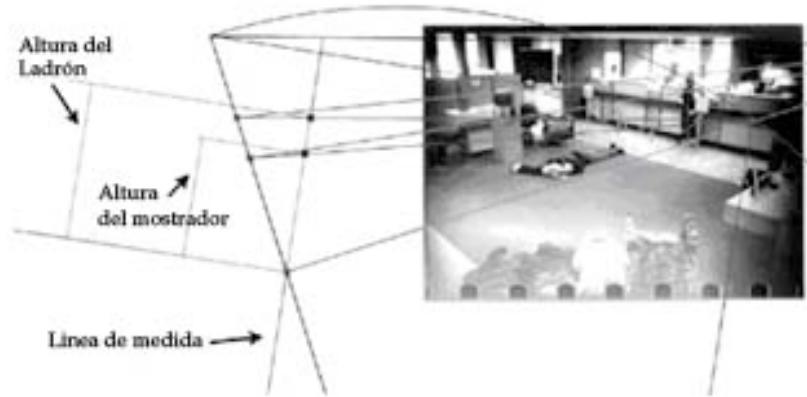


Figura 2.5 se estima la posición y tamaño que tiene el sujeto que esta asaltando un banco, en base a las dimensiones de otros objetos dentro de la foto.

Comparación fotográfica: la comparación fotográfica es la medición de la correspondencia entre características en imágenes, es decir las dimensiones de los objetos contenidos dentro de la imagen deben presentar cierta correspondencia, así como el ambiente tiene que ser congruente en los contrastes de color y el brillo.

2.9 Guía de procedimientos estándar para el procesamiento de imágenes digitales.

El propósito del procesamiento de imágenes es aplicar técnicas que intentan mejorar y restaurar imágenes digitales. Que una imagen digital pueda ser presentada como evidencia digital en una corte depende básicamente de cuatro factores: Que sea fiable, que se pueda reproducir, seguro y que pueda ser analizado. Para obtener resultados satisfactorios, es necesario seguir procedimientos estandarizados como lo son las recomendaciones emitidas por el SWGIT.

Equipamiento.

El mínimo hardware y software recomendado para el análisis de imágenes es el que se enlista a continuación.

Hardware:

- Dispositivos de captura de imágenes: Cámaras digitales con sensores de buena calidad al menos de 7.0 mega pixeles, escáner.
- Sistema de procesamiento de imágenes: unidades lectoras de las diferentes memorias existentes para cámara digital.
- Dispositivos de salida para imágenes: Pantallas, impresoras, plotters, proyectores, etc.

- Dispositivos de almacenamiento: discos duros, memorias, discos compactos, etc.

Software:

- Administrador de imágenes: sistema de archivos y sistema operativo en donde se encuentran alojadas las imágenes.
- Procesamiento de imágenes: Software de edición de imagen como Photoshop, CorelDraw, Paint, etc.

Procedimiento

Los pasos mínimos propuestos para procesar una imagen son los siguientes.

- Captura
- Procesamiento
- Almacenamiento
- Administración de la imagen
- Asegurar la imagen
- Presentación de la imagen

2.10 Recomendaciones INTERPOL

Un documento emitido por la INTERPOL que recoge las memorias de un simposio realizado en Francia en Octubre del 2001, deja ver la preocupación por autenticar las imágenes digitales y hace referencia al Netherlands Forensics Institute y el National Research Institute of Police Science in Japan¹⁶. Estos dos institutos trabajan en conjunto sobre diferentes métodos para examinar la autenticidad de una imagen, trabajan directamente con las cámaras digitales para determinar si una imagen fue creada en una cámara específica mediante los defectos que presenta el CCD (Charged Couple Device), también sobre los formatos de archivos y el ruido introducido por el arreglo de filtros de color o filtro de Bayer, que se vio en la figura 1.7.

En el documento emitido por la INTERPOL se hace referencia sobre las mejores prácticas recomendadas por el SWGIT y se señalan estas como el procedimiento aceptado para analizar imágenes digitales. Adicionalmente se presenta un proyecto llamado IMPROOFS¹⁷ el cual basa su análisis de imágenes en los siguientes puntos:

Mejoramiento de la imagen y restauración: El objetivo es mejorar la resolución, contraste y la señal de ruido.

Metrología: Es un sistema que permite estimar la dimensión de todos los objetos dentro de la escena.

¹⁶ <http://www.interpol.int/Public/Forensic/IFSS/meeting13/Reviews/Image.pdf>

¹⁷ <http://homes.esat.kuleuven.be/~konijn/improofs.html>

Identificación de personas: Se propone el modelado en 3D para reconstruir rostros, que ayuden a la identificación de características especiales y permita identificar personas.

2.11 Comentarios del capítulo.

Las etapas recomendadas para llevar a cabo un análisis forense en imágenes digitales consisten en los siguientes puntos.

- Conservar la imagen original íntegra
- Generar copias y trabajar sobre ellas
- Preparación de la evidencia, Hardware y Software adecuado.
- Proceso de análisis de la imagen
- Documentar los pasos en el proceso de análisis de la imagen.
- Interpretación de los datos extraídos de la etapa de análisis
- Reporte final
- El resultado final del análisis de la imagen podrá repetirse con base en los procesos documentados en el análisis.
- Los pasos documentados deben ser tan claros que cualquier otro analista pueda seguir el procedimiento y llegar al mismo resultado.

A continuación se detallan los puntos del análisis forense a una imagen digital.

La primera etapa en el proceso de análisis forense de imágenes digitales comprende la cadena de custodia, la cual busca garantizar que la imagen que será analizada no pueda ser accedida por personal que no tiene permiso para manipular dicha imagen.

Contar con Hardware y software adecuado para el análisis de imágenes.

Hardware: Computadora con buena capacidad de procesamiento y suficiente memoria en RAM para poder manipular imágenes.

Lectores de memoria para cámaras digitales.

Pantalla al menos de 21 pulgadas.

Escáner.

Impresora a color con una calidad de 600 x 600 dpi.

Discos Duros, memorias, discos compactos, etc.

Software: Photoshop CS3, Mat Lab 2006R, Paint.

Restauración de una imagen digital: es posible que la imagen digital que se está analizando haya sufrido algún tipo de daño y sea necesario restaurar algunas zonas, esto será posible y pertinente siempre y cuando esta restauración no modifique la estructura de la imagen.

Ajuste de brillo y contraste: la finalidad de ajustar el brillo y/o contraste en una imagen es para identificar algunos detalles que probablemente no sean perceptibles sin este ajuste.

Análisis de meta datos: la extracción y análisis de los meta datos de una imagen puede proveer información sustancial para el reporte final de la imagen, información tal como fecha de captura de la imagen, fecha de modificación, cámara y modelo usado, etc.

Generación de copias: es muy posible que necesitemos múltiples copias de la imagen ya que cuando se analiza una imagen está será sometida a diferentes procesos tratando de extraer información que indique la autenticidad o no de dicha imagen, es por ello que es necesario crear múltiples copias de la imagen original, para poder tener diferentes referencias de los procesos a los que ha sido sometida la imagen.

Proceso de análisis de la imagen: Como se ha visto el propósito del procesamiento de imágenes es aplicar técnicas que ayuden a mejorar el aspecto de una imagen, esto se puede conseguir aplicando alguna o todas las siguientes técnicas, Ajuste de brillo, Balance de color, Cortar, etc. Lo anterior con el fin de tener una mejor interpretación de la imagen que se está analizando en base a un profundo examen de los detalles que puedan ser extraídos de la imagen. En esta etapa la imagen será sometida a diferentes procesos con el fin de obtener información contundente que sirva para dictaminar una opinión de dicha imagen, por ejemplo, someter la imagen al algoritmo presentado en el capítulo 3 de esta tesis en busca de zonas clonadas.

Interpretación de los datos: la información extraída de la etapa anterior (Proceso de análisis de la imagen) tendrá que ser analizada en busca de pistas que permitan determinar la autenticidad o no de la imagen que está siendo analizada, en esta etapa es importante la pericia de la persona que está analizando los datos.

Reporte final: Dicho reporte tiene que incluir todo el proceso puntual al que fue sometido la imagen, así como el hardware y software usados en este procedimiento y finalmente, dictaminar si la imagen analizada es original o no.

Capítulo III

Análisis de zonas clonadas en una imagen digital.

3.1 Introducción

Imagine que desea manipular una imagen cualquiera copiando y pegando sectores de la misma imagen. El proceso para poder hacer esa manipulación es cargar dicha imagen en un software de edición, como puede ser Photoshop®, CorelDraw®, Paint®, etc., en el cual se realizarían las modificaciones deseadas. Los cambios que se van a analizar en este capítulo se centran en la verificación de las zonas clonadas, este tipo de manipulación se lleva a cabo cuando se requiere ocultar algo de la imagen o cuando simple y sencillamente se quiere modificar la percepción que se tiene de esa imagen.

3.2 Adquisición de la imagen con la cámara digital.

Como se ha mencionado en el capítulo anterior la metodología consiste en detectar la alteración en la información estadística que presenta la imagen, para entender en donde es que vamos a buscar es necesario comprender el proceso de adquisición de imágenes con la cámara digital de forma clara y precisa.

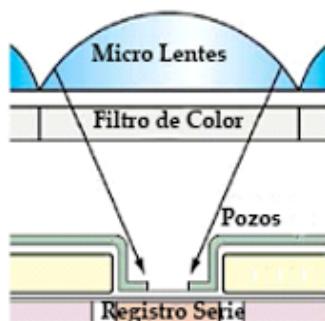


Figura 3.1 información que ingresa a la cámara para construir una imagen.

Las cámaras cuentan con un Charged Couple Device, este es el elemento central en una cámara digital, está construido con un semiconductor de silicio, que es fotosensible. Cuando se abre el obturador de la cámara es este dispositivo quien recibe la información de lo que se captura para construir la imagen, con ayuda de un filtro de Bayer (Figura 3.3), que es quien asigna los valores del Rojo Verde y Azul por sus siglas en inglés RGB, dependiendo la intensidad de la luz recibida, se asigna la información a una rejilla Roja, Verde o Azul, el filtro o mosaico de Bayer contiene el doble de rejillas Verdes que Azules o Rojas, esto es porque el ojo humano es más sensible a este color y le da mayor calidad a la vista de las personas.

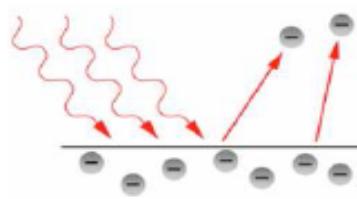


Figura 3.2 al llegar un fotón el semiconductor libera electrones.

Cuando llega un fotón el semiconductor libera electrones, como se ve en la figura 3.2, cada celda, (Figura 3.1) es un pozo que acumula los electrones que han saltado, el número de electrones liberados es proporcional a la intensidad de la luz que existe en el ambiente.

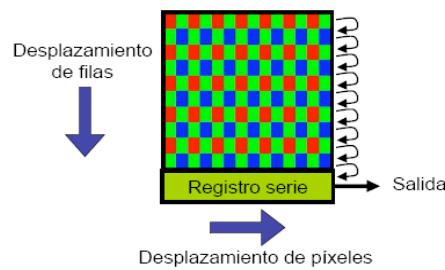


Figura 3.3 A la salida del Registro Serie, toda la información recibida en electrones es convertida en voltaje.

Tras abrir el obturador y cargar los pozos o rejillas del filtro de Bayer con la información de los pixels que el sensor percibió, se escanea línea por línea cada uno de los pozos que contienen información, y se desplazan hacia la zona de salida, donde se recibe la información de los valores de cada una de las líneas. A la salida del Registro Serie, como se muestra en la figura 3.3, toda la información recibida en electrones es convertida en voltaje. La información obtenida a la salida del registro serie es pasada por un conversor analógico a digital, y posteriormente esta información es procesada para obtener los pixels faltantes.

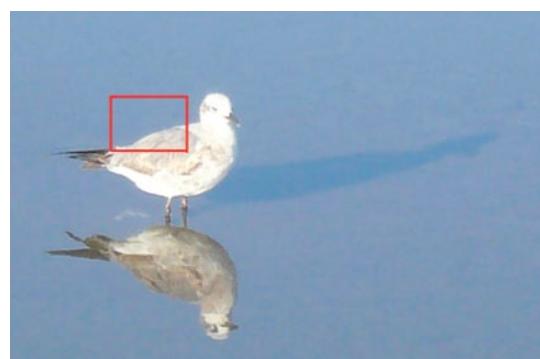


Figura 3.4 imagen para ejemplo de interpolación.

