

# Método para identificar el dispositivo de captura de una imagen digital no manipulada basado en la distancia de Hellinger

Identification method of the capture device of an unmanipulated digital image based on Hellinger distance

Ana Laura Quintanar Reséndiz<sup>1</sup>, Jerónimo de Jesús Hernández Sánchez<sup>2</sup>, Brenda Juárez Santiago<sup>2</sup>, Rene Santos Osorio<sup>2</sup>, Norma Alejandra Ledesma Uribe<sup>2</sup>, Rubén Vázquez Medina<sup>1\*</sup>

<sup>1\*</sup> Instituto Politécnico Nacional, Centro de Investigación en Ciencia Aplicada y Tecnología Avanzada, Unidad Querétaro. Cerro Blanco No. 141, Col. Colinas del Cimataro. Querétaro, México. C.P. 76090. Tel. 442 229 0804 Ext. 81049. [ruvazquez@ipn.mx](mailto:ruvazquez@ipn.mx)

<sup>2</sup> Mecatrónica y Tecnologías de la Información y Comunicación, Universidad Tecnológica de San Juan del Río.

\*Autor de correspondencia

## Resumen

Se propone un método basado en la distancia de Hellinger y la función de densidad de probabilidad de señales (*Photo Response Non-Uniformity* [PRNU]) para identificar el dispositivo de captura de imágenes digitales. El método asocia una imagen digital no modificada (imagen en disputa) con uno de un conjunto de dispositivos de captura candidatos, al comparar la huella digital insertada en la imagen en disputa contra la base de datos creada con las huellas digitales de los dispositivos de captura. El método propuesto se implementó en Matlab™ para demostrar su funcionamiento, luego se comparó en un caso de estudio controlado contra dos métodos diferentes: uno propuesto por Goljan *et al.* (2009) con un porcentaje de similitud promedio del 100% y el otro por Quintanar-Reséndiz *et al.* (2021) con el 99.35%, y para el método propuesto resultó ser de 97.68%.

**Palabras clave:** Funciones hash; códigos de autenticación; huellas de imágenes digitales; ruido intrínseco; distancia de Hellinger.

## Abstract

A method based on Hellinger distance and Photo Response Non-Uniformity (PRNU) signal probability density function is proposed to identify the digital image capture device. The method is applied to an unmanipulated digital image (disputed image) and allows to associate it with one of a set of candidates capture devices. This association is performed through the fingerprint imprinted by the capturing device on the disputed image, then this imprinted fingerprint is compared with the fingerprint of each capturing device. The proposed method was implemented in Matlab™ to show its performance and compared against two different methods. The first method, proposed by Goljan *et al.* (2009), reached a mean similarity percentage of 100%, and the second method, proposed by Quintanar-Reséndiz *et al.* (2021), reached 99.35%; and the method proposed here reached a mean similarity percentage of 97.68%.

**Keywords:** Hash functions; authentication codes; fingerprints in digital images; intrinsic noise; Hellinger distance.

Recibido: 10 de septiembre de 2021

Aceptado: 12 de diciembre de 2021

Publicado: 09 de marzo de 2022

**Cómo citar:** Quintanar Reséndiz, A.L., Hernández Sánchez, J.J., Juárez Santiago, B., Santos Osorio R., Ledesma Uribe, N.L. & Vázquez Medina, R. (2022). Método para identificar el dispositivo de captura de una imagen digital no manipulada basado en la distancia de Hellinger. *Acta Universitaria* 32, e3317. doi. <http://doi.org/10.15174/au.2022.3317>

## Introducción

En México, durante el año 2019, el 75.1% de la población con edad de seis años o más contaban con un teléfono celular inteligente, el cual incluía al menos una cámara digital integrada y tenía la capacidad de capturar y compartir archivos multimedia. De acuerdo con datos reportados en 2019 por el Instituto Nacional de Geografía y Estadística (INEGI), del total de usuarios de teléfonos celulares inteligentes, 45.5 millones instalaron aplicaciones; y de estos, el 89.5% instalaron mensajería instantánea, el 81.2% instalaron herramientas para acceso a redes sociales y el 71.9% instalaron aplicaciones de contenidos de audio y video con capacidad de compartir archivos multimedia (INEGI, 2019).

