A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection

La detección fiable de falsificaciones de imágenes requiere una batería de herramientas complementarias que explotan diferentes propiedades de imagen. Las técnicas basadas en la falta de uniformidad del ruido de la foto (PRNU) están entre las herramientas más valiosas, ya que, no detectan el objeto insertado, sino la ausencia de la cámara PRNU, una especie de huella dactilar, Elude la mayoría de las otras estrategias de detección. En este documento, proponemos un nuevo enfoque para la detección de falsificaciones utilizando ruido de patrón de sensor.

Las técnicas de optimización convexas modernas se adoptan para lograr una solución globalmente óptima y la estimación de PRNU se mejora mediante la eliminación no local del ruido.

Las imágenes digitales son cada vez más utilizadas para apoyar decisiones importantes.

Desafortunadamente, con la amplia disponibilidad de sofisticadas herramientas de manipulación de imágenes, la modificación de una fotografía digital, con pocos o ningún signo evidente de manipulación, se ha vuelto más fácil que nunca.

Es importante crear herramientas que ayuden a decidir sobre la autenticidad de una imagen digital, de hecho está creciendo el campo de detección de falsificaciones de imágenes.

Se han propuesto varios enfoques para detectar alteraciones de la imagen en una variedad de escenarios.

Una primera categoría comprende técnicas activas, para la autenticación de imágenes, basadas en el uso de marcas de agua y firmas. En el primer caso, la marca de agua está incrustada en la imagen (posiblemente originando pequeñas distorsiones), mientras que en el segundo, la firma se une a la imagen como información lateral. Aunque estos métodos son muy eficaces, sólo pueden aplicarse cuando la fuente digital está protegida en el origen, lo cual es probablemente en una minoría de los casos de interés.

Algunas técnicas están específicamente diseñadas para copiar y mover falsificaciones, donde partes de la imagen se cortan y pegan en otra parte de la misma imagen para duplicar u ocultar objetos de interés. Las partes duplicadas se descubren mediante procesamiento basado en bloques o, de manera más eficiente, por medio de características invariantes adecuadas.

Además, como muchas imágenes se guardan en algún formato JPEG comprimido, varias técnicas de detección de falsificación se basan en las huellas dejadas por la compresión JPEG múltiple. De hecho, cuando una imagen JPEG se modifica y se guarda de nuevo en formato JPEG, aparecen artefactos específicos como resultado de los múltiples procesos de cuantificación, lo que sugiere la presencia de algunas formas de manipulación.

La fase de adquisición, que a menudo deja huellas peculiares relacionadas con las características de la lente, la matriz de filtro de color (CFA), o el conjunto de sensores, que pueden ser usados para descubrir manipulaciones de la imagen. En este último contexto, la falta de uniformidad del ruido de la foto (PRNU) aparece como una de las herramientas más prometedoras.

Estas diferencias físicas proporcionan un patrón de sensor único, específico de cada cámara individual, constante en el tiempo e independiente de la escena.

De hecho, las formas más comunes de falsificación de imágenes, como copia pega o empalme, eliminan el PRNU original de la cámara, un hecho que puede detectarse a través de análisis adecuados, siempre que el PRNU de la cámara esté disponible.

El patrón PRNU es bastante robusto a varias formas comunes de procesamiento de imágenes, tales como compresión JPEG, filtrado o corrección gamma.

Desde que el PRNU es una señal muy débil, su estimación es crucial para el éxito del algoritmo. Típicamente, la estimación se calcula con una versión filtrada de la imagen observada, obteniendo un residuo donde el PRNU está presente, pero la imagen (vista como ruido en este contexto) se elimina en su mayor parte.

Los artefactos no únicos pueden conducir a resultados erróneos, especialmente en la identificación de la cámara, debido a la similitud entre las huellas digitales PRNU de diferentes dispositivos con características similares.

En este documento se propone un nuevo algoritmo de detección de falsificaciones basado en PRNU pero mejora algunos resultados preliminares se informan en [39].

Respeta: 1) en primer lugar, abandonamos la constante estrategia de falsas alarmas para adoptar una regla bayesiana más flexible; 2) lo más importante, las decisiones se toman ahora conjuntamente en la imagen completa y no individualmente para cada píxel; 3) destacar la solución global recurriendo a herramientas de optimización convexa, que garantizan la convergencia a un óptimo en un tiempo limitado; 4) las fuertes dependencias espaciales de la fuente se tienen en cuenta al modelar los datos; 5) finalmente, se mejora la calidad de los datos básicos mediante el uso de un algoritmo de *“denoising“* no local. Los experimentos demuestran que el algoritmo propuesto supera al de referencia, con un aumento muy limitado de la carga computacional.