**TIPOS DE FALSIFICACIÓN:**

**- Retocamiento:**

Técnica comúnmente usada el la industria de los medios de comunicación. Está aceptada y es un método de manipulación de imágenes muy atractivo.

Técnica popularmente usada en revistas de fotos y películas. La imagen es alterada para hacerla más atractiva, y en ocasiones algunas regiones de dicha imagen son transformada para obtener el resultado final. No está considerada una técnica de falsificación, pero está incluida porque incluye manipulación de la imagen original.

**- Copy-move:**

En la falsificación copy-move una parte de la imagen es copiada y pegada en otra parte de esa misma foto para conseguir un objetivo o duplicar ciertos elementos de la imagen.

El método consiste en convertir la imagen a escala de grises y se divide en bloques. El HOGM (Histogram Of Orientated Gabor Magnitude) se aplica a cada bloque para la extracción de características locales y reducir las dimensiones para facilitar la comparación de las medidas. Finalmente esas características son clasificadas y las partes falsificadas son detectadas.

**- Composición:**

La imagen compuesta se divide en varios componentes. Después la diferencia de ruido que permanece después de “de-noising” en cada componente se calcula y se usa como característica. Finalmente, la regiones falsificadas se detectan usando esta característica basándose en la regla de detección de falsificación.

**FORMATO JPG**

Inicialmente hay que señalar que todos los archivos JPEG comienzan con el valor binario „0xFFD8‟ SOI (Start Of Image) y terminan con el valor binario „0xFFD9‟ EOI (End Of Image). SOI y EOI son dos marcadores especiales sin datos posteriores. En cambio, todas las marcas salvo las dos anteriores contienen una estructura fija y datos. El formato básico de una marca se muestra en la tabla 1.

El campo tamaño de los datos sigue la alineación de bytes denominada “Motorola” (big-endian), es decir, la lectura comienza por los bits de peso más altos a los más bajos. Por ejemplo, „0xAB21‟ como tamaño de datos indica que son 43809 bytes. Es importante destacar que en el tamaño de los datos los dos bytes que indican el propio tamaño de los datos están incluidos. Por ejemplo, el marcador „0xFFC1000C‟ indica que la marca „0xFFC1‟ tiene „0x000C‟ bytes de datos, es decir, 12 bytes de datos. Pero en esos 12 bytes se incluyen los dos bytes que indican el tamaño de los datos. Por tanto, el campo datos tiene una longitud de 10 bytes. Los datos son los 10 bytes siguientes a „0x000C‟.

En el formato JPEG existe una marca especial para describir los datos del contenido de la imagen. Esta marca es „0xFFDA‟ y se denomina SOS (Start of Stream). Tras la marca SOS se encuentran los datos propiamente dichos de la imagen y se termina en la marca especial EOI (End Of Image). Un esquema general con la posibilidad de marcadores para metadatos (por ejemplo Exif) para una imagen JPEG se presenta en la tabla 2.

3.3. JPEG File Interchange Fomat

JFIF (JPEG File Interchange Fomat) es un formato de archivos de imagen estándar, que contienen las imágenes guardadas en compresión JPEG [37]. Permite el intercambio de metadatos entre una gran variedad de plataformas y aplicaciones. Es un formato simple cuyo único objetivo es el intercambio de imágenes comprimidas JPEG. No incluye algunas de las características avanzadas de otros formatos de archivo de intercambio de imágenes.

Formalmente los estándares Exif y JFIF son incompatibles, ya que ambos especifican que sus segmentos de aplicación deben de ir los primeros en el archivo de imagen. En la práctica muchas aplicaciones producen archivos con ambos segmentos, pero esto puede crear problemas.

[37] C. Hamilton, C. Cube: Microsystems. JPEG File Interchange Format. Version 1.02, September 1, 1992. http://www.w3.org/Graphics/JPEG/jfif3.pdf.