Un teléfono celular inteligente es un dispositivo personal que, a partir de las prestaciones que tiene disponibles, se considera el principal generador de imágenes digitales. En muchos casos, estas imágenes podrían usarse como material probatorio en un proceso legal, ya sea de carácter penal, civil, médico o administrativo. En ese sentido, podría requerirse relacionar a una imagen digital con su dispositivo de captura y, en consecuencia, establecer una relación de dicho dispositivo con una persona, típicamente el propietario. En México, bajo el marco legal actual, en el que es posible presentar imágenes digitales como material probatorio, la relación imagen-dispositivo y dispositivo-sujeto puede ser crucial; por ello, las acciones de análisis forense multimedia pueden adquirir relevancia. La identificación de los dispositivos de captura se hace comúnmente a través de los rasgos (metadatos y señal PRNU) que se encuentran en las imágenes analizadas. Aunque no son determinantes en un análisis forense, los metadatos constituyen información relevante que describe de manera general el contenido principal de un documento digital; en este caso, el documento es una imagen digital en formato JPEG. De no ser modificados maliciosamente o dañados sin intención, los metadatos resultan de gran ayuda en la documentación de un caso (Sandoval *et al.*, 2015).

Por otro lado, en acciones de análisis forense de imágenes digitales, la señal PRNU (*Photo Response Non-Uniformity*) es una de las más utilizadas. La señal PRNU es una de varias señales intrínsecas que un dispositivo de captura imprime en una imagen digital cuando la construye; por ello, es considerada un elemento útil en la identificación unívoca del dispositivo de captura de una imagen digital. De acuerdo con lo expresado en Fridrich (2009), son cinco las principales propiedades de la señal PRNU:

**Dimensionalidad.** Es de naturaleza aleatoria y de tamaño finito, con información de las características del sensor del dispositivo de captura.

**Universalidad.** Todos los sensores de imágenes la generan: Por lo tanto, se puede extraer de imágenes digitales generadas por cualquier dispositivo de captura.

**Generalidad.** Está presente en cada imagen digital independientemente del mecanismo óptico o configuración de la cámara, o del contenido de la escena, con la probable excepción de las imágenes que son completamente oscuras.

**Estabilidad.** Para un dispositivo de captura, y bajo condiciones de uso adecuado, esta señal no cambia en el tiempo y se mantiene para una amplia gama de condiciones ambientales (temperatura, humedad, etc.).

**Robustez.** Sobrevive a procesamientos típicos como la compresión con pérdidas, el filtrado, la corrección gamma entre otros.

La señal PRNU es una componente del ruido del patrón del sensor (*Sensor Pattern Noise* [SPN]), el cual está asociado a imperfecciones en las obleas de silicio con las que se fabrica el sensor del dispositivo de captura y causa la variación de la sensibilidad de los píxeles de la imagen. Por estas cinco propiedades, la señal PRNU puede usarse para definir la huella digital de los dispositivos de captura contenida en las imágenes digitales. Cabe destacar que la señal PRNU es el principal contribuyente del SPN.

Cuando se genera una imagen digital JPG, en ella se imprimen características intrínsecas del dispositivo de captura. Cuando estas características llegan a cumplir con las propiedades enunciadas anteriormente (Goljan *et al.*, 2009), permiten que una imagen pueda asociarse con un dispositivo de captura. La señal PRNU es un atributo bien conocido y muy utilizado. Este atributo extraído de las imágenes digitales fue usado por primera vez en Lukas *et al.* (2006); desde entonces, la comunidad científica ha propuesto diversos métodos que lo utilizan para identificar el dispositivo con el que se capturó una o más imágenes digitales (Lukas *et al.*, 2006). Así, en Goljan *et al.* (2009) se desarrolló un algoritmo para extraer la señal PRNU y con ella identificar dispositivos de captura. También en Li (2010) se propuso un método para identificar el dispositivo de captura de imágenes digitales considerando la señal PRNU y los rastros de la escena. Así mismo, en Cooper (2013) se realizó una selección de los píxeles con mayor intensidad de señal PRNU, para que de ellos se extrajera dicha señal para el proceso de discriminación de los dispositivos de captura. En Saito *et al.* (2017) se propuso un método que reduce los falsos positivos cuando se identifica el dispositivo de captura agrupando píxeles a través de un modelo de cálculo probabilístico. También, en Balamurugan *et al.* (2017) se presentó un método de identificación del dispositivo de captura basado en la extracción de la señal PRNU que consta de tres etapas: filtrado, estimación y mejora. Por otra parte, en Mehrish *et al.* (2018) la señal PRNU se estimó a partir de datos probabilísticos con el mismo propósito y se extrajo de videos de WhatsApp utilizando un filtro de segundo orden. De igual forma, en Long *et al.* (2019) se propuso un método para medir la similitud de señales PRNU para identificar un dispositivo de captura. También, en Zhao *et al.* (2019) fue presentado un clasificador que considera la textura de las imágenes digitales para identificar su dispositivo de captura, buscando distinguir entre dispositivos del mismo modelo. Por su parte, en Long *et al.* (2019) se utilizaron medidas de similitud de la señal PRNU para proponer un algoritmo que identifica el dispositivo de captura de imágenes generadas por computadora. En Seshadri *et al.* (2020) se identificó el dispositivo de captura con una red neuronal convolucional pre-entrenada que utiliza características residuales.