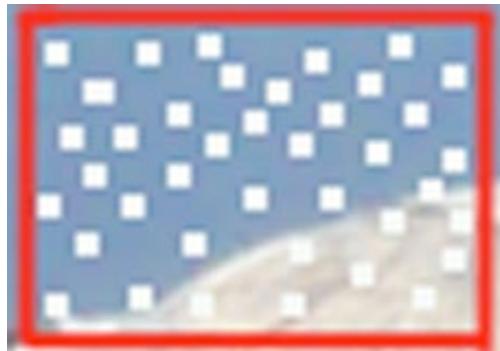


Figura 3.5 Ejemplo de interpolación, así estaría una imagen antes de ser interpolada.

En la figura 3.5 vemos un segmento de la imagen mostrada en la figura 3.4, previa al proceso de interpolación, todos los recuadros que se muestran en blanco son espacios sin información, pero la cámara procesa estos recuadros para asignarles información por medio de la interpolación.

En el subcampo matemático del análisis numérico, se denomina interpolación a la construcción de nuevos puntos partiendo del conocimiento de un conjunto discreto de puntos. En ingeniería y algunas ciencias es frecuente disponer de un determinado número de puntos obtenidos por muestreo o a partir de una estimación y pretender construir una función que los ajuste.

La idea es que, a partir de n parejas de puntos (x_k, y_k) , obtener una función f que verifique

$$f(x_k) = y_k, k = 1, \dots, n$$

A la que se denomina función interpolante de dichos puntos. A los puntos x_k se les llama nodos.

En el campo de la fotografía y mundo de la imagen digital, la interpolación aplica este mismo método para conseguir un tamaño mayor de la imagen inicial, rellenando la información que falta con datos obtenidos mediante la interpolación a partir de un algoritmo específico.

Existen varios algoritmos, los más comunes son los siguientes:

- Interpolación por aproximación: Es uno de los métodos más antiguos. Se basa en obtener el promedio de valores de los 2 pixeles más próximos. La interpolación bilineal es una mejora de la anterior, promediando en este caso 4 pixeles adyacentes.
- Interpolación bicúbica: Usada por programas como Adobe Photoshop o Paint Shop Pro es el método de interpolación considerado estándar (promedia 16 pixeles adyacentes). Photoshop además usa algunas variaciones como Interpolación bicúbica enfocada o Interpolación

bicúbica suavizada que se basa en aplicar algunos cambios a la imagen final.

- Interpolación en escalera: Se basa en la interpolación bicúbica con la diferencia que se va interpolando en incrementos de un 10% en cada paso con respecto al anterior.
- Interpolación S-Spline: Este método de interpolación determina el color de un pixel desconocido basándose en la totalidad de colores de la imagen, a diferencia de los métodos anteriores.

Un píxel o pixel (*picture element*) es la menor unidad homogénea en color que forma parte de una imagen digital.

Una vez que se tiene toda la información de la imagen, es almacenada en una memoria y así es como queda construida la imagen.

3.3 Composición de la imagen.

Como ya se vio, una imagen está compuesta por píxeles, que son la menor unidad fundamental en que se conforma una imagen digital.

Como se observa en la figura 3.6, ampliando lo suficiente una imagen digital, pueden observarse los píxeles que componen la imagen. Los píxeles aparecen como pequeños cuadrados o rectángulos en color, en blanco o en negro, o en matices de gris. Las imágenes se forman como una matriz rectangular de píxeles, donde cada píxel forma un área relativamente pequeña con respecto a la imagen total.



Figura 3.6 acercamiento a una imagen para identificar como esta compuesta por pequeños cuadros llamado píxeles.

En las imágenes de mapa de bits o en los dispositivos gráficos cada píxel se codifica mediante un conjunto de bits de longitud determinada (lo que se conoce como profundidad de color), por ejemplo, puede codificarse un píxel con un byte que sería blanco o negro, u 8 bits, de manera que cada píxel admite 256 variaciones (2^8 variaciones con repetición de 2 valores posibles en un bit tomados de 8 en 8). En las imágenes de color verdadero, se usan tres bytes para definir un color, es decir, en total se puede representar un total de 2^{24} colores, que suman 16.777.216 opciones de color.

Para poder transformar la información numérica que almacena un píxel en un color se debe de conocer, la profundidad de color (el tamaño en bits del pixel), el modelo de color que estamos usando. Como se explicó anteriormente, es el modelo de color RGB (*Red-Green-Blue*) quien permite crear un color componiendo tres colores básicos: el rojo, el verde y el azul. De esta forma, en función del nivel obtenido de cada uno de estos colores será el color final obtenido. Por ejemplo, el color amarillo se obtiene mezclando el rojo y el verde. Las distintas tonalidades del amarillo se obtienen variando la proporción en que intervienen ambas componentes. En el modelo RGB es frecuente que se usen 8 bits para representar la proporción de cada una de las tres componentes primarias, así como se muestra en la figura 3.7. De esta forma, cuando una de las componentes vale 0, significa que esta no interviene en la mezcla y cuando vale 255 ($2^8 - 1$) significa que interviene aportando el máximo de ese tono.

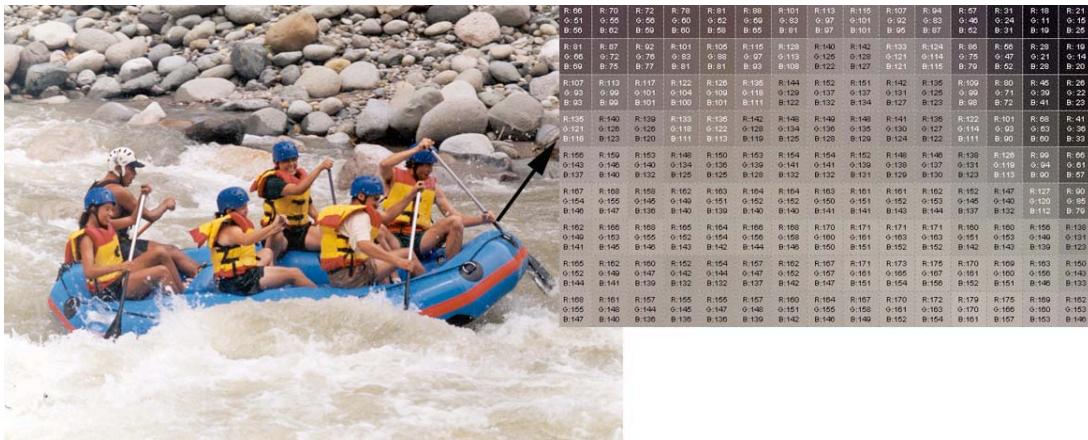


Figura 3.7 en esta imagen se muestra como se extrae un segmento de la misma y se hace un acercamiento a los pixeles, en los cuales podemos ver los valores que los componen.

3.4 Falsificación mediante clonación de zonas.

Es importante puntualizar que existen diferentes técnicas y mecanismos de falsificación de imágenes, por ello es preferible analizar por separado cada una de estas posibles falsificaciones. Aun cuando cada mecanismo o herramienta sea considerada para hacer un análisis por separado, es probable que no provean la suficiente evidencia para determinar la falsificación en una imagen digital, el uso de un grupo de técnicas o mecanismos de análisis puede ser fusionado para colectar la evidencia que será revisada por un experto en el análisis de imágenes y esta le permitirá emitir un juicio preciso sobre la originalidad de una imagen. Este capítulo está dedicado a la identificación de una de las formas de falsificación más común en las imágenes digitales, la clonación de regiones de una imagen, así como al desarrollo de un algoritmo para la identificación de estas zonas clonadas.

En la falsificación de zonas clonadas, una parte de la imagen es copiada y pegada en otra parte de la misma imagen. Usualmente se realiza este procedimiento con la intención de desaparecer un objeto de la imagen cubriendolo con un segmento copiado de otra parte de la imagen. Las zonas texturizadas, como el pasto, follaje, grava, o en términos generales las zonas irregulares, son ideales para este propósito ya que al ser copiadas y pegadas en otro segmento es difícil para el ojo humano detectar que hubo una manipulación, ya que la parte copiada viene de la misma imagen presentará las mismas propiedades de luz, colores, y nitidez de la imagen, lo que la hace compatible con el resto de la imagen. Adicionalmente el uso de software como Photoshop permite hacer falsificaciones sumamente difíciles de identificar y puede enmascarar cualquier rastro de este tipo de manipulación.

Un ejemplo de clonar zonas de una misma imagen se muestra en la figura 3.8, donde se muestra una falsificación en la que se clonó el ave que aparece en el agua. Esto no es muy difícil de identificar ya que las aves son exactamente iguales, en la figura 3.9 se muestra del lado izquierdo la imagen antes de ser manipulada, en el lado derecho se muestra la imagen alterada en la cual se ha eliminado la persona que aparecía en la foto original, dicha manipulación se realizó simplemente con clonar zonas de la misma imagen y sobreponiéndolas en el segmento donde se requiere alterar la imagen.



Figura 3.8 imagen que muestra la clonación de objetos dentro de una imagen.



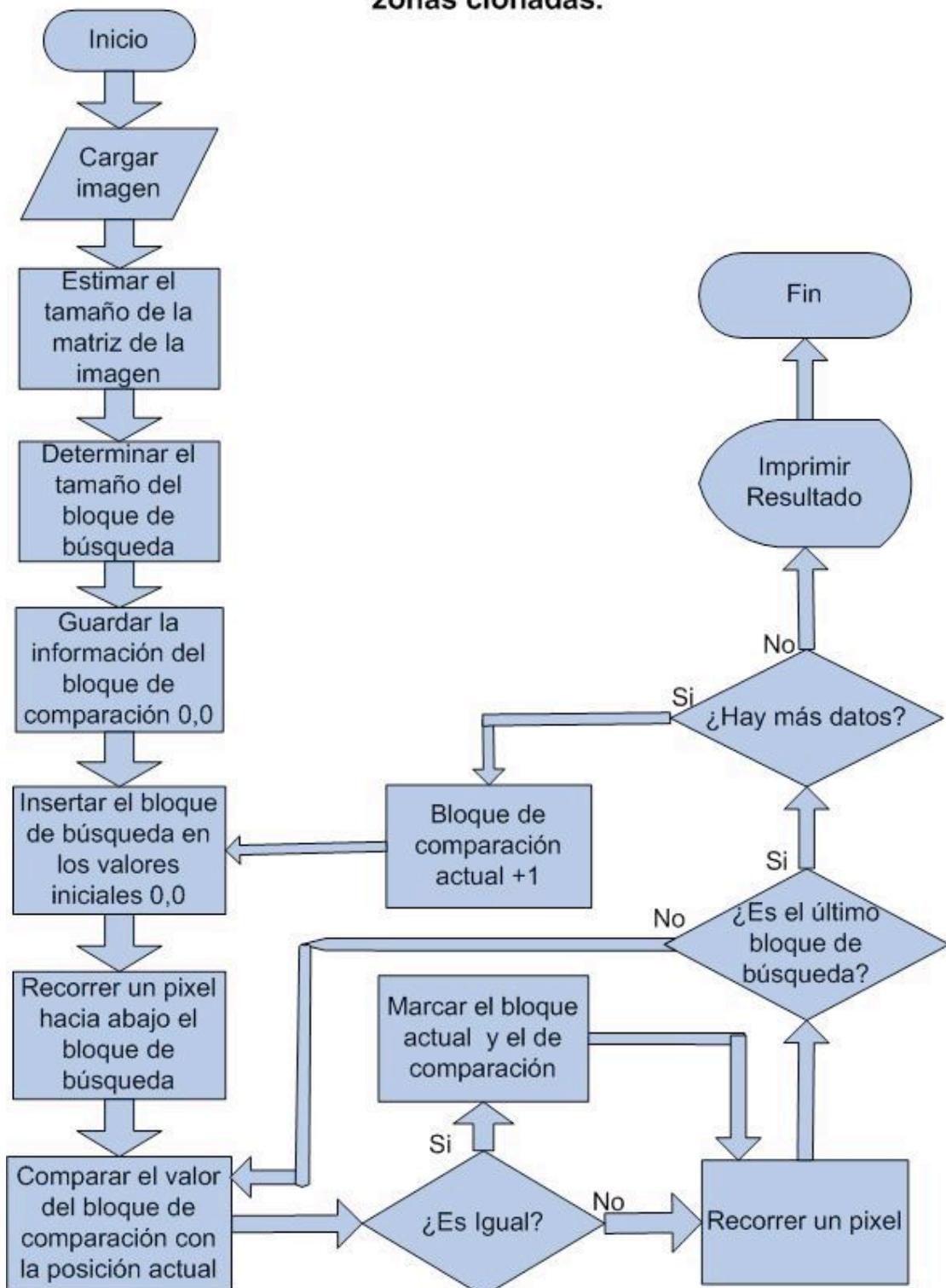
Figura 3.9 Imágenes que muestran como mediante clonación de zonas se puede eliminar información de una imagen.

