Identificación de la Fuente de Imágenes de Dispositivos Móviles Basada en el Ruido del Sensor

Jocelin Rosales Corripio, David Manuel Arenas González, Ana Lucila Sandoval Orozco, Luis Javier García Villalba

Grupo de Análisis, Seguridad y Sistemas (GASS), Departamento de Ingeniería del Software e Inteligencia Artificial
Facultad de Informática, Despacho 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid
Email: jocerosa@ucm.es, {darenas, asandoval, javiergv}@fdi.ucm.es

***Resumen*—La fuente de una imagen digital se puede identificar a través de los rasgos que el dispositivo que la genera impregna en ella durante el proceso de su generación. La mayoría de las investigaciones realizadas en los últimos años sobre técnicas de identificación de fuente se han enfocado únicamente en la identificación de cámaras tradicionales DSC (*Digital Still Camera*). Considerando que hoy en día las cámaras de los dispositivos móviles prácticamente han sustituido a las DSCs se detectó la necesidad de realizar investigación sobre las técnicas para identificar la fuente de imágenes generadas por dispositivos móviles. Las imágenes digitales generadas por una cámara digital contienen intrínsecamente un patrón del ruido del sensor que se puede usar como medio de identificación de la fuente. Específicamente, las cámaras digitales de dispositivos móviles cuentan en su mayoría con un tipo de sensor que deja rasgos característicos en la imagen. En este trabajo se propone un algoritmo basado en el ruido del sensor y en la transformada wavelet para identificar el dispositivo móvil (marca y modelo) que ha generado determinadas imágenes bajo investigación.**

***Palabras clave*—Análisis forense, imagen digital, patrón de ruido del sensor, PRNU. *(Forensics analysis, digital image, sensor pattern noise, PRNU)*.**

I. Introduction

Con frecuencia las fotografías son consideradas como una parte de la verdad al ser hechos reales capturados por dispositivos electrónicos (cámaras). Sin embargo, con el desarrollo de la tecnología han surgido herramientas potentes y sofisticadas que facilitan de una manera impresionante la alteración de las imágenes digitales, incluso para quienes no tienen conocimientos técnicos o especializados en el área [1].

El desarrollo de las tecnologías digitales ha estado y continúa avanzando a un ritmo imparable. Cada día el número de cámaras digitales va creciendo, así como la facilidad de acceso a ellas. Las cámaras digitales de móviles merecen especial atención, ya que estudios realizados indican que al final del año 2012 el número total de dispositivos móviles activos alcanzó los 6,7 billones y se estima que para el verano del 2013 este número igualará al total de la población del planeta 7,1 billones. El 83 % de estos dispositivos móviles cuentan con cámara digital integrada, las cuales a diferencia de las cámaras digitales convencionales son llevadas por sus dueños todo el tiempo a la mayoría de lugares que asiste y en muchos casos tienen conexión a internet [2].

Debido al incremento en sus capacidades de almacenamiento, procesamiento, usabilidad y portabilidad así como a su bajo coste, los dispositivos móviles están presentes en diversidad de actividades, lugares y eventos de la vida diaria. A causa del extenso uso de las cámaras digitales de dispositivos móviles se han generado polémicas, discusiones y normas sobre la prohibición de su uso en lugares como escuelas, oficinas de gobierno, eventos empresariales, conciertos, empresas, etc. Una consecuencia más de su extenso uso es que las imágenes digitales en la actualidad son utilizadas como testigos silenciosos en procesos judiciales, siendo una pieza crucial de la evidencia del crimen [3]. Es por ello que contar con herramientas que permitan identificar a los dispositivos que han generado una cierta imagen digital cobra importancia ya que podría servir en diversas áreas como la lucha contra la pornografía infantil, la prevención de robo de tarjetas de crédito, el combate a la piratería, la prevención de secuestros, etc.