Uno de los métodos más populares y utilizados para la extracción de la señal PRNU es el módulo de extracción de ruido que se encuentra en el algoritmo de identificación de dispositivos de captura desarrollado en Goljan *et al.* (2009). Ese módulo de extracción de la señal PRNU consta de dos etapas de filtrado, una es del tipo *denoising*, que devuelve el ruido con todos sus componentes separándola de la imagen sin ruido, y la otra aplica un filtro Wiener para que del ruido de la primera etapa de filtrado se eliminen los componentes de ruido aditivo, quedando así solo la señal PRNU. Así, a partir del uso de las señales PRNU contenidas en las imágenes digitales, en este trabajo se propone un método estadístico que, basado en la distancia de Hellinger, identifica el dispositivo de captura de una imagen digital. En el método propuesto se hace una distinción entre dos objetos, la huella digital del dispositivo de captura y la huella digital insertada en la imagen en disputa, la cual tiene relación con la huella digital del dispositivo que la capturó. Para obtener ambas huellas digitales se extrae la señal PRNU de las imágenes digitales y se calcula su correspondiente función de densidad de probabilidad (*Probability Density Function* [PDF]). La huella digital de una imagen en disputa será la PDF de la señal PRNU que le sea extraída, y la huella digital del dispositivo de captura será el promedio de las PDF obtenidas para las señales PRNU de 29 imágenes de referencia, las cuales se capturaron con ese dispositivo. En este método se generan 30 huellas digitales por dispositivo de captura de la siguiente manera:

- Con cada dispositivo se capturan 30 imágenes de referencia unitono y se numeran del 1 al 30.
- Para calcular la primera huella digital no se incluye en el promedio de las PDF, la PDF de la señal PRNU de la primera imagen de referencia.
- Para calcular la segunda huella digital no se incluye en el promedio de las PDF la PDF de la señal PRNU de la segunda imagen de referencia.
- Y así sucesivamente hasta obtener las 30 huellas digitales por dispositivo de captura.

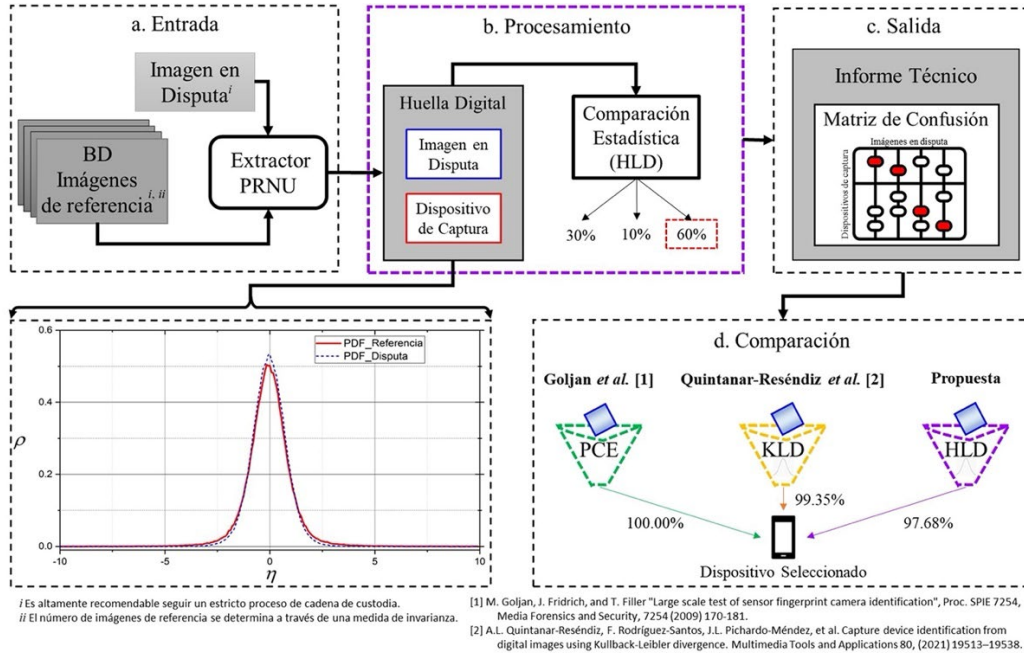
Posteriormente, para cada una de las 20 imágenes en disputa por dispositivo de captura se calcula la distancia de Hellinger entre su huella digital insertada y las 30 huellas digitales de cada uno de los ocho dispositivos de captura candidatos. Después, para cada una de las 20 imágenes en disputa se cuantifica el porcentaje del número de veces que se obtuvo el valor más pequeño de las distancias de Hellinger calculadas entre su huella digital insertada y las 30 huellas digitales de todos los dispositivos de captura. El valor más pequeño de dicha distancia indica el dispositivo que capturó una imagen en disputa. Finalmente, por dispositivo de captura y para todas las imágenes en disputa se calcula el promedio de los porcentajes mencionados anteriormente. Con esto, el dispositivo de captura de cada imagen en disputa se identifica a través del valor más grande de los promedios calculados anteriormente para cada dispositivo de captura.