3.5 Identificar falsificación en una imagen.

Toda falsificación basada en la técnica de clonación de zonas introduce una correlación entre el segmento original de la imagen y la zona clonada de dicho segmento. Esta correlación puede ser usada como base para una detección satisfactoria de este tipo de falsificación. Con base en lo anterior se formularon los siguientes requisitos para desarrollar un algoritmo en Matlab para la detección de zonas clonadas.

1. El algoritmo de detección tiene que permitir escanear una imagen en pequeños bloques de pixels e ir recorriendo dicho bloque píxel por pixel hasta terminar la imagen.
2. El algoritmo tiene que comparar cada uno de los bloques con el resto de los pixels contenidos en la imagen.
3. Al encontrar dos bloques exactamente iguales debe marcarlos para ubicar dicha clonación.
4. Una vez marcado el bloque deberá continuar buscando una duplicidad del mismo bloque hasta terminar la imagen y continuar con el siguiente bloque.
5. Cuando ya no existan mas datos que analizar mostrar el resultado en pantalla.

Diagrama de flujo del algoritmo de detección de zonas clonadas.



En un principio el usuario debe especificar el tamaño mínimo del segmento que quiere ser identificado. Ahora suponga que este segmento es un cuadrado con $B \times B$ pixels. El cuadro se deslizará píxel por píxel a lo largo de toda la imagen desde la esquina superior izquierda hasta llegar a la esquina inferior derecha de la imagen. Para cada posición del bloque $B \times B$ los valores de los pixels serán extraídos y comparados columna por columna en un arreglo de dos dimensiones A generado con las columnas B^2 y $(M - B + 1)(N - B + 1)$ líneas. Cada línea corresponde a una posición del bloque deslizante.

Dos líneas idénticas en la matriz A corresponden a dos bloques idénticos $B \times B$. Para identificar la clonación de segmentos en una imagen el bloque $B \times B$ recorre toda la matriz A, al encontrar un bloque de la misma dimensión y con exactamente los mismos valores pondrá los dos bloques con un valor de 0, para identificar que dichos bloques son copia exacta uno del otro.

3.6 Resultados

El algoritmo de detección fue implementado en Matlab y probado en diferentes imágenes. Al procesar una imagen con el algoritmo de detección de zonas clonadas, entrega dos imágenes. En la primera imagen muestra la imagen que fue sometida al algoritmo de detección Figura 3.10. La segunda imagen muestra los bloques que fueron identificados como clonados y los pone en color blanco para que sea fácil ubicarlos Figura 3.11, aun cuando el algoritmo es muy preciso en este tipo de manipulación de imágenes, la interpretación humana sigue siendo necesaria para determinar cual zona fue copiada, en la figura 3.11 se puede ver que el bloque de color blanco que se muestra pegado del lado izquierdo es mayor que los otros dos y podemos determinar que se copiaron los segmentos de los otros dos bloques y fueron pegados en la zona donde se muestra el bloque de mayor tamaño, La figura 3.12 muestra la imagen original antes de ser manipulada.

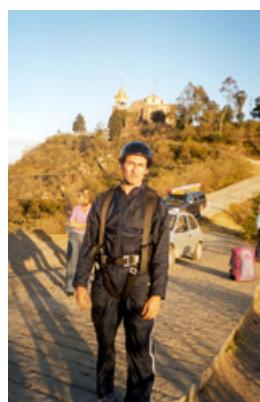


Figura 3.10 imagen que se analizara con el software de detección de zonas clonadas.

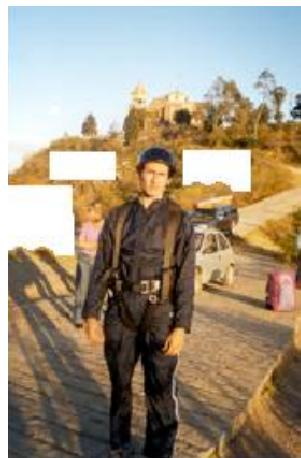


Figura 3.11 resultado después de haber sido sometida al software para detección de zonas clonadas.



Figura 3.12 imagen original antes de ser manipulada.

En la Figura 3.13 se presenta una imagen en la que se ven unos campos de futbol, a simple vista no se puede detectar ningún rastro de alteración la imagen parece común, una foto que podríamos decir de paisaje y la cual no oculta nada.



Figura 3.13 Imagen que será analizada con el software de detección de zonas clonadas.

La imagen de la Figura 3.13 es cargada en la herramienta para detección de zonas clonadas donde se lleva a cabo el proceso de análisis que se mostró en el diagrama de flujo del algoritmo de detección de zonas clonadas, una vez que la imagen ha sido analizada obtenemos los resultados mostrados en la Figura 3.14, en la que podemos ver marcadas en rojo una gran cantidad de zonas que fueron detectadas como zonas clonadas dentro de la imagen y en una zona muy concreta, lo cual lleva a pensar que en esa zona existía algo que se quiso ocultar.



Figura 3.14 resultado de la imagen después de haber sido sometida a revisión en el software de detección de zonas clonadas.

En la Figura 3.15 se puede ver la imagen original antes de ser manipulada y en la cual se muestra que la herramienta presentada en este capítulo para detección de zonas clonadas funciona de forma adecuada, detectando de forma fiable cualquier segmento que haya sido clonado dentro de la imagen, esto nos provee de un mecanismo de detección ante imágenes que hayan sido manipuladas.



Figura 3.15 imagen original antes de ser manipulada.

Capítulo IV

Análisis de la imagen mediante la dirección de la luz.

4.1 Introducción

En este capítulo se muestra una técnica para analizar imágenes digitales mediante el uso de las zonas de luz y sombra generadas por los objetos contenidos dentro de la imagen. Este procedimiento se lleva a cabo determinando las zonas de reflexión de luz de los objetos y estimando el ángulo de impacto de la fuente de luz en cada objeto dentro de la imagen. De esta manera se determina si todos estos objetos estuvieron incluidos desde el primer momento en que se tomó la imagen.

4.2 Manipulación de la imagen.

Imagine la creación de una imagen falsa que muestra a un par de rivales políticos conviviendo de forma amigable en un evento público. Para poder crear una imagen como la descrita sería necesario adjuntar información de una imagen en otra, en este caso sobreponer, o desplazar la imagen a un lado del político. El problema que se presenta en una manipulación de este tipo es que será sumamente difícil ajustar las dos imágenes para que muestren los mismos efectos de luz, así como la dirección de la misma. Analizando la diferencia que se pudiera presentar en la dirección de la luz, así como los efectos de la misma en los objetos dentro de la imagen, podemos determinar si una imagen ha sido manipulada o no. Como se muestra en la Figura 4.1, es una imagen compuesta en donde las dos personas que la componen fueron fotografiadas con diferentes posiciones y condiciones de luz.

La posición de la fuente de luz, así como su dirección, puede ser estimada por diferentes objetos o personas dentro de la imagen, la inconsistencia en estas estimaciones puede ser determinante para dictaminar la falsificación de una imagen. En este capítulo se describe una técnica para estimar la dirección de la luz en una imagen digital, y se demuestra su eficacia para el análisis forense de imágenes digitales.



Figura 4.1 Imagen falsificada en la que se muestra a un par de personajes políticos con diferentes tonos de brillo en el rostro.

4.3 Efecto de la luz en la fotografía digital.

Para comprender de mejor forma como afecta la luz las imágenes, es necesario saber que es la luz. "Luz" es una radiación electromagnética que viaja a través de las ondas. Las ondas de esta radiación pueden tener diferentes longitudes, espectro de luces (la distancia entre los picos de las ondas). Las longitudes de onda pueden ir desde ultra pequeñas (rayos x por ejemplo) a un amplio rango (como las radio transmisiones). Esto tiene su explicación en el espectro de luz. El espectro de luz va desde azules a rojos, o rojos y azules. Más allá de los rojos son los llamados rayos x, y más allá de los azules son los llamados ultravioleta, y solamente una porción de ese espectro es la que el ojo humano puede percibir. La luz sensible al ojo humano "luz visible" es realmente una minúscula porción de este amplio rango o espectro. Pequeñas variaciones en las longitudes de onda crean esta luz visible en el espectro y eso nos hace ver diferentes colores. Por ejemplo la luz azul tiene una longitud de onda más pequeña que la luz roja.

Ahora se analizará por qué el ojo humano ve los objetos de cierto color. Cuando la luz (radiaciones Electro Magnéticas) caen sobre un objeto, algunas de esta radiaciones son absorbidas por el objeto y convertidas en calor, y otra parte es reflejada fuera de la superficie del objeto hasta nuestros ojos. Algunos materiales tienden a absorber más de una cierta longitud de onda del espectro visible, y menos de esa longitud de onda es reflejada a nuestros ojos. Así, un objeto que podemos ver como azul significa que la superficie del objeto absorbe mucha menos longitud de onda por lo cual da una luz azul, por ello las longitudes de onda de la luz que alcanza a percibir el ojo serán dominadas por estas que dan una luz azul. Esta información debería aclarar más o menos el comportamiento de la luz. Cuando se ve un objeto es porque la luz es reflejada desde la superficie hacia tus ojos, toda luz que impacta en un objeto refleja luz. Se puede establecer el color de un objeto por los parámetros convenientemente llamados color de reflexión. Otro punto importante es que puesto que esta luz es absorbida por la superficie, no hay manera de que la superficie nos refleje mucha más luz de la que está recibiendo.

Lo que marca la diferencia entre una superficie que refleja la luz perfectamente como un espejo, y una superficie que no lo hace como una alfombra, es la rugosidad en la superficie. Cuando una superficie es casi perfectamente lisa, los rayos de luz que se reflejan desde la superficie son más o menos uniformes en la dirección que toman y esto crea una imagen clara del entorno que está siendo reflejado a los ojos (o en el caso de las imágenes digitales a la cámara digital) desde la superficie del objeto. Por otra parte, si la superficie es muy rugosa, los rayos que llegan rebotarán en direcciones aleatorias desde la superficie dando una imagen muy rugosa del entorno de vuelta a los ojos.

Al tener menor rugosidad significa que la superficie reflejará la luz que le llega de un modo perfecto, obteniendo lo reflexiones especulares (brillos). Lo contrario a las reflexiones especulares es cuando la imagen tiene Lambertian, lo que significa que todas las luces son reflejadas en la superficie en un modo

difuso (sin brillo), la superficie absorbe una gran cantidad de la luz y es por ello que esta misma no es reflejada.

4.4 ¿Porque un objeto puede ser más o menos transparente?

La radiación electro magnética (Luz), incluso la visible porción de ella, no sólo golpea la superficie de un objeto y rebota, sino que también penetra en la superficie. La penetración de esta radiación en la superficie depende mucho de que tan denso es el objeto. Más densidad significa más átomos, de esta forma los rayos de luz se introducen en el objeto y chocan con sus átomos haciéndole perder energía. Se puede decir que los rayos de luz son absorbidos más rápidamente que los átomos son golpeados. Algunos rayos de luz pueden atravesar el objeto entero. Si no hay suficiente densidad para absorberlo todo, los rayos de luz atraviesan el objeto. Los objetos entonces llegan a ser transparentes. Cuantos más rayos de luz atraviesen al objeto, más transparente será.

Algunas longitudes de onda son absorbidas más rápidamente que otras, dependiendo entre otras cosas de las propiedades del material por el que pasan. Es por eso que se ven cristales tintados. Un cristal verde significa que todas las longitudes de onda excepto estas que dan luz verde han sido absorbidas y mirando a través de este cristal se puede ver que todas las cosas tienen un aspecto verdoso. Teniendo todo esto en cuenta, el parámetro distancia de atenuación, significa cuanta distancia puede atravesar un rayo de luz un objeto antes de que la mitad de su energía sea absorbida. Por ejemplo, si tenemos un objeto de 1 cm de grosor y se establece la distancia de atenuación a 1 cm, significa que la mitad de la energía de todos los rayos que lo atraviesan será absorbida, así que la luz que cae a través del objeto será la mitad de brillante que en la del otro lado.

4.5 Generación de sombra

Una sombra es una región de oscuridad donde la luz es obstaculizada. Una sombra se genera en el espacio que existe detrás de un objeto opaco con una fuente de luz frente a él. La sección eficaz de una sombra es una silueta bidimensional o una proyección invertida del objeto que bloquea la luz.