------------------------------------------PAPER 6 ---------------------------------------------------

**Estándar JPEG**

Es un estándar muy popular para la codificación de imágenes digitales. Utiliza varias técnicas para garantizar tasas de compresión muy altas a expensas de una pequeña degradación de la calidad de la imagen. En pocas palabras, esta técnica supone que una imagen de entrada está codificada en el formato YCbCr, donde el canal Y contiene la componente de luminancia de la imagen, y los canales de crominancia Cb y Cr mantienen, respectivamente, el componente luminoso menos azul de la imagen y la componente de luminancia menos roja de la imagen.

Una vez en el dominio de la frecuencia, estos coeficientes se comprimen reduciendo drásticamente la cantidad de información proporcionada por las altas frecuencias y, a continuación, redondeando los valores resultantes.

El factor de calidad de una imagen JPEG puede variar en el rango [1, 100], donde valores más pequeños resultan en una calidad inferior de la imagen comprimida y un mayor grado de compresión.

**Integridad de imagen JPEG**

El campo de investigación de la integridad de la imagen digital se refiere al problema de evaluar si una imagen digital es el resultado de alguna operación de falsificación.

Detectar la falsificación de una imagen JPEG puede ser más difícil que para otros formatos porque los pasos de compresión empleados por esta codificación pueden borrar los trazos de falsificación dejados en una imagen alterada.

Las señales introducidas por la compresión JPEG pueden verse como una "marca de agua" inherente para las imágenes comprimidas. Estos artefactos resultan modificados cuando se modifica una imagen JPEG mediante operaciones de falsificación.

Estos algoritmos utilizan algunas de las propiedades estadísticas de los coeficientes DCT para detectar inconsistencias en los artefactos de bloqueo de una imagen JPEG objetivo.

“*Farid”* propuso una técnica, basada en la detección de *fantasmas* JPEG, para establecer si una región de una imagen fue originalmente comprimida con un factor de calidad diferente de otras regiones de la misma imagen. La desventaja de esta técnica es que sólo funciona cuando la región alterada tiene una calidad inferior a la imagen circundante.

**OTROS FORMATOS**

* TIFF
* PNG
* GIF
* RAW, BMP, PSP, PSD, ...

**TÉCNICAS QUE USAN JPG**

------------------------------PAPER 3----------------------------------------------------------------

La detección de imágenes compuestas no tiene referencia de regiones para poder comprobar las que están duplicadas. En general una imagen compuesta se crea cogiendo una porción de una imagen origen y pegándola en otra imagen después de haber realizado cambios en la geometría (como rotación, volteado, escalado…). La imagen compuesta contiene regiones falsificadas y originales. Las características inconsistentes se usan para detectar la falsificación como el ruido, compresión JPEG y sombras. La detección de imágenes compuestas es más complicada que la copy-move.

Mahdian y Saic propusieron un método de detección de imágenes compuestas basado en los niveles de ruido local inconsistentes. DWT primero se aplica a la imagen compuesta para obtener el HH “sub-band image”. Después el HH obtenido se divide en bloques de un tamaño fijo, no solapados. La desviación estándar del ruido de cada bloque se calcula usando el “median-based method”. Finalmente la región incorporada con el algoritmo se aplica a los bloques vecinos que sean similares dentro de un umbral para detectar las regiones falsificadas.

Fan , propuso una nueva herramienta de detección de manipulación, que relaciona las características del ruido con características seleccionadas de 3 intercambiables formatos de imagen (EXIF). Esa característica se formula como una suma media de las características del ruido. Este método solo es útil para formatos EXIF.

Zuo, propuso un método de detección de imágenes compuestas basado en trazas de muestreo y compresión JPEG. La imagen se divide en bloques solapados, después se define un factor de medida y se evalúa. El factor de medida contiene las características del muestreo y del formato JPEG de cada bloque. Finalmente el factor de medida se aplica para detectar las regiones falsificadas. A diferencia de otros métodos, cuando la calidad del factor de doble compresión es más pequeña que la primera, el método sigue funcionando correctamente. No obstante basándose en las sugerencias del autor, el método es inefectivo cuando la imagen compuesta está formada por dos imágenes no comprimidas y las regiones falsificadas no son propensas a cambios geométricos.

La compresión JPEG, o sombras, SPN (sensor pattern noise) es el resultado de de las imperfecciones de la imagen. SPN es la diferencia entre la imagen original y su versión sin ruido.