II. Técnicas de Análisis Forense en Imagenes

La investigación en este campo estudia el diseño de técnicas para identificar las características, especialmente marca y modelo, de los dispositivos utilizados para la generación de imágenes digitales. El éxito de estas técnicas depende del supuesto de que todas las imágenes adquiridas por un mismo dispositivo presentan características intrínsecas del dispositivo. Las características que se usan para identificar marca y modelo de las cámaras digitales se derivan de las diferencias que existen entre las técnicas de procesamiento de las imágenes y las tecnologías de los componentes que se utilizan [4]. El mayor problema con este enfoque es que los diferentes modelos de las cámaras digitales usan componentes de un número reducido de fabricantes, y que los algoritmos que usan también son muy similares entre modelos de la misma marca. Es por ello que la fiabilidad de la identificación de la cámara fuente depende en gran parte de la identificación de varias características independientes del modelo. Según [4] se pueden establecer cuatro grupos de técnicas para este fin: utilización de la aberración de las lentes, interpolación de la matriz CFA, uso de las características de la imagen e imperfecciones del sensor. Esta última constituye el objeto de

ISBN: 978-84-9717-323-0

este trabajo. Además de las anteriores existe otro grupo de técnicas basadas en los metadatos.

Las técnicas basadas en el estudio de las huellas que los defectos del sensor dejan sobre las imágenes se dividen en dos ramas: defectos de píxel y patrón de ruido del sensor SPN (Sensor Pattern Noise). En la primera se estudian los defectos de píxel, los píxeles calientes, los píxeles muertos, los defectos de fila o columna, y los defectos de grupo. En la segunda se construye un patrón del ruido promediando los múltiples residuos de ruido obtenidos mediante algún filtro de eliminación de ruido. La presencia del patrón se determina utilizando algún método de clasificación como correlación o máquinas SVM.

En [5] se estudian los defectos de los píxeles en los sensores de tipo CCD, centrándose en la evaluación de diferentes características para examinar las imágenes e identificar la fuente: defectos del sensor CCD, formato de los archivos usados, ruido introducido en la imagen y marcas de agua introducidas por el fabricante de la cámara. Entre los defectos del sensor CCD considerados se encuentran los puntos calientes, los píxeles muertos, los defectos en grupo y los defectos de fila o columna. En sus resultados se observa que cada una de las cámaras tiene un patrón de defecto diferente. Sin embargo, también se señala que el número de defectos en los píxeles para una cámara es diferente entre fotos y varía demasiado en función del contenido de la imagen. Asimismo, se revela que el número de defectos cambia con la temperatura. Al considerar únicamente los defectos de los sensores de tipo CCD este estudio no es aplicable al análisis de imágenes generadas por dispositivos móviles.

En [6] se analiza el patrón de ruido del sensor de un conjunto de cámaras, el cual funciona como una huella dactilar, permitiendo la identificación única de cada cámara. Para obtener este patrón se realiza un promedio del ruido obtenido a partir de diferentes imágenes utilizando un filtro de eliminación de ruido. Para identificar la cámara a partir de una imagen dada, se considera el patrón de referencia como una marca de agua cuya presencia en la imagen es establecida mediante un detector de correlación. El estudio se realizó con 320 imágenes procedentes de 9 modelos distintos de cámaras. También se demuestra que este método está afectado por algoritmos de procesamiento de la imagen como la compresión JPEG y la corrección gamma. Los resultados para fotografías con diferentes tamaños y recortadas no son satisfactorios [4].

En [7] se propone un enfoque para la identificación de la cámara fuente considerando escenarios abiertos, donde a diferencia de los escenarios cerrados no se da por sentado contar con acceso a todas las posibles cámaras de origen de la imagen. Este enfoque, considera 9 diferentes áreas de interés ROI (*Region Of Interest*) que se encuentran en las esquinas y el centro de las imágenes. El uso de las regiones de interés permite trabajar con imágenes de diferentes resoluciones sin la necesidad de rellenar con ceros las imágenes y sin el uso de artefactos de interpolación de color. Para determinar las características se calcula el SPN para cada uno de los canales R, G y B. Asimismo, se calcula el SPN para el canal Y (luminancia), generándose un total de 36 características para representar cada imagen. Después, las imágenes tomadas por la cámara bajo investigación son etiquetadas como la clase positiva y las tomadas por las cámaras disponibles restantes como las clases negativas. Después de la fase de entrenamiento de la SVM en la que se calcula el hiper-plano que separa los casos positivos y negativos toman en cuenta las clases desconocidas del escenario abierto moviendo el hiper-plano generado por un valor dado ya sea hacia adentro (hacia las clases positivas) o hacia afuera (las clases negativas). En los experimentos utilizan un conjunto de 25 cámaras digitales de 9 fabricantes, 150 imágenes en formato JPEG de cada cámara con diferentes configuraciones de luz, zoom y flash. Los resultados de los experimentos mostraron una precisión del 94,49 %, del 96,77 % y del 98,10 %, utilizando conjuntos abiertos con 2/25, 5/25, y 15/25 cámaras, respectivamente, definiendo un conjunto abierto x/y como el conjunto de y cámaras donde x cámaras son usadas para entrenar y probar las imágenes que pueden pertenecer a cualquiera de las cámaras x conocidas, así como a las otras y-x cámaras desconocidas.