Además, con fines de comparación se presenta un programa de software desarrollado en Matlab™, el cual integra tanto el método propuesto y los métodos propuestos en Goljan *et al.* (2009) y en Quintanar-Reséndiz *et al.* (2021).

Este trabajo está organizado como se indica a continuación. La sección de Materiales y Métodos describe el proceso de extracción de los metadatos y de las señales PRNU, así como el cálculo de las PDF de todas las señales PRNU extraídas de las imágenes a analizar. Se indican las ventajas de usar las señales PRNU como indicios para identificar el dispositivo de captura de una imagen digital y presenta la definición e implementación de la distancia de Hellinger como método estadístico de identificación. Así mismo, explica los supuestos del caso de estudio y los requisitos que debe cumplir un analista forense para el manejo de las imágenes y los dispositivos de captura que se reciben cuando se atiende un caso. También incluye un diagrama de proceso del proceder que debe seguir un analista forense, el cual sirvió para definir la funcionalidad del programa de *software* presentado. En la sección Resultados se presenta una descripción de los casos de estudios planteados y sus respectivas tablas de discriminación. También se calcula la precisión que tiene el método propuesto con base en el caso de estudio definido. Finalmente, se presenta la discusión y las conclusiones.

## Materiales y métodos

El método de análisis forense propuesto en este trabajo consta de cuatro fases: *Entrada*, *Procesamiento*, *Salida* y *Comparación*. En la Figura 1 se muestra gráficamente cada una de ellas.



En la fase de Entrada se presentan la imagen en disputa y los dispositivos de captura con los que se obtendrán las imágenes de referencia. En esta fase, además, se verifica la integridad y autenticidad de los objetos digitales que se involucren en el proceso de identificación. Estas acciones permitirán conocer si dichos objetos digitales fueron o no modificados, lo que ayudará a fortalecer la cadena de custodia. En particular, la integridad de las imágenes analizadas se puede verificar a través de una función resumen, comúnmente denominada función HASH, la cual permite obtener una cadena de caracteres unívoca asociada a un archivo, en este caso una imagen digital. La aplicación de una función HASH a la imagen digital de interés permite disponer de un elemento de prueba que ayude a detectar si se generó algún cambio, aunque mínimo, en dicha imagen. Es importante resaltar que las funciones HASH se diseñan bajo el principio del efecto avalancha, esto quiere decir que un pequeño cambio en la cadena de caracteres, recibida a la entrada de la función, generará un gran cambio en la cadena de caracteres que se producen en su salida. Así, en este trabajo, para disponer de las funciones HASH se utiliza la herramienta reportada en Jan (2022), denominada DataHash, la cual contiene las funciones SHA-1, SHA-256, SHA-384, SHA-512, MD2 y MD5. Se considera el uso de esta herramienta debido a la diversidad de funciones HASH que ofrece, ya que incluye variantes de las dos más comunes, la SHA y la MD. Los formatos de salida que entrega esta herramienta son: hexadecimal, HEX, doble, uint8, base64, y para cada imagen digital el valor HASH se calcula a partir del contenido del archivo. En particular, en el programa de software presentado se preconfiguró el uso de la función SHA-1 con salida uint8.