Mientras mayor sea el ángulo entre la dirección de la luz y un objeto alargado que la obstaculice, más corta será su sombra. Por otro lado, mientras menor sea el ángulo entre la fuente de luz y la superficie en la que aparece la sombra, más larga será ésta. Si el objeto está cerca de la fuente de luz, la sombra será mayor que si el objeto se encuentra lejos. Si la superficie está curvada y no es uniforme, habrá más distorsiones de la sombra proyectada por el objeto que la genera.

Cuanto más ancha es la fuente de luz, más difuminada o borrosa será la sombra.

Si hay múltiples fuentes luminosas, habrá múltiples sombras, con las partes solapadas más oscuras, o con una combinación de colores. Cuando una persona o un objeto está en contacto con la superficie, como una persona sentada en el suelo o un poste clavado, las sombras convergen al punto de contacto.

Si existe una sola fuente de luz, las sombras arrojadas por la misma siempre serán grises, no importando el color de la fuente de luz. Sin embargo, si existen dos fuentes de luz de diferente color, supongamos verde y azul, las sombras proyectadas por cada una de ellas serán del color de la otra fuente de luz, y sólo la zona en donde se intersectan ambas sombras será gris. Es decir, la sombra de la luz verde será azul, pues está iluminada por la fuente azul, y viceversa. En el caso de existir más fuentes de luz, cada sombra será del color resultante de la adición de las fuentes que aún iluminan esa zona, permaneciendo en gris las zonas donde intersecten las sombras de todas las fuentes luminosas.

4.6 Metodología

Se presenta una técnica probada en imágenes capturadas al aire libre en un día claro y soleado (En donde existe una fuente de luz infinita), de igual forma se usaron imágenes controladas en un ambiente que permitiera hacer mediciones sobre objetos afectados por una única fuente de luz. Estas imágenes fueron capturadas con una cámara Lumix DMC-FX07 con lente LEICA a una resolución de 8.0 megapixeles, en un formato de compresión JPEG.

La dirección de la Luz fue estimada localizando manualmente lo puntos límite de la imagen

Existen algunas técnicas que permiten detectar si una imagen ha sido modificada observando las inconsistencias en las propiedades de dicha imagen. Estas inconsistencias pueden aparecer como desviaciones abruptas o inesperadas de la norma de la imagen ó como similitudes incorrectas sobre la imagen, presentado en el capítulo 3 de la presente tesis. Este fenómeno ha sido estudiado en [1] y [2] en donde el trabajo de dichas técnicas de detección de alteración de imágenes, consiste primeramente en identificar los cambios estadísticos asociados a la manipulación de la imagen. Se han estudiado otras técnicas como [3] en la que se presenta una forma de detección de alteraciones en imágenes digitales asumiendo que se poseen otras imágenes tomadas de la misma cámara con la que se tomó la imagen que se está analizando. Este método se basa en detectar patrones de ruido en algunas regiones de la imagen, creados por la cámara, única característica estocástica presentada por el censor CCD (Charged Couple Device). Sin embargo en este trabajo el método que se utiliza para detectar si una imagen ha sido modificada o no, es estimando la dirección de incidencia de la luz sobre los objetos de la imagen.

Posteriormente se compara la dirección de luz estimada para cada objeto con la dirección de luz estimada para el resto de los objetos, y así se detecta si fue modificada o si se encuentra en su estado original.

4.7 Desarrollo de la metodología propuesta

Para poder hacer un análisis sobre las imágenes digitales usando la técnica propuesta, se debe considerar que las imágenes deben cumplir con las siguientes características; a) Los objetos contenidos en la imagen deben generar reflexión de la luz que ilumina su superficie, y al menos en algunos de estos segmentos donde se refleja luz, la superficie debe ser uniforme para poder generar una reflexión constante. b) La superficie debe ser iluminada por una sola fuente de luz. c) Los objetos contenidos dentro de la imagen deben generar sombras.

En el siguiente ejemplo se tiene una imagen que cumple con los requisitos descritos. Ejemplo: Considérese la imagen de la figura 4.2 la cual fue tomada a las 5 de la tarde, con una cámara digital Lumix, lente leica con resolución de 8.0 mega píxeles, en formato JPG con máxima calidad. Esta imagen se usó para desarrollar nuestra técnica, porque satisface los requisitos establecidos anteriormente, ya que fue tomada en un día soleado, al aire libre, y las superficies donde impacta la luz solar y en donde se generan sombras son lo suficientemente uniformes para hacer nuestros cálculos. El método de análisis que se propone consta de los siguientes pasos:

- 1) Binarizar la imagen, esto funciona para este análisis en específico por las características de nuestra imagen, pero tal vez en otras se tenga que hacer otro procedimiento que permita identificar bien las sombras, como ajustar los niveles de brillo y contraste.
- 2) Establecer los ejes de referencia.
- 3) Trazar un triángulo usando los ejes de referencia y las sombras proyectadas del objeto a analizar en la imagen.
- 4) Usando la ley de cósenos estimar el ángulo con el que la fuente de luz impacta el objeto.
- 5) Repetir el procedimiento para otro objeto de la imagen.
- 6) Comparar los ángulos obtenidos.
- 7) Dictaminar si la imagen ha sido manipulada.



Figura 4.2 imagen para hacer análisis de ángulo de incidencia.

La imagen de la Figura 4.2 se binariza, el resultado será la imagen mostrada en la figura 4.3, esto se hace con el fin de determinar detalladamente la sombra que genera el individuo dentro de la imagen, ya que será en base a esa misma sombra con la que se hará el análisis.



Figura 4.3 Imagen binarizada para pruebas.

El siguiente paso será trazar los ejes que servirán para calcular el ángulo con el que la luz impacta al individuo, esto lo podemos ver en la figura 4.4.

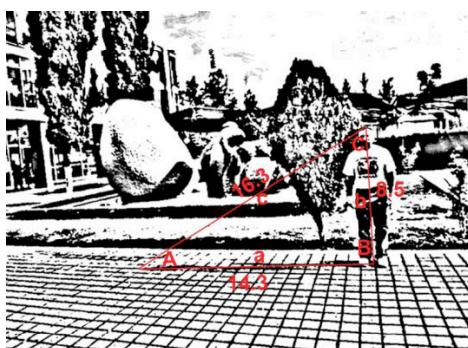


Figura 4.4 extracción de medidas para calcular ángulo.

En la Figura 4.4 podemos ver las medidas que se toman de la imagen. En primer lugar trazamos un triángulo en base a tres puntos: 1. La parte más alta del sujeto a analizar, ya que esta parte será la que genere la punta de la sombra 2. La proyección de la sombra del mismo, tomando la punta de esta

como referencia 3. La base del sujeto tomado por la mitad de su cuerpo en la parte más baja del mismo. Después se traza un triangulo con relación a estos puntos y sacamos la longitud de cada uno de sus lados como se muestra en la figura 4.4. Utilizando la función trigonométrica que relaciona a los lados conocidos con el ángulo se obtiene el ángulo de impacto con el que la fuente de luz golpea al objeto.

$$a^2 = b^2 + c^2 - 2bc \cos A$$

Ecuación 1.

$$\cos^{-1} A = \frac{b^2 + c^2 - a^2}{2bc}$$

Ecuación 2.

Sustituyendo las literales por sus valores numéricos obtenemos el siguiente resultado.

$$\cos^{-1} A = \frac{(8.5)^2 + (16.3)^2 - (14.3)^2}{2(8.5)(16.3)}$$

Ecuación 3.

$$\cos^{-1} A = \frac{133.45}{277.1}$$

$$\cos^{-1} A = 0.481595092$$

$$A = 6121'$$

Así se obtiene que el ángulo con el que la luz incide sobre el objeto es $A = 6121'$.



Figura 4.5 ángulo calculado para la persona que aparece en la foto.

Todos los objetos contenidos dentro de esta imagen tendrán el mismo ángulo o uno muy parecido. Esto ocurrirá siempre y cuando los objetos en la imagen se encuentren desde el primer momento en que se tomó la imagen original. Considérese ahora otro objeto en este caso el árbol. Aplicando el mismo procedimiento.

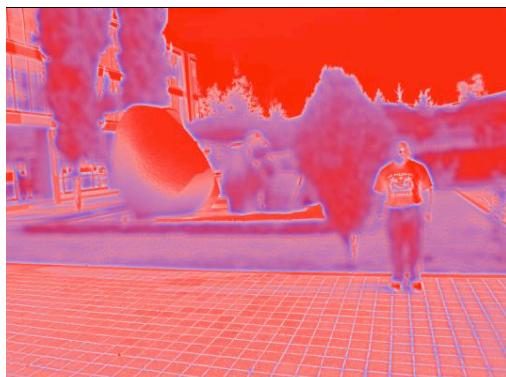


Figura 4.6 imagen para extraer las medidas del árbol y comparara su ángulo con el de la persona.

En la figura 4.6 se generó una extrapolación de la imagen usada en la prueba, para definir un poco más la sombra y poder hacer el cálculo de la longitud proyectada en el piso. Siguiendo la ley de cósenos para determinar el ángulo en A se obtienen los siguientes datos.

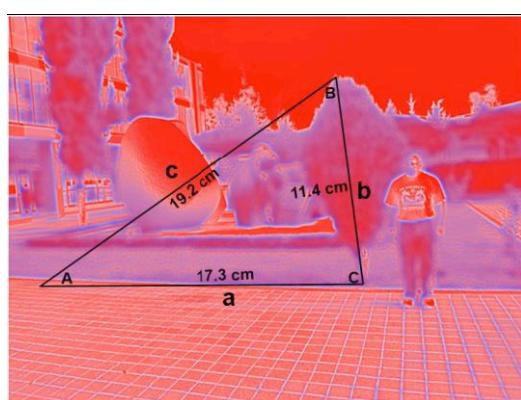


Figura 4.7 medidas del árbol para obtener su ángulo.

Calculando el ángulo en A tenemos:

$$a^2 = b^2 + c^2 - 2bc \cos A$$

Ecuación 4.

$$\cos^{-1} A = 0.455295138$$
$$A = 62^\circ 54'$$

Si se comparan los resultados obtenidos para la estimación en la figura 4.5 y figura 4.7, el ángulo de impacto es de $A = 6121'$ y $A = 6254'$ grados respectivamente, lo cual confirma la teoría de que todos los objetos contenidos en una imagen deben de poseer un ángulo de impacto de la fuente de luz igual o muy parecida.

Adicionalmente se estima la razón de los ángulos obtenidos para tener un criterio de comparación normalizando a 1, mientras mas cerca este a 1 será mejor, así obtenemos para este caso un valor de 0.9787.

Conclusiones

Aún cuando la falsificación de imágenes no es un fenómeno nuevo, la disponibilidad de tecnología para imágenes digitales y el software de procesamiento de imágenes hacen realmente fácil la falsificación de imágenes digitales para cualquier persona. En la actualidad se pueden ver imágenes digitales manipuladas en todos lados, en la televisión, revistas, periódicos, espectaculares, revistas científicas, etc. Estas imágenes pueden tener un gran impacto en la sociedad. Es entonces cuando se ve una clara necesidad de herramientas que permitan determinar la autenticidad de las imágenes digitales. La informática forense surge como la ciencia encargada de hacer el análisis "post mortem" de los equipos informáticos, identificando las causas y el posible culpable que ocasionó el daño a equipos informáticos o información digital. La forensia digital se encarga de analizar las imágenes digitales buscando mitigar el problema de la falsificación de imágenes digitales, aún en la ausencia del uso de hardware especializado o marcas de agua que facilitarían el análisis de la integridad de las imágenes. La forensia en imágenes digitales asume que las imágenes poseen ciertas características y regularidades estadísticas que pueden ser cuantificables, tales como las características del ambiente donde fue capturada la imagen y el mismo proceso interno de la cámara para formar dicha imagen. Mediante el análisis forense a imágenes digitales se pueden exponer o identificar estas irregularidades para detectar cambios en la imagen, lo cual evidenciará la falsificación de una imagen.

La primera herramienta forense presentada en esta tesis explota la correlación que se presenta cuando se ha manipulado una imagen mediante la técnica de clonación de zonas. Cuando se falsifica una imagen digital copiando partes de la misma imagen y se pegan en otro segmento de la imagen, esto presenta un fenómeno muy poco probable de ocurrir en una imagen digital y es que se presentarán bloques de píxeles exactamente iguales dentro de la imagen digital, esto es muy difícil si se tiene en cuenta que para imágenes con una profundidad de 8 bits un píxel puede tomar un valor de entre 16777216 posibilidades, así que la herramienta desarrollada y presentada en esta tesis busca identificar dicha correlación entre bloques, los identificará y marcará para que puedan ser ubicados por quien realiza el análisis de la imagen, cabe mencionar que esta herramienta solo funciona para dicho tipo de falsificación (zonas clonadas en una imagen), y su efectividad depende en gran medida de la adecuada interpretación que el analista haga de los resultados arrojados por el programa, para determinar qué zona de la imagen es la que se ocultó.

