**Forensic use of photo response non-uniformity of imaging sensors and a counter method**

1. INTRODUCCIÓN

Con los avances en tecnología, es posible editar y manipular multimedia con bajo coste, poco esfuerzo y experiencia. *“The availability of such technologies and their ease of use risk the credibility of digital information. “* Entonces, cuando la información digital es usada o presentada debe haber una serie de garantías sobre su origen, integridad y naturaleza del contenido digital.

La autenticidad de una imagen puede ser verificada usando el ruido característico del escáner del sensor, defectos físicos, distorsiones en la ruta óptica y sus efectos en el escaneo del resultado. PRNU es temporalmente constante y lateralmente no uniforme. Por lo tanto, puede considerarse una huella digital intrínseca del escáner de un sensor y puede usarse para trazar una imagen I a su fuente X cuando su autenticidad es cuestionada. Estudios en literatura muestran que PRNU-based camera identification es bastante robusto para imágenes manipuladas tanto como compresión JPEG, recortados, impresos y reducción de tamaño.

Hay varios métodos forenses para detectar la transferencia de ruido, tienen limitaciones y funcionan bajo ciertas circunstancias. Además PRNU-based camera identification tiene un potencial para ser usado bajo adversidades para el rastreo de identidades ilegales de imágenes compartidas en diferentes redes sociales violando los derechos de privacidad.

2. PRNU BASED SOURCE CAMERA IDENTIFICATION

De acuerdo a la naturaleza del PRNU, cada pixel en el escáner del sensor produce una reacción diferente al mismo nivel de intensidad de luz. Esta imperfección causa un patrón de ruido temporal aleatorio que puede ser considerado una huella digital intrínseca de una cámara digital.

3. THEORETICAL MODEL

Para un satisfactorio PRNU-based image anonimización, el término PRNU en el modelo de impresión debe ser 0.

4. ANONIMIZACIÓN DE LA FUENTE DE LA IMAGEN

El principal objetivo de la anonimización de la fuente de la imagen es eliminar el término PRNU. Este objetivo puede ser realizado extrayendo el ruido del sensor estimado, el cual es multiplicado con un factor específico (gain) de la imagen.

6. DISCUSIÓN

Los resultados experimentales muestran que el método propuesto mejora “flat-fielding and denoising methods” de 9 cámaras incluyendo DSLR, Smart pone, y cámaras compactas.

El usuario puede aumentar la fortaleza de su privacidad usando un mayor número de imágenes durante la fase de la estimación de la huella digital. Sin embargo, queda demostrado en estudios posteriores que algunas imágenes no se pueden identificar satisfactoriamente si el adversario tiene un estimador de huella digital similar o parecido.

7. CONCLUSIÓN

Usando análisis teórico y experimental, queda demostrado que la fuente de anonimización de la imagen es viable para varios sensores de cámaras digitales. El método propuesto no requiere ningún acceso físico al artefacto. No obstante, una serie de imágenes tomadas de una cámara es suficiente para aportar una huella digital inicial para impedir la identificación de la cámara. Los resultados experimentales muestran que el método contador propuesto no sacrifica la calidad de la imagen mientras se degrada el ruido PRNU. Además, las investigaciones muestran que el anonimato de la cámara fuente se queda confidencial incluso si un adversario usa un método mejor de estimación de la huella digital para identificar la cámara fuente.