En [8] se basan en el trabajo de [6] para extraer el ruido del sensor usando el cálculo de similitudes como método de la clasificación. Exponen que el ruido del sensor puede estar muy contaminado por los detalles de los escenarios y proponen que entre más fuerte es un componente del ruido del sensor es menos fiable y por lo tanto debe ser atenuado. Proponen una forma de atenuar los valores altos del ruido del sensor y realizan experimentos de identificación con 6 cámaras tradicionales diferentes (100 imágenes de cada cámara). Para las imágenes de 1536x2048 pixeles obtuvieron una tasa de acierto del 38.5 % con la implementación sin la mejora y del 80.8 % con la mejora propuesta; para las imágenes de 512x512 píxeles obtuvieron una tasa de acierto del 21.8 % sin la mejora y del 78.7 % con la mejora propuesta.

III. Algoritmo de Identificación de la Fuente

Debido a la propiedad determinista del patrón de ruido del sensor que está presente en cada imagen capturada, se puede usar este patrón como huella para identificar el dispositivo que generó la imagen objeto en investigación. Haciendo una analogía, se puede decir que el patrón del ruido del sensor es para una cámara digital lo que la huella para un ser humano.

Para poder identificar la marca y el modelo de la cámara digital de un dispositivo móvil se requiere de un algoritmo que nos permita extraer el ruido del sensor y otro que nos permita obtener las características de las huellas obtenidas para así poder clasificarlas e identificarlas.

Tomando como referencia las ideas principales de [6] se propone un algoritmo para extraer el ruido del sensor (también conocido como ruido residual) que se describe en el algoritmo 1.

Con el promediado a cero se limpia la huella de las características que no son intrínsecas al sensor aplicando como se sugiere en [9], de tal manera que los promedios de las filas y de las columnas sean iguales a cero. Esto se logra restando el promedio de la columna a cada píxel de la columna y

Algoritmo 1: Extraer ruido del sensor

Input: Imagen
varianza: (adaptativa o no adaptativa)
Result: Huella del sensor de la imagen

1 **procedure** EXTRAERHUELLA(I)
2 Realizar descomposición wavelet de 4 niveles de I_n;
3 **foreach** *nivel de la descomposición wavelet* **do**
4 **foreach** $c \in \{H,V,D\}$ **do**
5 Calcular la varianza local;
6 **if** *varianza adaptativa* **then**
7 Calcular 4 varianzas con ventanas de tamaños 3, 5 ,7 y 9 respectivamente;
8 Seleccionar la varianzas mínima;
else
9 Calcular la varianza con una ventana de tamaño 3;
10 Calcular los componentes wavelet sin ruido aplicando el filtro de Wiener a la varianza;
11 Obtener la imagen limpia del ruido del sensor aplicando la Transformada Inversa Wavelet;
12 Calcular el ruido del sensor con $I_{ruido}=I_{entrada}-I_{limpia}$;
13 Aplicar a I_{ruido} un promediado a cero;
14 Aumentar en I_{ruido} el peso del canal verde con $I_{ruido}=0{,}3\cdot I_{ruido_R}+0{,}6\cdot I_{ruido_G}+0{,}1\cdot I_{ruido_B}$;
15 **end procedure**

Algoritmo 2: Extracción de Características

Input: Imagen
Huella del sensor de la imagen
Result: 81 características

1 **procedure** EXTRAERCARACTERISTICAS(I)
2 Separar los canales R, G y B de la huella del sensor;
3 **foreach** *canal de color* **do**
4 Hacer una descomposición wavelet de un nivel;
5 **foreach** $c \in \{H,V,D\}$ **do**
6 Calcular k momentos centrales con $m_k = \frac{1}{n}\sum_{i=1}^{n} |c_i - \overline{c}|^k$;
7 **end procedure**

posteriormente restando el promedio de la fila a cada píxel de la fila. Esta operación se aplica a todas las filas y columnas de la imagen. Después de limpiar la imagen se le da un mayor peso al canal verde ya que debido a la configuración de la matriz de color éste contiene más información sobre la imagen que el resto de los canales de color [10][11]. La identificación de las cámaras se realiza utilizando una máquina de soporte vectorial SVM para lo que es necesario extraer una serie de características que representen a las huellas de los sensores. Se calculan un total de 81 características (3 canales x 3 componentes wavelet x 9 momentos centrales) mediante el algoritmo 2.