La técnica presentada en el capítulo cuatro explora las regularidades presentadas en la imagen digital generadas por el ambiente en el cual fue capturada dicha imagen, y esta técnica trabaja asumiendo que existe una sola fuente de luz a una distancia muy lejana y que la imagen es capturada al aire libre en un día razonablemente claro o en un lugar cerrado con una buena luz.

Se describe como estimar el ángulo con el que la luz incide sobre un objeto en la imagen, y se define un método para comparar la estimación presentada en diferentes objetos de la imagen. Se muestra el resultado en el análisis a una imagen digital real.

Una limitante que presenta esta técnica es la intensidad de la fuente de luz, ya que si esta no es lo suficientemente potente el contorno de las sombras generadas por el objeto a estimar será difuso y no se podrán determinar con exactitud los puntos que sirven para hacer su análisis. Un método que sirve para mitigar este problema es hacer pasar la imagen a analizar por un filtro pasa-bajas¹⁸, con esto conseguiremos delimitar un poco más las zonas de sombras para así obtener un mejor patrón de referencia para su estimación.

Aun cuando la herramienta y técnicas presentadas en esta tesis pueden ser un punto de partida para futuros trabajos, es importante considerar los diferentes tipos de falsificación de imágenes que existen, para crear otras herramientas que ayuden a identificar estos diferentes tipos de falsificaciones. Las técnicas y herramienta mostradas en esta tesis fueron diseñadas para identificar específicamente dos diferentes tipos de falsificación de imágenes, y pueden identificar la manipulación de imágenes siempre y cuando hayan sido sometidas a alguna de las falsificaciones para las cuales están diseñadas estas herramientas. Estas herramientas no son prácticas cuando se tiene que analizar una gran cantidad de imágenes, ya que los procesos a los cuales es sometida la imagen para extraer la información son lentos.

Aun cuando estas herramientas son efectivas en el análisis para el cual fueron diseñadas, pueden llegar a tener problemas, por ejemplo, en el análisis de las imágenes mediante la dirección de luz si la imagen falsificada se produce con mucho cuidado y detallando todo a la perfección será sumamente difícil establecer los parámetros que permitan determinar la originalidad o no de dicha imagen. En el caso de las zonas clonadas si la imagen se reinterpola se insertarían nuevos valores de pixeles perdiendo esa correlación entre los bloques copiados y la zona donde fueron pegados. Ninguna de estas técnicas es completamente efectiva cuando la falsificación es realizada por una persona con buenos conocimientos en la falsificación de imágenes y uso de herramientas de procesamiento digital.

El análisis forense en imágenes digitales está en una etapa temprana, es un tema de investigación relativamente nuevo, y existen muchas cosas que investigar. Es nuestra intención que este trabajo de tesis contribuya a comprender de mejor forma las imágenes digitales y los procesos de las mismas. Adicionalmente la intención es hacer más difícil el trabajo de quienes falsifican imágenes digitales

¹⁸ Los filtros pasa-bajas enfatizan las bajas frecuencias, suavizando las imágenes y suprimiendo ruidos. Se trata de asemejar los valores de los píxeles vecinos, reduciendo la variabilidad espacial de la imagen. Ello produce un adelgazamiento de los bordes, perdiéndose en nitidez visual de la imagen, pero ganando en homogeneidad.

Bibliografía

- [1] **J. Lukas and J. Fridrich.** Estimation of primary quatization matrix in double compressed, Proc. Of DFRWS, 2003
- [2] **A. C. Popescu and Hany Farid.** Estadistical Tools for Digital Forensics. Proc of IHW, 2006
- [3] **Jan Lukás, Jessica Fridrich y Miroslav Goljan.** Detecting Digital Image Forgeries Using Sensor Pattern Noise, Department of Electrical and Computer Engineering SUNY Binghamton, Binghamton NY, 2005.
- [4] **Scientific Working Group on Imaging Technology,** Best Practices for forensics image analysis, section 12, 2007.
- [5] **Micah Kimo Johnson,** Lighting and Optical Tools for Image Forensics, PhD Thesis, DartMouth College, Hanover Newhampshire, Septiembre 2007.
- [6] **Micah Kimo Johnson, Hany Farid.** Exposing Digital Forgeries in Complex Lighting Environments, DartMouth College, Hanover Newhampshire.
- [7] **Hany Farid, Micah Kimo Johnson.** Exposing Digital Forgeries Through Specular Highlights on the Eye, DartMouth College, Hanover Newhampshire.
- [8] **"Understanding How Image Sensors Work"**,<http://www.shortcourses.com/how/sensors/sensors.htm>. Septiembre 2007.
- [9] **"A CONVERSATION WITH HANY FARID; Proving That Seeing Shouldn't Always Be Believing"**
<http://query.nytimes.com/gst/fullpage.html?res=9905E2D7173EF931A35753C1A9619C8B63> Octubre 2007.
- [10] **"Tell-All PCs and Phones Transforming Divorce"**
<http://www.nytimes.com/2007/09/15/business/15divorce.html>, Octubre 2007
- [11] **Mariana Monzoy Villuendas, Aarón Ruiz Zúñiga, Mariko Nakano Miyatake y Héctor Pérez Meana** "Marca de Agua Semifrágil para Autenticación de Imágenes Digitales", Sección de estudios de posgrado e investigación unidad Culhuacan, Escuela Superior de Ingeniería Mecánica y Eléctrica. Instituto Politécnico Nacional. Conferencia Mexicana de Seguridad Informática, Noviembre 2006
- [12] **Xiang Zhou, Xiaohui Duan, Daoxian Wang** "A semi-Fragile watermark scheme for image authentication" International Conference on Multimedia Modeling, septiembre 2004

- [13] **William K. Pratt** DIGITAL IMAGE PROCESSING, Third Edition, John Wiley & Sons, Inc. 2001.
- [14] **Tian-Tsong Ng, Shih-Fu Chang, Ching-Yung Lin, Qibin Sun.** Passive-blind Image Forensics, Department of Electrical Engineering Columbia University, Junio 23, 2006.
- [15] **Micah K. Jhonson, Hany Fard.** Exposing Digital Forgeries Through Chromatic Aberration, Department of Computer Science Dartmouth College Hanover, NH.
- [16] **Alin C. Popescu.** Exposing Digital Forgeries in Color Filter Array Interpolated Images, Dartmouth College, 2005.
- [17] **Robert Fiete.** Photo Fakery, ITT Industries, Enero 2005.
- [18] **Hany Farid.** Digital Image Ballistic from JPEG Quantization, Department of computer Science Dartmouth College, Hanover, 2006.
- [19] **Erik Valdemar Cuevas, Daniel Zaldivar Navarro.** Visión por Computadora utilizando MatLAB y el Toolbox de Procesamiento Digital de Imágenes.
- [20] **Cox, I., Miller, M.L., and Bloom, J.A.:** *Digital Watermarking*, Morgan Kaufmann, San Francisco, 2001.

Lista de tablas y figuras.

Figura 1.1 Foto en Marte de la NASA	1
Figura 1.2 Foto Lenin y Trotsky	2
Figura 1.3 Imagen Ejercito ingles falsificada	3
Figura 1.4 Imagen guerra de Irak	4
Figura 1.5 Portadas de revistas	5
Figura 1.6 Proceso de evaluación de imagen con DVK-E1	6
Figura 1.7 Fases de adquisición de una imagen digital	9
Figura 1.8 Adherencia de ruido en imágenes	10
Figura 2.1 Ajuste de contraste en imagen	16
Figura 2.2 Ajuste de brillo en imagen	16
Figura 2.3 Imagen para extraer meta datos	20
Figura 2.4 Meta datos de imagen	20
Figura 2.5 Estimación de dimensiones	21
Figura 3.1 Pozos del Charged Couple Device	25
Figura 3.2 Semiconductor	26
Figura 3.3 Proceso del filtro de Bayer	26
Figura 3.4 Imagen ejemplo para interpolación	26
Figura 3.5 Ejemplo interpolación	27
Figura 3.6 Acercamiento a una imagen para ver los pixeles	28
Figura 3.7 Imagen con extracción de pixeles	29
Figura 3.8 Imagen falsa con clonación de zonas	30
Figura 3.9 Imagen ejemplo de clonación de zonas	31
Figura 3.10 Imagen para analizar por zonas clonadas	33
Figura 3.11 Resultado después de ser analizada	34
Figura 3.12 Imagen original	34
Figura 3.13 Imagen para analizar	34
Figura 3.14 Resultado de imagen	35
Figura 3.15 Imagen antes de falsificarse	35
Figura 4.1 Imagen falsa rivales políticos	36
Figura 4.2 Imagen para analizar	41
Figura 4.3 Imagen binarizada	41
Figura 4.4 Extracción de medidas	41
Figura 4.5 Ángulo calculado	43
Figura 4.6 Extracción medidas árbol	43
Figura 4.7 Medidas del árbol	43

Anexo

Artículos y Conferencias

Análisis forense en imágenes digitales usando la incidencia de la luz en los objetos contenidos dentro de la imagen

Ing. Marcos A. Rosales García, M. en C. Rubén Vázquez Medina

Escuela Superior de Ingeniería Mecánica y Eléctrica unidad Culhuacan IPN

Av. Santa Ana No 1000 Col. San Francisco Culhuacan México D.F. Tel. 57296000 Ext. 73262, Fax 56562058

E-mail marcosrosales@gmail.com

Resumen: En este trabajo se muestra una técnica para analizar imágenes digitales, mediante el uso de las zonas de luz y sombra generadas por los objetos contenidos dentro de la imagen. Este procedimiento se lleva a cabo determinando las zonas de reflexión de luz de los objetos y estimando el ángulo de impacto de la fuente de luz en cada objeto, dentro de la imagen. De esta manera se determina si todos ellos estuvieron incluidos desde el primer momento en que se tomó la imagen.

Introducción

En la actualidad las imágenes tienen un gran impacto en la vida diaria, son una forma de representar muchas situaciones y eventos que suceden a diario. Las imágenes que vemos todos los días van desde publicitarias, con fines de mercadeo, hasta imágenes informativas que representan la noticia del día. Muchas de estas imágenes son manipuladas digitalmente y tal vez, en su mayoría, no exista ningún problema por dicha manipulación. Pero habrá algunas imágenes que por la naturaleza de la información que representan se tiene que garantizar su autenticidad, detectando si han sido manipuladas.



Figura 1

Un ejemplo trivial se muestra en la Figura 1, donde se puede ver que la composición digital en la imagen del presidente de Cuba, Fidel Castro, lado izquierdo es distinta a la composición digital de la imagen del presidente de los Estados Unidos de América, George W. Bush, lado derecho. En esta imagen se nota la ausencia de reflexión de luz en el rostro del presidente George W. Bush, lo cual demuestra que las imágenes fueron tomadas en diferentes ambientes de luz.

Imagine la falsificación de una imagen digital en la cual se muestra a un par de rivales políticos conviviendo de forma muy amigable. Esta imagen se crearía fusionando las dos imágenes que muestran individualmente a cada uno de los políticos. Para superar la detección trivial como en el caso de la figura 1, se debería hacer coincidir los efectos de la luz en las imágenes sobreuestas, así como la dirección de los rayos de luz (ejemplo, el sol en un día claro). Esta tarea no es fácil pero tampoco imposible, y durante la fase de detección de modificación se debe considerar que es posible hacerlo. Sobre todo por las facilidades que ofrecen las herramientas de edición de imágenes actuales, no bastará sólo con hacer un análisis visual superficial, se debe contar con técnicas especializadas que detecten si una imagen ha sido modificada.

Otra imagen en donde se puede detectar la manipulación de la misma, utilizando el análisis de las zonas de luz, sombras, y el ángulo con el que la luz golpea los objetos, es la presentada en la figura 2¹, en esta imagen se puede ver como la luz está golpeando en diferentes direcciones las pantorrillas de los dos actores que aparecen en ella, del lado Izquierdo Brad Pitt la luz le golpea del lado derecho hacia el izquierdo en sus pantorrillas, mientras que a la actriz Angelina Jolie la luz le golpea del lado izquierdo hacia el derecho en las pantorrillas, por lo tanto podemos decir que las imágenes fueron tomadas en diferentes habitaciones de luz y montadas en un escenario en el que tal vez

ROC&C'2007 – CP-27 PONENCIA RECOMENDADA
POR EL **COMITÉ DE COMPUTACIÓN**
DEL **IEEE SECCIÓN MÉXICO** Y PRESENTADA
EN LA **REUNIÓN DE OTOÑO, ROC&C'2007**,
ACAPULCO, GRO., DEL 25 AL 30 DE NOVIEMBRE DEL 2007.