Por otro lado, la autenticidad de la imagen se puede verificar a través de una función MAC (*Message Authentication Code*), que incluye la contraseña personal del analista que realiza el proceso forense. Una función MAC ayuda a asociar un objeto digital con una persona; en este caso, la función MAC relacionará

a la imagen analizada con el analista forense que realizó el análisis. Así, durante el proceso de análisis forense se puede verificar que esa relación se mantenga sin cambio (Bellare *et al.*, 1996). En este trabajo se usa la función HMAC propuesta en Grunnet (2021), la cual incluye las siguientes funciones HASH con contraseñas: SHA-1, SHA-256, SHA-384, SHA-512. De manera similar al caso de las funciones HASH, la herramienta propuesta por Grunnet (2021) ofrece funciones MAC basadas en las variantes de la función SHA. En este caso, y por consistencia con la verificación de integridad, la interfaz presentada tiene preconfigurada el uso de la función HMAC basada en SHA-1 con salida uint8.

En este trabajo, en consistencia con lo indicado en Quintanar-Reséndiz *et al.* (2021) para un caso de análisis, el número de imágenes de referencia obtenidas por cada dispositivo de captura candidato se determina a través de una medida de invarianza. Después, se extrae la señal PRNU de las imágenes de referencia y de las imágenes en disputa. Para este proceso se hace uso del módulo de extracción de señal PRNU que se encuentra en el algoritmo de identificación de dispositivos de captura propuesto en Goljan *et al.* (2009). Este módulo de extracción de señal PRNU se basa en el modelo de ruido  $I = I_0(1 + \varphi) + \delta$  enunciado en Quintanar-Reséndiz *et al.* (2021). Dicho algoritmo de extracción de señal PRNU consta de tres funciones principales: getFingerprint.m, PCE.m y NoiseExtractFromImage.m, las cuales están disponibles en [http://dde.binghamton.edu/download/camera\\_fingerprint/](http://dde.binghamton.edu/download/camera_fingerprint/).

Luego, en la fase de Procesamiento, para todas las señales PRNU extraídas se calcula su PDF, aproximándola a través de la frecuencia relativa como se explica en Quintanar-Reséndiz *et al.* (2021). Un ejemplo de la aproximación de la PDF se puede ver en la Figura 2; en este caso, se capturaron dos imágenes digitales con el dispositivo de captura Casio EX-Z150. La línea en rojo representa la PDF de una imagen considerada de referencia, y la línea punteada en azul representa la PDF de una imagen considerada en disputa. Nótese que las dos PDF son muy parecidas entre sí, esto se debe a que provienen de imágenes capturadas por el mismo dispositivo de captura.

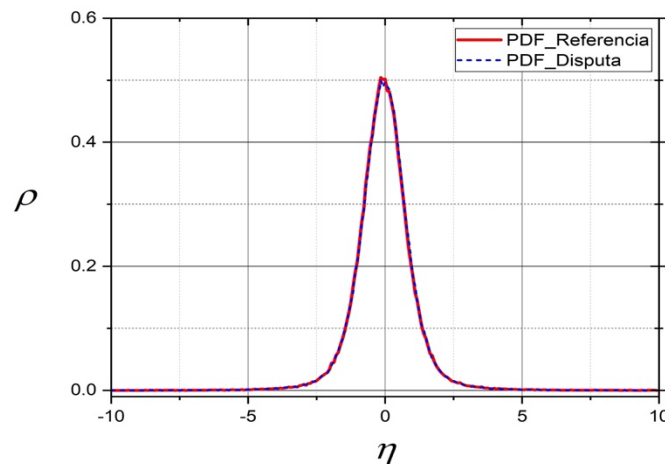


Figura 2. Aproximación de las PDF de dos señales PRNU extraídas de imágenes del mismo dispositivo de captura.  
Fuente: Elaboración propia.

Un caso contrario es el que se presenta en la Figura 3. En este caso, la imagen de referencia se capturó con el dispositivo Casio EX-Z150, y la imagen considerada en disputa se capturó con el dispositivo Olympus  $\mu 1050SW$ . Nótese que es posible diferenciar entre dispositivos a través de la aproximación de las PDF.