Con las características que se extraen tanto de las imágenes para entrenamiento como para probar se alimenta la máquina SVM y se obtienen las clasificaciones.

IV. EXPERIMENTOS Y RESULTADOS

Para evaluar la efectividad del algoritmo de identificación de la fuente de dispositivos móviles se realizaron dos experimentos, en los que se consideraron los 1024x1024 píxeles centrales de las fotografías como se recomienda ampliamente en [12]. La Tabla I resume los principales parámetros utilizados.

En el primer experimento se probó con un grupo de 8 cámaras digitales de dispositivos móviles de 4 fabricantes. De Apple se consideraron los modelos iPhone3G (A1), iPhone4S (A2) y iPhone3 (A3); de BlackBerry el 8520 (B1); de Sony Ericsson el UST25a (SE1) y el U5I (SE2); y de Samsung el GTI9100 (S1) y el GTS5830 (S2). El algoritmo propuesto obtuvo un porcentaje de acierto promedio de 93.625 % al identificar entre marca y modelo como se observa en la matriz de confusión de la Tabla II.

Tabla I
PARÁMETROS UTILIZADOS EN LOS EXPERIMENTOS

Parámetro	Valor
Tipo de Fotos	Sin ninguna restricción
Dimensiones	1024 x1024
Fotos Entrenadas x Cámara	100
Fotos Probadas x Cámara	100
Cálculo de la Varianza	Enfoque no adaptativo

Tabla II
MATRIZ DE CONFUSIÓN DEL EXPERIMENTO 1

Cámara	A1	A2	A3	B1	SE1	SE2	S1	S2
A1	**92**	1	0	0	0	1	0	6
A2	0	**96**	0	0	1	0	3	0
A3	0	0	**99**	0	0	0	1	0
B1	0	0	0	**94**	0	2	0	4
SE1	7	2	0	0	**91**	0	0	0
SE2	2	0	0	1	0	**94**	1	2
S1	4	8	0	0	0	5	**83**	0
S2	0	0	0	0	0	0	0	**100**

Con la finalidad de acercarse a escenarios más reales el segundo experimento se realizó con 14 cámaras digitales de dispositivos móviles de 7 fabricantes. De Apple se consideraron los modelos iPhone3G (A1), iPhone4S (A2), iPhone3 (A3) y iPhone5 (A4); de BlackBerry el 8520 (B1); de Sony Ericsson el UST25a (SE1) y el U5I (SE2); de Samsung el GTI9100 (S1), el GTS5830 (S2) y el GT-S5830M (S3); de Lg el E400 (L1); de HTC el DesireHD (H1) y el Desire (H2); y de Nokia el E61I (N1). El algoritmo propuesto obtuvo un porcentaje de acierto promedio de 87,214 % como se puede observar en la matriz de confusión de la Tabla III.

Tabla III
MATRIZ DE CONFUSIÓN DEL EXPERIMENTO 2

Cámara	A1	A2	A3	A4	B1	SE1	SE1	S1	S1	S3	L1	H1	H2	N1
A1	**90**	0	0	2	0	0	0	0	7	0	1	0	0	0
A2	0	**91**	0	3	0	0	0	3	0	0	0	1	2	0
A3	0	0	**98**	0	0	0	0	2	0	0	0	0	0	0
A4	0	0	1	**88**	0	0	0	0	0	0	3	6	0	2
B1	0	0	0	2	**73**	0	0	0	4	0	0	1	0	20
SE1	7	0	0	0	0	**80**	0	0	0	0	1	12	0	0
SE2	1	0	0	2	2	0	**86**	1	2	5	1	0	0	0
S1	4	5	0	4	0	0	1	**83**	0	0	1	0	2	0
S2	0	0	0	0	0	0	0	0	**100**	0	0	0	0	0
S3	0	0	1	0	0	0	8	0	0	**85**	0	1	0	5
L1	0	0	0	9	0	6	0	0	2	0	**70**	13	0	0
H1	2	0	0	0	0	11	0	0	1	0	1	**85**	0	0
H2	0	6	0	0	0	0	0	0	0	0	0	0	**94**	0
N1	0	0	0	0	2	0	0	0	0	0	0	0	0	**98**