¹ Imagen tomada de www.ams.org/images/aaas2007-pitt-jolie.jpg

ninguno de los dos se encontró originalmente, lo que es seguro es que al menos uno de los dos sujetos no estaba cuando se tomó la imagen original.



Figura 2

1. Metodología de análisis para imágenes digitales

Existen diferentes técnicas que permiten detectar si una imagen ha sido modificada observando las inconsistencias en las propiedades de dicha imagen. Estas inconsistencias pueden aparecer como desviaciones abruptas o inesperadas de la norma de la imagen ó como similitudes incorrectas sobre la imagen. Este fenómeno ha sido estudiado en [1] y [2] en donde el trabajo de dichas técnicas de detección de alteración de imágenes, consiste primeramente en identificar los cambios estadísticos asociados a la manipulación de la imagen. Se han estudiado otras técnicas como [3] en la que se presenta una forma de detección de alteraciones en imágenes digitales asumiendo que se poseen otras imágenes tomadas de la misma cámara con la que se tomó la imagen que se está analizando. Este método está basado en detectar patrones de ruido en algunas regiones de la imagen, creados por la cámara, única característica estocástica presentada por el sensor CCD (Charged Couple Device). Sin embargo en este trabajo el método que se utiliza para detectar si una imagen ha sido modificada o no, es estimando la dirección de incidencia de la luz sobre los objetos de la imagen. Posteriormente se compara la dirección de luz estimada para cada objeto con la dirección de luz estimada para el resto de los objetos, y así se detecta si fue modificada o si se encuentra en su estado original.

2 Desarrollo de la metodología propuesta

Para poder hacer un análisis sobre las imágenes digitales usando la técnica propuesta, se debe considerar que las imágenes deben de cumplir con las siguientes características; a) Los objetos contenidos en la imagen deben generar reflexión de la luz que ilumina su superficie, y al menos en algunos de estos segmentos, donde se refleja luz, la superficie debe ser uniforme para poder generar una reflexión constante. b) La superficie debe ser iluminada por una sola fuente de luz. c) Los objetos contenidos dentro de la imagen deben generar sombras.

En el siguiente ejemplo se tiene una imagen que cumple con los requisitos descritos.

Ejemplo:

Considérese la imagen de la figura 3 la cual fue tomada a las 5 de la tarde, con una cámara digital Lumix, lente Leica con resolución de 8.2 mega píxeles, en formato JPG con máxima calidad. Esta imagen se usó para desarrollar nuestra técnica, porque satisface los requisitos establecidos anteriormente, ya que fue tomada en un día soleado, al aire libre, y las superficies donde impacta la luz solar y en donde se generan sombras son lo suficientemente uniformes que nos permita hacer nuestros cálculos.

El método de análisis que se propone consta de los siguientes pasos:

1)Binarizar la imagen, esto funciona para este análisis en específico por las características de nuestra imagen, pero tal vez en otras, se tenga que hacer otro procedimiento que permita identificar bien las sombras.

2)Establecer los ejes de referencia.

3)Trazar un triángulo usando los ejes de referencia y las sombras proyectadas del objeto a analizar en la imagen.

4)Usando la ley de cósenos estimar el ángulo con que la fuente de luz impacta el objeto.

5)Repetir el procedimiento para otro objeto de la imagen.

6)Comparar los ángulos obtenidos

7)Dictaminar si la imagen ha sido manipulada



Figura 3

La imagen de la Figura 3 se binariza, esto se hace con el fin de determinar detalladamente la sombra que genera el individuo dentro de la imagen, ya que será en base a esa misma sombra con la que haremos nuestro análisis.



Figura 4

El siguiente paso será trazar los ejes que servirán para calcular el ángulo con el que la luz impacta al individuo, esto lo podemos ver en la Figura 5.

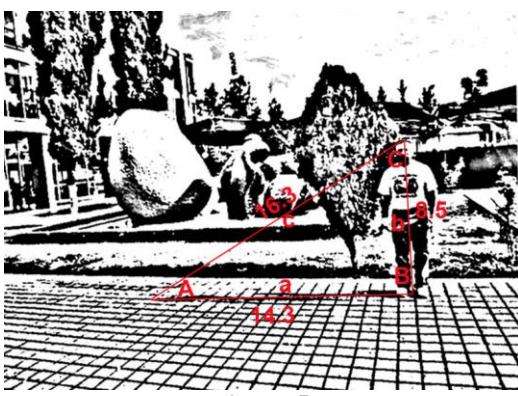


Figura 5.

En la Figura 5 podemos ver las medidas que se toman de la imagen. En primer lugar trazamos un triángulo en base a tres puntos: 1. la parte más alta del sujeto a analizar, ya que esta parte será, la que genere la punta de la sombra que será otro de los puntos que analizaremos 2. la

proyección de la sombra del mismo, tomando la punta de esta como referencia 3. la base del sujeto tomado por la mitad de su cuerpo en la parte más baja del mismo. Después trazamos un triángulo con relación a estos puntos y sacamos la longitud de cada uno de sus lados como se muestra en la figura 5.

Utilizando la función trigonométrica que relaciona a los lados conocidos con el ángulo se obtiene el ángulo de impacto con el que la fuente de luz golpea al objeto.

$$a^2 = b^2 + c^2 - 2bc \cos A$$

$$\cos^{-1} A = \frac{b^2 + c^2 - a^2}{2bc}$$

Sustituyendo las literales por sus valores numéricos obtenemos el siguiente resultado.

$$\cos^{-1} A = \frac{(8.5)^2 + (16.3)^2 - (14.3)^2}{2(8.5)(16.3)}$$

$$\cos^{-1} A = \frac{133.45}{277.1}$$

$$\cos^{-1} A = 0.481595092$$

$$A = 61^\circ 21'$$

Así se obtiene que el ángulo con el que la luz incide sobre el objeto es $A = 61^\circ 21'$.



Figura 6

Todos los objetos contenidos dentro de esta imagen tendrán el mismo ángulo o uno muy parecido. Esto ocurrirá siempre y cuando los objetos en la imagen se encuentren desde el

primer momento en que se tomó la imagen original. Considérese ahora otro objeto en este caso el árbol. Aplicando el mismo procedimiento.

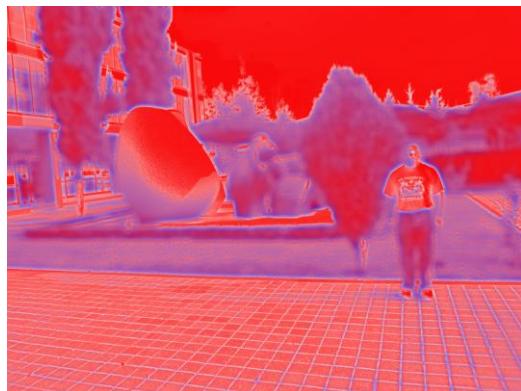


Figura 7

En la Figura 7 se generó una extrapolación de la imagen usada en la prueba, para definir un poco más la sombra y poder hacer el cálculo de la longitud proyectada en el piso.

Siguiendo la ley de cósenos para determinar el ángulo en A obtenemos los siguientes datos.

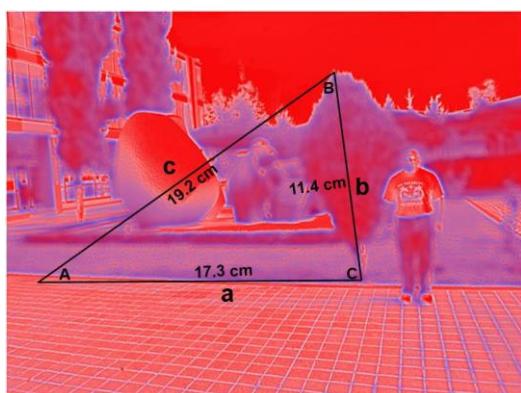


Figura 8

Calculando el ángulo en A tenemos:

$$a^2 = b^2 + c^2 - 2bc \cos A$$

$$\cos^{-1} A = 0.455295138$$

$$A = 62^\circ 54'$$

Si comparamos los resultados obtenidos para la estimación en la Figura 6 y Figura 8, el ángulo de impacto es de $61^\circ 21'$ y $62^\circ 54'$ grados respectivamente, lo cual confirma la teoría de que todos los objetos contenidos en una imagen deben de poseer un ángulo de impacto de la fuente de luz igual o muy parecida.

Adicionalmente se estima la razón de los ángulos obtenidos para tener un criterio de comparación normalizando a 1, mientras mas cerca este a 1 será mejor, así obtenemos para nuestro caso un valor de 0.9787.

Conclusiones

Se ha probado esta técnica analizando una imagen capturada en un espacio abierto, en un día despejado, lo cual permite que la luz natural golpee directamente a los objetos y estos generen sombras que sirvan para hacer el análisis, aunque esta misma técnica puede implementarse en imágenes tomadas en un salón cerrado, con la condición de que sólo exista una fuente de luz artificial y que ésta tenga una sola dirección. La imagen que se usó para hacer el análisis fue tomada con una cámara Lumix en formato de compresión JPEG.

La estimación de la dirección de la luz requiere que se localicen manualmente los límites de la sombra proyectada por el o los objetos a analizar y que ésta se pueda medir con respecto al objeto que la proyecta. Los tres puntos esenciales que se deben localizar; a) Es la parte más baja del objeto a medir, justo por la mitad del objeto y que hace contacto con la superficie, b) La parte más alta del objeto, y b) La parte donde termina la sombra, estos tres puntos se unen para generar el triángulo que sirve para estimar el ángulo de proyección de la luz, también es necesario que la superficie sobre la que se encuentran los objetos a analizar sea medianamente regular. En ocasiones la intensidad de la sombra no será lo suficientemente nítida que permita hacer la estimación de su longitud, así que se tendrá que generar un proceso que nos permita tener bien definida la sombra, en algunas ocasiones extrapolar la intensidad de la luz puede ayudar a este proceso.

El ángulo con el que la luz golpea a los diferentes objetos dentro de una imagen, puede variar un poco, esto depende de la distancia hacia la derecha o izquierda que exista entre los objetos a compararse, como pudo verse en el caso particular de las pruebas realizadas en el presente artículo la diferencia del ángulo con el que la luz golpea a los objetos que analizamos es mínima, esto se debe a que son objetos que se encuentran muy cerca uno del otro dentro de la imagen.

Bibliografía

- [1] **J. Lukas and J. Fridrich.** Estimation of primary quatization matrix in double compressed, Proc. Of DFRWS, 2003
- [2] **A. C. Popescu and Hany Farid.** Estadistical Tools for Digital Forensics. Proc of IHW, 2006
- [3] **Jan Lukás, Jessica Fridrich y Miroslav Goljan.** Detecting Digital Image Forgeries Using Sensor Pattern Noise, 2005
- [4] **Scientific Working Group on Imaging Technology,** Best Practices for forensics image analysis, section 12, 2007.
- [5] **Micah Kimo Johnson,** Lighting and Optical Tools for Image Forensics, PhD Thesis, DartMouth College, Hanover Newhampshire, Septiembre 2007.
- [6] **Micah Kimo Johnson, Hany Farid,** Exposing Digital Forgeries in Complex Lighting Environments, DartMouth College, Hanover Newhampshire.
- [7] **Hany Farid, Micah Kimo Johnson,** Exposing Digital Forgeries Through Specular Highlights on the Eye, DartMouth College, Hanover Newhampshire.
- [8] “**Understanding How Image Sensors Work**”,<http://www.shortcourses.com/how/sensors/sensors.htm>. Septiembre 2007.
- [9] “**A CONVERSATION WITH HANY FARID; Proving That Seeing Shouldn't Always Be Believing**” <http://query.nytimes.com/gst/fullpage.html?res=9905E2D7173EF931A35753C1A9619C8B63> Octubre 2007.
- [10]”**Tell-All PCs and Phones Transforming Divorce**”
<http://www.nytimes.com/2007/09/15/business/15divorce.html>, Octubre 2007

Currículum Vitae.



Marcos Arturo Rosales García, Nació en México D.F. en 1977, Ingeniero en Computación por la Universidad Nacional Autónoma de México (2004), candidato a Maestro en Ciencias por la Sección de Estudios de Posgrado e Investigación de la Escuela Superior de Ingeniería Mecánica Eléctrica unidad Culhuacan del Instituto Politécnico Nacional, profesor de la carrera de ingeniería en computación desde Enero del 2007. Sus áreas de interés son la seguridad en los sistemas de información, auditoria en sistemas, y análisis forense en imágenes digitales y sistemas informáticos.