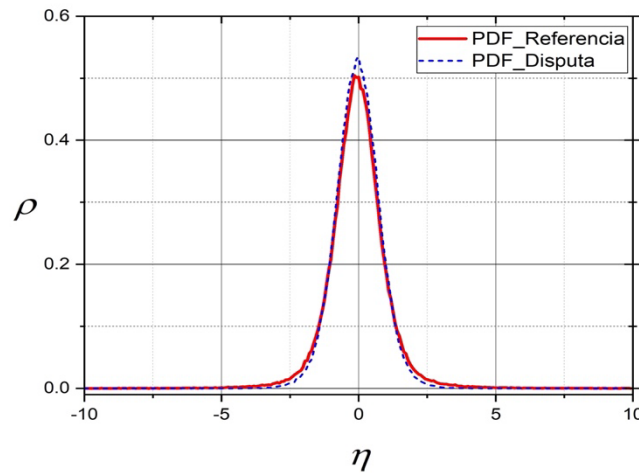


Figura 3. Aproximación de las PDF de dos señales PRNU extraídas de imágenes de diferentes dispositivos de captura.  
Fuente: Elaboración propia.

Entonces, para aproximar la PDF de una señal PRNU es necesario calcular la frecuencia relativa de sus componentes. En la Figura 4 se muestra un ejemplo de las variables involucradas en dicha aproximación.

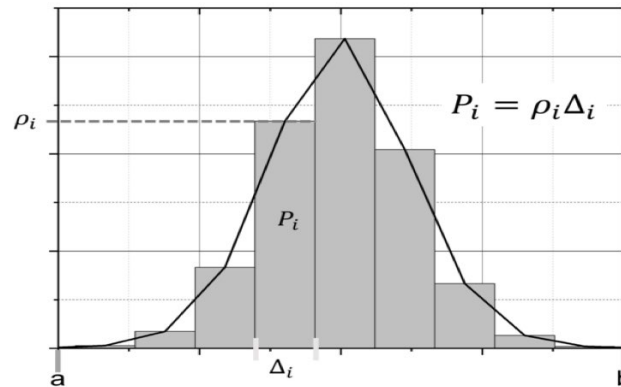


Figura 4. Variables involucradas en la aproximación de la PDF de una señal PRNU extraída de una imagen digital.  
Fuente: Elaboración propia.

De este modo, considerando que la probabilidad de ocurrencia de los componentes en la señal PRNU en total debe ser igual a 1, primero se identifica el rango dinámico de la señal PRNU, esto es, el intervalo  $[a, b]$  donde existe la mayor cantidad de energía de la señal. Después, se define una partición de tamaño  $W$ , esto es, el número de subintervalos en los que se habrá de subdividir el intervalo de observación de la señal PRNU y que servirá para saber cuántas veces la señal PRNU visita cada subintervalo. En este caso, se considera  $W = 256$  y valor que permite observar una PDF de comportamiento suave. De la experiencia de este trabajo observamos que una  $W < 100$  genera un rizo en la PDF y consecuentemente una pérdida de precisión en su definición, y una  $W > 256$  implicaría mayor cálculo para estimar la PDF sin una ganancia importante en la precisión de su definición. Así, una aproximación a la PDF de la señal PRNU se puede establecer a partir de la probabilidad de ocurrencia de la señal PRNU asociada a cada subintervalo, según se expresa en la ecuación 1 y se observa en las Figuras 3 y 4.

$$P_{Ai} = \rho_i \cdot \Delta_{Ai} , \quad (1)$$

$$\Delta_{Ai} = \Delta_{Aj} = \Delta, i \neq j ,$$

donde  $\Delta = \frac{b-a}{W}$ ,  $\sum_i^W P_{Ai} = 1$ ,  $a$  y  $b$  son los límites inferior y superior del rango dinámico y  $W$  es el tamaño de partición.

Por lo tanto, la aproximación a cada componente de la PDF de la señal PRNU se puede definir como sigue:

$$\rho_i = \frac{P_{Ai}}{\Delta} = \frac{1}{m \cdot n} \sum_{u=1}^n \sum_{v=1}^m \frac{1}{\Delta} \cdot B_{Ai}(u, v) , \quad (2)$$

donde  $B_{Ai}$  indica si el píxel de ruido pertenece o no al subintervalo  $A_i$ , y de acuerdo con Quintanar-Reséndiz et al. (2021) se define como sigue:

$$B_{Ai}(u, v) = \begin{cases} 1, & \text{si } (u, v) \in A_i \\ 0, & \text{si } (u, v) \notin A_i \end{cases} \quad (3)$$

Entonces, cuando se considera una partición regular, la ecuación 2 se puede escribir de la siguiente manera:

$$\rho_i = \frac{W}{b-a} \cdot \frac{1}{m \cdot n} \sum_u^n \sum_v^m B_{Ai}(u, v) . \quad (4)$$

Es así como se puede calcular la PDF de la señal PRNU extraída de cada una de las imágenes digitales analizadas y, como se muestra en las Figuras 3 y 4, es posible usar la PDF como una huella digital que permita asociar una imagen en disputa con las imágenes de referencia tomadas de su dispositivo de captura.