V. CONCLUSIONES

En este trabajo se estudian las diferentes técnicas de análisis forense de imágenes para solucionar el problema de la identificación de la fuente de una imagen. Se describe la idea principal de cada una de las técnicas así como algunos de los trabajos más representativos que se han realizado aplicándolas. De acuerdo a la estructura y funcionamiento de las cámaras digitales de dispositivos móviles las técnicas más adecuadas para realizar análisis forense en ellas son las que se basan en el ruido del sensor y las que utilizan las transformadas wavelet. En virtud de lo anterior se propuso un algoritmo para la identificación de los dispositivos móviles fuente combinando las técnicas basadas en la huella del sensor y en la transformación wavelet. Por último con los experimentos realizados y sus resultados se demuestra que la combinación de estas técnicas es efectiva para la identificación del modelo y fabricante con un alto porcentaje de acierto.

Aún estimando que son buenos los resultados obtenidos por la técnica, obviamente existe margen de mejora de las tasas de acierto, sobre todo teniendo en cuenta el caso en el que el número de cámaras aumenta considerablemente. Cuanto mayor sea la mejora en la tasa de acierto mayor será la posibilidad de aplicación de la técnica a situaciones reales. A grandes rasgos las principales líneas de investigación a tener en cuenta en los trabajos futuros son: mejora en la selección del recorte de la fotografía (distintas dimensiones y zonas), optimización de los parámetros de configuración de la máquina SVM, optimización en la selección de la función wavelet y la combinación de esta técnica con otras como las basadas en las caracterísitcas del color, las basadas en las métricas de calidad de la imagen o las que utilizan otros tipos de características extraídas del ruido del sensor.

REFERENCIAS

[1] T. Gloe, M. Kirchner, A. Winkler, and R. Bohme, "Can We Trust Digital Image Forensics?" in *Proceedings of the 15th International Conference on Multimedia*, September 2007, pp. 78–86.

[2] T. Ahonen and A. Moore, "Tomi Ahonen Almanac 2012: Mobile Telecoms Industry Annual Review," 2012. [Online]. Available: http://www.tomiahonen.com/ebook/almanac.html

[3] M. Al-Zarouni, "Mobile Handset Forensic Evidence: a Challenge for Law Enforcement," in *Proceedings of the 4th Australian Digital Forensics Conference*, December 2006.

[4] T. Van Lanh, K. S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A Survey on Digital Camera Image Forensic Methods," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, July 2007, pp. 16–19.

[5] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, "Methods for Identification of Images Acquired with Digital Cameras," in *Proceedings of the Enabling Technologies for Law Enforcement and Security Conference*, vol. 4232, February 2001, pp. 505–512.

[6] J. Lukas, J. Fridrich, and M. Goljan, "Digital Camera Identification from Sensor Pattern Noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[7] F. D. O. Costa, M. Eckmann, W. J. Scheirer, and A. Rocha, "Open Set Source Camera Attribution," in *Proceedings of the 25th Conference on Graphics, Patterns and Images*, August 2012, pp. 71–78.

[8] C. T. Li, "Source Camera Linking Using eEnhanced Sensor Pattern Noise Extracted from Images," in *Proceedings of the 3rd International Conference on Crime Detection and Prevention (ICDP 2009)*. Curran Associates, Inc., December 2009, pp. 1–6.

[9] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining Image Origin and Integrity Using Sensor Noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, March 2008.

[10] O. Celiktutan, B. Sankur, and I. Avcibas, "Blind Identification of Source Cell-Phone Model," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 553–566, September 2008.

[11] C. McKay, "Forensic Analysis of Digital Imaging Devices," University of Maryland," Technical Report, 2007.

[12] C. T. Li and R. Satta, "On the Location-Dependent Quality of the Sensor Pattern Noise and its Implication in Multimedia Forensics," in *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011)*. Curran Associates, Inc., November 2011, pp. 1–6.