Rubén Vázquez Medina, Nació en México D.F. en 1966 y es Ingeniero en Electrónica con especialidad en Comunicaciones por la Universidad Autónoma Metropolitana unidad

Iztapalapa (1989), obtuvo el grado de Maestro en Ciencias con especialidad en Telecomunicaciones en el Centro de Investigación y Estudios Avanzados del IPN (1994), y cuenta con los créditos por materias del Doctorado en Ciencias en la Universidad Autónoma Metropolitana unidad Iztapalapa. Desde 1997 es profesor investigador titular en la Sección de Estudios de Posgrado e Investigación de la Escuela Superior de Ingeniería Mecánica y Eléctrica unidad Culhuacan del IPN. Es profesor de la Maestría en Ciencias de Ingeniería en Microelectrónica y la Especialización en Seguridad Informática y Tecnologías de la Información en la ESIME Culhuacan. También es profesor invitado en la Maestría en Seguridad de la Información en la Secretaría de Marina Armada de México. Cuenta con 19 Artículos Publicados en Revistas Internacionales, 10 Artículos Publicados en Revistas Nacionales, 9 Proyectos Institucionales de Investigación, 56 Artículos en Congresos Internacionales y 33 Artículos en Congresos

Nacionales. Además, ha formado a 19 Maestros en Ciencias, dos de los cuales son de la Maestría en Seguridad de la Información de la SEMAR y 17 en el Instituto Politécnico Nacional. Sus áreas de interés son la seguridad informática, criptografía, esteganografía, la informática forense y la forensia digital.

Panorámica sobre el análisis forense de imágenes digitales

J. Baltazar – R. Vázquez – M. A. Rosales

Instituto Politécnico Nacional

SEPI - ESIME Culhuacan, México DF

[jbaltazar@gmail.com, ruvazquez@ipn.mx, marcosrosales@gmail.com]

Resumen: En este documento se examinan trabajos recientes con el propósito de mostrar las implicaciones de la forensia de imágenes digitales y los resultados que se han obtenido en esta dirección. Los trabajos que se analizan corresponden principalmente a aquellos que abordan el problema de la identificación de imágenes alteradas o falsificadas basándose en un análisis de las inconsistencias en las propiedades de la imagen y su proceso de adquisición. Se incluye un experimento para la detección de doble compresión en imágenes.

Introducción

La fotografía ha sido comúnmente aceptada como registro y prueba de la ocurrencia de un suceso real. Sin embargo hoy día, en esta era digital, con cámaras digitales de alta resolución a bajo costo, herramientas de edición de imágenes ampliamente difundidas y un poco de pericia, resulta fácil la generación de imágenes artificiales, siendo posible mostrar sucesos que nunca ocurrieron, y por otro lado también es sencillo alterar una fotografía digital original, al modificar su contenido y transmitir así información falseada. Como resultado de esta situación, se ha llegado a la conclusión de que no se puede dar por garantizada la autenticidad e integridad de una imagen digital. Esto afecta la credibilidad de la información que estas aportan, lo cual adquiere gran relevancia cuando se requiere tomar decisiones con base en imágenes digitales, que son presentadas como evidencia legal ante una corte.

Un tribunal podría tomar decisiones erradas que afecten la libertad de personas inocentes. Supóngase una fotografía digital de un accidente automovilístico en la que las placas de un auto son alteradas o una fotografía en la que se agregan o eliminan lesiones al rostro de una persona; y un posible montaje en una imagen digital usada para mostrar la participación de alguien en cierto acto ilícito.

Sin duda, una fuerte motivación para la investigación en este campo son las implicaciones legales. Es importante hacer notar que, así como existen ciertos criterios para validar una fotografía convencional, también es necesario establecer otros para autenticar y aceptar como evidencia legal imágenes digitales. Sobre este tema, un sistema legal de un país como México también las requiere. Considérese el caso de una persona que distribuye fotografías de pornografía infantil por Internet. Si fuese capturada podría alegar en su defensa que las imágenes no son reales, sino que fueron generadas por computadora, obtenidas al hacer montajes de fotografías. Este argumento lo podría librar de una penalización severa y no se haría justicia a las víctimas.

Se podría extender los casos a fotografía militar que identifique la ubicación de objetivos irreales o una imagen industrial que muestre problemas en materiales que generaría productos de consumo defectuosos y peligrosos. Ante los ejemplos mencionados, la distinción entre una imagen digital original y una versión modificada es de gran importancia.

Otro aspecto que atender, está relacionado con la necesidad de hacer correcciones y ajustes a una imagen digital con el fin de mejorar su calidad y extraer la información que aportan. Si la imagen es sometida a procesos, como por ejemplo, filtrado, compensación de color, ajuste de brillo o contraste, es importante mantener su integridad desde el momento de su captura hasta su uso final. Existen una serie de mejores prácticas recomendadas para la edición de imágenes digitales, las cuales pueden encontrarse en documentos del *Scientific Working Group on Imaging Technologies (SWGIT)* guidelines, donde se establece que cualquier procesamiento de imágenes

**ROC&C'2007 – CP-36 PONENCIA RECOMENDADA
POR EL COMITÉ DE COMPUTACIÓN
DEL IEEE SECCIÓN MÉXICO Y PRESENTADA
EN LA REUNIÓN DE OTOÑO, ROC&C'2007,
ACAPULCO, GRO., DEL 25 AL 30 DE NOVIEMBRE DEL 2007.**

digitales debe ser científicamente demostrable y repetible. El responsable de procesar una imagen debe tener procedimientos específicos orientados a asegurar un tratamiento confiable de las imágenes considerando una cadena de custodia, mecanismos de resguardo de imágenes originales y auditoria de cambios.

La investigación en la forensia de imágenes digitales, se centra en atender este tipo de cuestiones al proponer técnicas que buscan asegurar la integridad y autenticidad de imágenes digitales en ausencia de una marca de agua o firma digital. Estas técnicas están relacionadas con la identificación de imágenes alteradas o falsificadas a través de un análisis de las propiedades de la imagen, lo cual se hace estableciendo métricas y clasificadores que sirvan como referencia para poner al descubierto inconsistencias en las características subyacentes de una imagen que no son perceptibles a simple vista. De esta manera, la forensia digital da respuesta al cómo podría identificarse si una imagen es original o es resultado de un montaje, cómo saber si una imagen representa un suceso real o ha sido alterada para engañar al observador y cómo identificar que porciones de una imagen han sido modificadas.

Las marcas de agua [1, 2] han sido propuestas como mecanismos confiables de autenticación. Aunque la utilidad de una marca de agua requiere que ésta sea insertada al momento de la captura de la imagen, la mayoría de la tecnología de fotografía digital en el mercado no incluye este tipo de mecanismos.

En los últimos años ha habido una investigación creciente en el campo de la forensia digital de imágenes y comúnmente el trabajo contempla varios tipos de problemas:

- Identificación de la fuente de la imagen, para determinar con qué tipo de dispositivo específico fue obtenida una imagen (ej. cámara digital, escáner). Esto implica asociar una imagen con un tipo de dispositivos con características comunes y finalmente identificar un dispositivo fuente individual.
- Distinción entre imágenes artificiales generadas por computadora e imágenes originales que representan sucesos reales.
- Detección de falsificación o manipulación de imágenes, que han sido alteradas en su contenido sometiéndolas a procesos posteriores a su captura.

Este documento se centra en el último punto para dar un panorama de las técnicas de forensia en

imágenes digitales sobre las cuales se ha trabajado hasta ahora.

Detección de imágenes alteradas

La modificación de una imagen es una tarea relativamente sencilla, la detección de alteraciones es uno de los objetivos principales para la forensia de imágenes digitales. Esta detección se logra tomando como base el hecho de que, para crear una falsificación convincente, se requiere que la imagen sea sometida a distintos procesos como redimensionar, ampliar o rotar partes de la imagen, ajustar diferencias de brillo aplicando luminosidad, compensación de color y suprimir detalles mediante filtrado, compresión o adición de ruido. Es posible que estos procesos no dejen rastros visuales en la imagen que indiquen que ha sido alterada; sin embargo, sí alteran ciertas características y propiedades estadísticas de la imagen que, pueden introducir correlaciones específicas, las cuales al ser detectadas pueden usarse como evidencia de manipulación digital. Una posible clasificación de las técnicas de análisis que se enfocan en esta problemática, son las que se ocupan de detectar inconsistencias en las propiedades de una imagen y en el proceso de su adquisición, como las que se describen a continuación.

Inconsistencias en las propiedades de una imagen

Este tipo de técnicas trata de detectar imágenes alteradas basándose en variaciones inconsistentes de características seleccionadas a través de la imagen. Estas variaciones pueden aparecer como desviaciones abruptas de los clasificadores utilizados para medir las características propias de la imagen o como similitudes inesperadas sobre la imagen.

Uno de los primeros métodos de este tipo se basa en la presencia de doble compresión JPEG. La compresión de una imagen ya comprimida, a una diferente tasa de compresión o factor de calidad, distorsiona la uniformidad de los histogramas de coeficientes de la DCT (Discrete Cosine Transform) y genera patrones identificables en los nuevos histogramas de los coeficientes DCT.

Cuando la segunda tasa de compresión es menor, algunos elementos en los histogramas se hacen ceros, dando un patrón periódico de picos y valles. Por otra parte, cuando la segunda tasa de compresión es mayor que la primera, todos los valores del histograma estarán presentes pero con divisiones irregulares y mezcla de elementos del histograma; de

igual manera, presentará patrones periódicos de picos. Este fenómeno ha sido estudiado por Lukas *et al.* en [3] y en el 2006 por Popescu *et al.* [4], con enfoques similares, para determinar los parámetros de la compresión inicial y para detectar doble compresión en imágenes, para lo cual extraen las tablas de cuantización y generan los histogramas de los coeficientes DCT.

Para comprobar lo descrito en tales referencias, se realizó el experimento con una fotografía digital a color con dimensiones 2048x1536, tomada con una Sony DSC-P72. Los resultados de la implementación ejemplifican de manera directa la alteración en los histogramas de una imagen, como se aprecia en las siguientes figuras, donde la Figura 1 es la imagen original y la Figura 2 la misma imagen sometida a dos procesos de compresión JPEG de distintas magnitudes:



Figura 1. Imagen Original



Figura 2. Imagen con doble compresión

A simple vista las imágenes parecen ser idénticas, pero al analizar sus histogramas, se detecta la pérdida del patrón de correlación que presenta una imagen que no tiene una doble compresión. Tal y como se aprecia en la Figura 3 que muestra el histograma de la

imagen original y observando el histograma de la Figura 4 correspondiente a la imagen sometida al doble proceso de compresión, resulta evidente la alteración que se genera, presentando valores irregulares.

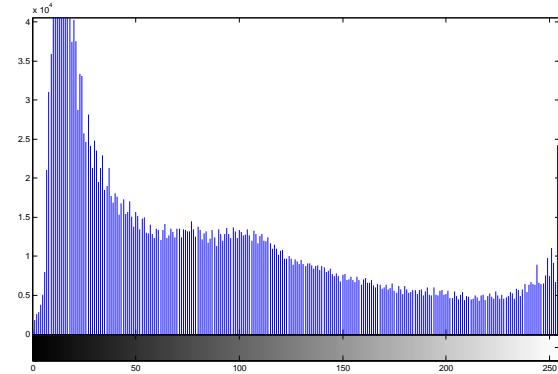


Figura 3. Histograma de imagen sin doble compresión.

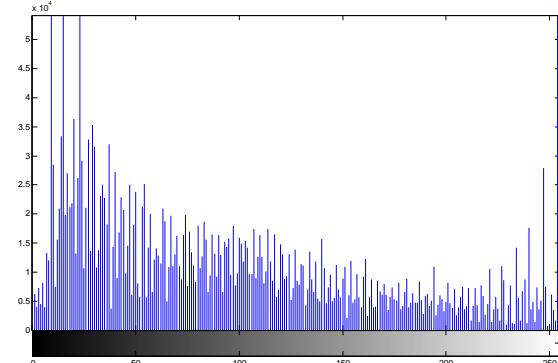


Figura 4. Histograma de imagen con doble compresión.

En el histograma anterior se puede ver como se pierde la correlación en algunos segmentos de la imagen, lo cual es señal de una variación del esquema original de la imagen.