Ahora, para realizar un proceso de discriminación objetivo se utiliza a la distancia de Hellinger como una métrica que permita encontrar la similitud entre las imágenes que pertenecen a un dispositivo de captura.

La integral de Hellinger fue introducida por E. Hellinger en 1909 y, en términos de ella, se definió la distancia de Hellinger (HLD), que es utilizada para medir la similitud entre dos funciones de densidad de probabilidad. Para obtener la HLD de dos PDF discretas:  $P = (p_1, p_2, p_3, \dots, p_N)$  y  $Q = (q_1, q_2, q_3, \dots, q_N)$ , es necesario aplicar la ecuación 5 (Chang et al., 2015):

$$HLD^2(P, Q) = 1 - \sum_{n=1}^N \sqrt{p_n q_n} , \quad (5)$$

donde  $0 \leq HLD^2 \leq 1$ ,  $HLD^2 = 0$  si y solo si  $P = Q$ .

Otra métrica que se utiliza para medir la similitud entre dos PDF es la divergencia de Kullback-Leibler (KLD) utilizada en Quintanar-Reséndiz et al. (2021), pero presenta un problema de cálculo, ya que se indetermina cuando se evalúa para los casos en que  $P = 0$  o  $Q = 0$ . En esos casos, si no se tiene cuidado en la implementación, ocurre una división por 0 o el cálculo del logaritmo de 0. En una implementación



práctica se tiene que establecer una condición que evite estas dos situaciones de indeterminación. En el caso de la HLD, esto no ocurre, ya que  $0 \leq HLD^2 \leq 1$ ,  $HLD^2 = 0$  si y solo si  $P = Q$  y  $HLD^2 = 1$  si  $P = 0$  o  $Q = 0$ .

Para el proceso de discriminación se considera que  $D_{[d]}^{[j]}$  es la  $j$ -ésima imagen de disputa perteneciente al dispositivo de captura  $d$ , con  $j = 1, 2, 3, \dots, N$ , y  $R_{[r]}^{[i]}$  es la  $i$ -ésima imagen de referencia tomada con el dispositivo de captura  $r$ , con  $i = 1, 2, 3, \dots, S$ . Así, para cada par  $[D_{[d]}^{[j]}, R_{[r]}^{[i]}]$ , y sobre el total  $C$  de dispositivos de captura, se calcula el mínimo entre el total de las  $C$  distancias de Hellinger calculadas entre la PDF de la señal PRNU de  $D_{[d]}^{[j]}$  y la PDF de la señal PRNU de  $R_{[r]}^{[i]}$ ; es decir,

$$mHLD(D_{[d]}^{[j]}, R_{[h]}^{[i]}) = \min(HLD(D_{[d]}^{[j]}, R_{[l]}^{[i]})_{l=1}^C). \quad (6)$$

Además, en este proceso, y con la finalidad de definir una medida de similitud, se identifica el dispositivo de captura  $h \in [1, C]$ , para el cual se obtuvo ese valor mínimo entre todas las HLD calculadas. Entonces, el valor de  $h$  queda definido por la ecuación 7:

$$h = l \text{ cuando } HLD(D_{[d]}^{[j]}, R_{[l]}^{[i]}) = mHLD(D_{[d]}^{[j]}, R_{[h]}^{[i]}). \quad (7)$$

De esta manera, la tasa de asociación de la imagen de disputa  $D_{[d]}^{[j]}$  respecto a cada dispositivo candidato  $k$  se define por la ecuación 8:

$$f_k(h, D_{[d]}^{[j]}) = \frac{1}{S} \sum_{i=1}^S T_i(h, k), \quad (8)$$

donde la función de pertenencia queda definida como

$$T_i(h, k) = \begin{cases} 1, & \text{si } h = k \\ 0, & \text{si } h \neq k \end{cases}$$

De este modo, la matriz de confusión definida para la fase Salida se construye a través de la función de similitud dada por la ecuación 9:

$$SIM_{k,d} = \left[ \frac{1}{N} \sum_{j=1}^N f_k(h, D_{[d]}^{[j]}) \right] \times 100. \quad (9)$$

