Estado del arte

En el documento [1] se hace referencia a un algoritmo que emplea los coeficientes DCT para detectar falsificaciones del tipo copia pega en una imagen digital, cuando se ha copiado un bloque o región de una imagen y ha sido pegada en la misma imagen.

El algoritmo consiste en lo siguiente:

1. La imagen de entrada debe ser una escala de grises, por tanto, si es una imagen a color se pasará a escala de grises utilizando la fórmula estándar: I = 0,299R + 0,587G + 0,114B.
2. Se deslizará una ventana cuadrada de tamaño fijo b x b por cada pixel desde la esquina superior izquierda hasta la esquina inferior derecha para dividir la imagen en (m – b + 1) (n – b + 1) bloques superpuestos.
3. Aplicar DCT a cada bloque y remodelar la matriz cuantificada, ordenando los coeficientes DCT en zigzag. Para reducir el tamaño del vector y retener solo coeficientes de baja frecuencia, el vector es truncado a p x b2 elementos para mantener solo coeficientes de baja frecuencia. El parámetro p decide el número de coeficientes conservados.
4. Todos los vectores se clasifican lexicográficamente y forman una matriz de (mb + 1) (n – b + 1) x pb2.
5. Para cada fila ai se prueban sus filas vecinas aj para ver si satisfacen la condición que los primeros ‘q’ coeficientes DCT cuantificados son los mismos, ya que éstos son suficientes para representar la distribución de intensidad sobre el bloque.
6. Si ai y aj son similares, la distancia entre ellos debe ser más que el tamaño del bloque, es decir, que b.
7. Si la distancia es mayor, entonces se calcula el vector de desplazamiento y se aumenta el recuento de ‘s’, dónde s = (s1, s2) = (i1-j1, i2-j2), dónde las coordenadas de los bloques son (i1, j1) y (i2, j2).
8. El mayor recuento de 's' se toma como umbral de frecuencia. Además, debe ser más que b x b para representar una duplicación significativa.
9. Para todos los bloques que tienen un valor de cambio mayor que el valor del umbral, marca las regiones de la imagen con el color rojo para representar regiones movidas por copia.

En el articulo “Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes “se emplea un algoritmo que detecta falsificaciones de imágenes en las que se muestra un fondo que ha sido manipulado, ya que no es el original de la imagen.

La identificación de las imágenes manipuladas se obtiene utilizando una serie de reglas, a través de los umbrales para comprobar principalmente el primer plano y el fondo, respectivamente.

En el artículo, “RAKE TRANSFORM AND EDGE STATISTICS FOR IMAGE FORGERY

DETECTION”, anteriormente probado y con una efectividad del 99,14%, se proponen características estadísticas efectivas basadas en un modelo de imagen natural a través de un análisis de los cambios en la distribución de la frecuencia y características de los bordes de las imágenes. Al existir regiones que no son naturales, se presentan irregularidades en sus fronteras. Estas irregularidades pueden verse como los cambios no naturales de los valores de los píxeles, que corresponde a la adición de ruido.

Este algoritmo se emplea para detectar imágenes falsificadas a través de empalmes con otras imágenes.

En el artículo “An efficient forgery detection algorithm for object removal by exemplar-based image inpainting” presentaron un algoritmo de detección de falsificaciones eficaz para la eliminación de objetos mediante pinturas basadas en ejemplares. Este método puede reducir el tiempo de procesamiento manteniendo la precisión de detección.

Zuo, propuso en el artículo "Tampering Detection for Composite Images Based on Re-sampling and JPEG Compression" 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.

El algoritmo del articulo "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis" detecta imágenes manipuladas examinando el doble factor de cuantificación (DQ) contenido en los coeficientes DCT. Este efecto ocurre cuando el histograma de coeficientes de DCT de una imagen tiene valores perdidos periódicamente o algún patrón periódico de picos y valles. De acuerdo con Lin et al., Este efecto puede usarse para la autenticación de imágenes. Con este fin, muestran que las regiones de imagen (es decir, 8 x 8 bloques) que no exhiben el efecto DQ son probablemente alteradas. Es decir, en una imagen alterada, los bloques no modificados exhibirán el efecto de DQ, mientras que los bloques manipulados (también llamados bloques modificados) no lo harán.

El análisis de la CFA ha sido útil en la detección de la presencia de alteración mediante la utilización del algoritmo de la expectativa maximización "Exposing Digital Forgeries in Color Filter Array Interpolated Images".Esta técnica presentada en este trabajo produjo 0% de falsos positivos, con cerca del 100% de precisión para los algoritmos de interpolación probados tanto en imágenes no manipuladas como en imágenes con corrección gamma puntual no lineal. Sin embargo, la precisión disminuye ligeramente cuando una imagen se procesa con ruido gaussiano, y disminuye considerablemente en presencia de una creciente compresión JPEG. Además, hubo vulnerabilidad en el algoritmo cuando se probó contra el esquema de compresión JPEG2000. Explican que la cuantificación de los coeficientes wavelet introduce artefactos que son indistinguibles de los artefactos causados ​​por la interpolación CFA.

[1] V. Sharma, S. Jha, y R. K. Bharti, «Image Forgery and it’s Detection Technique: A Review», 2016.