Digital Image Forensics

Los medios visuales digitales representan hoy en día uno de los principales medios de comunicación.

La imagen forense digital representa un campo de investigación atractivo para muchos investigadores.

Existen dos problemas: la identificación del dispositivo de imagen que capturó la imagen, y la detección de trazas de falsificaciones.

Las imágenes y videos representan una fuente común de evidencia, tanto en las cosas de la vida cotidiana como en los juicios.

La accesibilidad de los medios digitales visuales trae un inconveniente importante. Los expertos en procesamiento de imágenes pueden acceder y modificar fácilmente el contenido de la imagen y, por lo tanto, su significado, sin dejar huellas visualmente detectables. Además, con la difusión de herramientas de edición de bajo costo y de fácil uso, el arte de manipular y falsificar el contenido visual no está más restringido a los expertos. Como consecuencia, la modificación de imágenes con fines maliciosos es ahora más común que nunca. Digital Image Forensics es la rama de la seguridad multimedia que, junto con Digital Watermarking, pretende contrastar y exponer la manipulación de imágenes maliciosas.

Dos preguntas sobre la historia de la imagen en las que nos basamos:

A) ¿La imagen fue capturada por el dispositivo con el que se afirma que se adquirió?

B) ¿La imagen sigue representando su contenido original?

(DIF) tiene como objetivo proporcionar herramientas para apoyar la “blind investigation”.

Trata el procesamiento de imágenes y herramientas de análisis para recuperar información sobre la historia de una imagen. Dos caminos principales de investigación evolucionan bajo el nombre de Digital Image Forensics. El primero incluye métodos que intentan responder a la pregunta a), realizando algún tipo de análisis para identificar el dispositivo que capturó la imagen, o al menos para determinar qué dispositivos no lo capturaron.

El segundo grupo de métodos apunta en cambio a exponer rastros de manipulación semántica (es decir, falsificaciones) estudiando inconsistencias en las estadísticas de imágenes naturales.

Las disciplinas forenses en general apuntan a exponer pruebas de crímenes; Para hacerlo, tienen que lidiar con la capacidad de los ladrones para ocultarse o posiblemente para falsificar sus huellas.

En la imagen digital, tanto el proceso de adquisición como las técnicas de manipulación pueden dejar rastros sutiles. La tarea de los expertos forenses es exponer estas huellas explotando los conocimientos existentes sobre los mecanismos de imagen digital.

La marca de agua digital consiste en esconder una marca o un mensaje en una imagen para proteger sus derechos de autor.

Una marca de agua se puede ver como un ruido específico.

Una aplicación particular para la marca de agua es la protección de la integridad de la imagen. En este caso, se aplica una marca de agua frágil a la imagen de cubierta para que se destruya en un intento de manipulación. Esto asegura cierto control sobre la manipulación del contenido de la imagen.

La esteganografía consiste en comunicarse secretamente a través de algunos medios.

El objetivo del uso de esta tecnología es no ser detectado por un tercero. Para que el mensaje no sea detectable, los algoritmos mezclan información secreta en altas frecuencias con otros ruidos existentes.

Todas estas técnicas están trabajando en altas frecuencias para agregar, para recuperar, para detectar, o más generalmente para analizar "ruidos", o patrones característicos.

Digital Image Forensics tiene un papel muy preciso entre las disciplinas de seguridad multimedia: la autenticación de imágenes para las que no se conoce ninguna referencia y no se ha establecido ninguna protección de integridad anterior