Una variante de este tipo de alteración de fotografías digitales, es la de hacer montajes uniendo piezas de distintas imágenes, lo que implica unir fragmentos con distintas tasas de compresión. Por lo tanto, las partes ensambladas en la nueva imagen tendrán características de doble compresión distintas en comparación con otros segmentos de la misma imagen. En 2006 J. He *et al.* [5] desarrollaron un algoritmo para la detección automática de segmentos alterados. En este método, el histograma de coeficientes de cada canal DCT es analizado buscando efectos de doble compresión y asigna a cada bloque DCT de 8x8 elementos una probabilidad de haber sido manipulado. Las probabilidades de cada bloque son puestas juntas para obtener un mapa normalizado de bloques, y la decisión de si la imagen ha sido o no alterada se toma en base a la presencia y

ubicación de agrupamientos en el mapa. Experimentos realizados en un pequeño número de imágenes alteradas han demostrado el éxito de este algoritmo. Aunque aún se requieren experimentos para determinar los resultados de este método al trabajar con distintos tipos de alteración de imágenes.

En 2005, Popescu et al. [6] proponen un método para detectar redimensionamiento de partes de una imagen, lo que es una indicación potencial de alteración. El principio de este método se basa en el hecho de que el proceso de remuestreo o interpolación, introduce correlaciones periódicas específicas entre los coeficientes. Por lo tanto, la presencia de correlaciones entre pixeles puede ser usada para determinar que partes de la imagen fueron redimensionadas. Para extraer la forma específica de correlación, el autor toma modelos probabilísticos para la predicción de errores de coeficientes interpolados y no interpolados. La estimación de distribución de parámetros y agrupación de coeficientes son ejecutados simultáneamente por el algoritmo EM (Estimación-Maximización). Los resultados obtenidos en imágenes JPEG de alta calidad sometidas a distintos procesos como cambio de tamaño, rotación y corrección gamma tienen una precisión de casi 100%. Sin embargo, la precisión para detectar regiones de la imagen que han sido manipuladas todavía tiene que ser probada.

Otra forma común de alteración de imágenes es la repetición de contenido mediante copiar y pegar partes de una imagen en otra de sus áreas para esconder detalles en dicha imagen. Aunque este tipo de manipulación puede ser fácilmente detectado mediante una búsqueda exhaustiva de propiedades de correlación en la imagen, estos métodos no son prácticos considerando el costo computacional y no tienen buen desempeño cuando las partes copiadas son pequeñas. Sobre este problema, en [7] Fridrich et al. propone un mejor método, más rápido y preciso. Este método obtiene los coeficientes DCT desde una ventana que se desplaza a través de toda la imagen. Los coeficientes resultantes son ordenados e insertados en una matriz. Los renglones de coeficientes DCT son dispuestos en orden lexicográfico y a través de la comparación de renglones se determina cuales son similares. Una alternativa a este método es mostrada en [8] donde Popescu et al. usa una representación en bloques, usándolo como elemento de análisis para identificar bloques similares en la imagen. En esta técnica, después de dividir la imagen en bloques pequeños de tamaño fijo se extraen las componentes principales para lograr una reducción de la dimensionalidad de los datos con los cuales trabajar, los coeficientes de

cada bloque son vectorizados e insertados en una matriz, obteniendo después su correspondiente matriz de covariación y finalmente se ordenan lexicográficamente identificando así las regiones duplicadas. La robustez de este método en detectar partes alteradas se ha demostrado en imágenes JPEG con distintas tasas de compresión y diferentes niveles de ruido aditivo.

Inconsistencias en el proceso de adquisición de imágenes

El trabajo en este campo se centra en identificar características distintivas de las cámaras digitales, basándose en las diferencias de técnicas de procesamiento de imágenes que emplean y sus componentes tecnológicos, como pueden ser, las distorsiones ópticas de las lentes, el tamaño del sensor de imagen, el CFA (Color Filter Array) y sus algoritmos de procesamiento de color. Considerando que estas características deben ser uniformes a través de toda la imagen, las inconsistencias pueden ser tomadas como base para detectar alteraciones. Sobre este campo, en 2006, Swaminathan *et al.* [9] emplea las inconsistencias en la interpolación del array de filtros de color para detectar partes modificadas en una imagen, basándose en la obtención de un patrón CFA de una cámara y haciendo la comparación de este con el que presenta la imagen. Los resultados obtenidos con imágenes de prueba sometidas a rotaciones, compresión y redimensionamiento reportan una precisión de detección de casi 90%.

En otro enfoque, Lukas et al. en [10] propone un análisis de inconsistencias en el patrón de ruido del sensor extraído de la imagen para detectar y localizar alteraciones. El patrón de ruido obtenido desde diferentes regiones de la imagen es correlacionado con la correspondiente región del patrón de referencia de la cámara y la decisión está basada en la comparación de las correlaciones resultantes de la región de interés con la de otras regiones. En la misma línea, Popescu et al. en [11] propone detectar la presencia de interpolación CFA en bloques sobrepuertos de una imagen para detectar alteraciones. Los experimentos fueron efectuados con imágenes de un número limitado de cámaras digitales para identificar rastros de interpolación de CFA en cada bloque.

Finalmente en 2006, M. K. Johnson et al. [12] proponen un nuevo enfoque al analizar inconsistencias en la aberración cromática lateral como un signo de modificación. La aberración lateral se genera debido a la las lentes no pueden enfocar perfectamente la luz de cualquier longitud de onda en

el sensor de imagen, causando una pérdida de alineación entre los canales de colores que empeora con la distancia desde el centro óptico. Este método trata la desviación entre los canales de colores como una expansión o contracción de un canal de color con respecto a otro, e intenta estimar parámetros de referencia (foco y constante de aberración) para lograr alinearlos. La entropía mutua es usada para encontrar la constante de aberración exacta que da la mayor entropía mutua entre canales de color. Para detectar modificaciones, la imagen es dividida en bloques y la aberración estimada en cada bloque es comparada con un estimador global. Cualquier bloque que se desvíe significativamente del estimador de referencia se considera alterado. El umbral de desviación está determinado experimentalmente bajo distintas tasas de compresión; sin embargo, se requieren más experimentos para generalizar los resultados y determinar si existe dependencia con el contenido de la imagen.

Conclusiones y trabajo futuro

El área de análisis forense de imágenes digitales afronta diferentes desafíos que implican mucho trabajo todavía, pues, aunque muchas de estas técnicas propuestas son prometedoras e innovadoras, tienen limitaciones pues ninguna de ellas por sí sola ofrece una solución completa. En última instancia, estas técnicas tienen que ser usadas juntas para obtener resultados útiles con cierta probabilidad de confiabilidad. Se requiere todavía de más experimentos con distintos tipos de imágenes con configuraciones o características de un rango más amplio para determinar la robustez de las técnicas mencionadas; además de buscar posibles modificaciones a los algoritmos utilizados para mejorar su desempeño.

Referencias

- [1] Cox, I., Miller, M.L., and Bloom, J.A.: *Digital Watermarking*, Morgan Kaufmann, San Francisco, 2001
- [2] Arnold, M., Wolthusen, S.D., Schmucker, M.; *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House Publishers, 2003
- [3] J. Lukas and J. Fridrich, *Estimation of Primary Quantization Matrix in Double Compressed JPEG Images*, Proc. of DFRWS, 2003.
- [4] A. C. Popescu and H. Farid, *Statistical Tools for Digital Forensics*, Proc. of IHW, 2006.
- [5] J. He, Z. Lin, L. Wang and X. Tang, *Detecting Doctored JPEG Images via DCT Coefficient Analysis*, Proc. of ECCV, 2006.
- [6] A. C. Popescu and H. Farid, *Exposing Digital Forgeries by Detecting Traces of Re-Sampling*, IEEE Trans. Signal Processing, vol. 53, no. 2. pp. 758-767, 2005.
- [7] J. Fridrich, D. Soukal and J. Lukas, *Detection of Copy-Move Forgery in Digital Images*, Proc. of DFRWS, 2003.
- [8] A. C. Popescu and H. Farid, *Exposing Digital Forgeries by Detecting Duplicated Image Regions*, Technical Report, TR2004-515, Dartmouth College, Computer Science.
- [9] A. Swaminathan, M. Wu and K. J. R. Liu, *Image Tampering Identification Using Blind Deconvolution*, Proc. of IEEE ICIP, 2006.
- [10] J. Lukas, J. Fridrich and M. Goljan, *Detecting Digital Image Forgeries Using Sensor Pattern Noise*, Proc. of SPIE, 2006.
- [11] A. C. Popescu and H. Farid, *Exposing Digital Forgeries in Color Filter Array Interpolated Images*, IEEE Trans. Signal Processing, vol. 53, no. 10, pp. 3948-3959, 2005.
- [12] M. K. Johnson and H. Farid, *Exposing Digital Forgeries through Chromatic Aberration*, Proc. of ACM Multimedia Security Workshop, 2006.
- [13] Lukas J., Fridrich J., and Goljan M.: “Determining Digital Image Origin Using Sensor Imperfections”, Proc. SPIE Electronic Imaging, Image and Video Communication and Processing, San Jose, California, pp. 249–260, January 16–20, 2005
- [14] Johnson M.K. and Farid H.: “Exposing Digital Forgeries by Detecting Inconsistencies in Lighting”, Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.
- [15] Ng T.-T. and Chang S.-H.: “Blind Detection of Digital Photomontages using Higher Order Statistics”, ADVENT Technical Report #201-2004-1, Columbia University, June 2004.
- [16] Popescu A.C. and Farid H.: “Exposing Digital Forgeries by Detecting Traces of Resampling”, IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.
- [17] C. Carson, S. Belongie, H. Greenspan, and J. Malik, “*Blobworld: Image Segmentation Using Expectation-Maximization and its Application to*

Image Querying" IEEE Trans. Pattern Anal. Machine Intell., vol. 24, no. 8, pp. 1026-1038, 2002.

Curriculum Vitae

Juan Baltazar Padilla



Ingeniero en Sistemas Computacionales egresado de la Universidad de la Sierra A.C. en 2003. Actualmente está adscrito a la Sección de Estudios de Posgrado e Investigación de la Escuela Superior de Ingeniería Mecánica y Eléctrica unidad Culhuacan del Instituto Politécnico Nacional donde es candidato a Maestro en Ciencias de Ingeniería en Microelectrónica. Áreas de interés: seguridad informática, informática forense y forensia digital.

Rubén Vázquez Medina



Ingeniero en Electrónica con especialidad en Comunicaciones por la Universidad Autónoma Metropolitana unidad Iztapalapa (1989), obtuvo el grado de Maestro en Ciencias con especialidad en Telecomunicaciones en el Centro de Investigación y Estudios Avanzados del IPN (1994), y cuenta con los créditos por materias del Doctorado en Ciencias en la Universidad Autónoma Metropolitana unidad Iztapalapa. Desde 1997 es profesor investigador titular en la Sección de Estudios de Posgrado e Investigación de la Escuela Superior de Ingeniería Mecánica y Eléctrica unidad Culhuacan del IPN. Es profesor de la Maestría en Ciencias de Ingeniería en Microelectrónica y la Especialización en Seguridad Informática y Tecnologías de la Información en la ESIME Culhuacan. También es profesor invitado en la Maestría en Seguridad de la Información en la

Secretaría de Marina Armada de México. Cuenta con 19 Artículos Publicados en Revistas Internacionales, 10 Artículos Publicados en Revistas Nacionales, 9 Proyectos Institucionales de Investigación, 56 Artículos en Congresos Internacionales y 33 Artículos en Congresos Nacionales. Además, ha formado a 19 Maestros en Ciencias, dos de los cuales son de la Maestría en Seguridad de la Información de la SEMAR y 17 en el Instituto Politécnico Nacional. Sus áreas de interés son la seguridad informática, criptografía, esteganografía, la informática forense y la forensia digital.

Marcos Arturo Rosales García



Ingeniero en Computación por la Universidad Nacional Autónoma de México (2004), candidato a Maestro en Ciencias por la Sección de Estudios de Posgrado e Investigación de la Escuela Superior de Ingeniería Mecánica Eléctrica unidad Culhuacan del Instituto Politécnico Nacional, profesor de la carrera de ingeniería en computación desde Enero del 2007. Sus áreas de interés son la seguridad en los sistemas de información, auditoria en sistemas, y análisis forense en imágenes digitales y sistemas informáticos.

SEP



SECRETARÍA DE
EDUCACIÓN PÚBLICA



juntos
lo podemos
todo

LA UNIVERSIDAD POLITÉCNICA DE PACHUCA

OTORGА EL PRESENTE

Reconocimiento

AL : Ing. Marcos Arturo Rosales García

Por su destacada participación con la conferencia

Informática Forense en Imágenes

e invaluable contribución a la formación integral de nuestra
comunidad universitaria, en el *Encuentro de Tecnologías 2008*.

Zempoala, Hgo., abril 24 de 2008

Dr. Gustavo Núñez Esquer
Rector