La matriz de confusión servirá como un resumen que permitirá ver todos los resultados de las imágenes analizadas contra los posibles dispositivos de captura. Las columnas de esta matriz representarán las imágenes en disputa analizadas, y en las filas se encontrarán los posibles dispositivos de captura. En la diagonal principal se espera que ocurran los valores máximos, indicando que aquel dispositivo de captura que se encuentre en la misma fila será el dispositivo de captura identificado. Completada la matriz de

confusión se podrán determinar los dispositivos de captura para cada una de las imágenes en disputa analizadas y generar un informe técnico que además de presentarla indicará el porcentaje de precisión del método propuesto. Finalmente, se llegará a la fase de *Comparación*, en la que los resultados obtenidos pueden compararse contra los resultados obtenidos por otros autores. Cabe hacer mención que el programa de *software* desarrollado incluye también el método propuesto por Quintanar-Resendiz *et al.* (2021), y contra este método también podría hacerse una comparación para cualquier otro caso de estudio. En este trabajo se usa el mismo caso de estudio definido para Quintanar-Resendiz *et al.* (2021), y en la Sección de Resultados se presenta una comparación entre el método propuesto contra los métodos presentados por Quintanar-Resendiz *et al.* (2021). Con la finalidad de tener una herramienta de análisis forense que permita aplicar el método propuesto, se diseñó e implementó un programa de *software* en el entorno de Matlab™. La Figura 5 muestra el diagrama de proceso que debe seguir un analista forense cuando pretende identificar un dispositivo de captura para una o más imágenes digitales utilizando el programa de *software* desarrollado. En este proceso las premisas operativas básicas que debe seguir son:

-Recibir una o varias imágenes en disputa, las cuales estarán bajo estudio, así como un conjunto de *C* dispositivos de captura candidatos.

-Generar para cada dispositivo de captura un conjunto de *S* imágenes de referencia. A partir de ellas, se obtendrá la huella digital de cada dispositivo de captura. En congruencia con Zhao *et al.* (2019) y Al-Ani & Khelifi (2017), el tamaño de cada conjunto debe incluir 50 imágenes, pero como lo menciona Quintanar-Reséndiz *et al.* (2021), es suficiente incluir en cada conjunto 30 imágenes, por lo tanto,  $S=30$ .

-Ejecutar un proceso de discriminación basado en la señal PRNU extraída con el algoritmo propuesto en Goljan *et al.* (2009) e identificar el dispositivo de captura a través de una implementación de la distancia de Hellinger que compara las PDF de las señales PRNU extraídas tanto de las imágenes en disputa como de las imágenes de referencia de cada dispositivo de captura candidato.

-Interpretar el reporte generado en este proceso y emitir una opinión técnica.

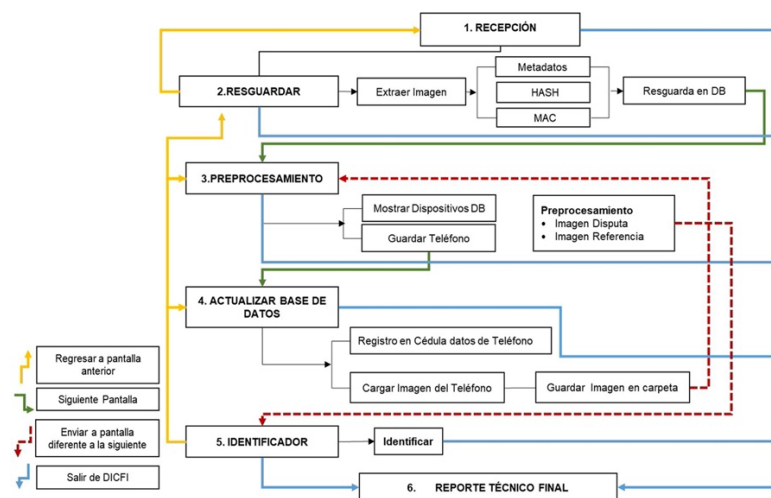


Figura 5. Diagrama de proceso que un analista forense debe seguir si quiere identificar el dispositivo de captura de una imagen digital en disputa a través del programa de *software* desarrollado en Matlab™.

Fuente: Elaboración propia.

Los módulos del programa de *software* desarrollado son seis. Los módulos que corresponden a la fase de Entrada son del 1 al 4 y los módulos 5 y 6 corresponden a la fase de Procesamiento y Salida, respectivamente. En el módulo 1, "RECEPCIÓN", se recibe la información del caso de estudio, las imágenes en disputa y los dispositivos de captura elegibles. En este módulo se debe documentar el caso de estudio. El módulo 2, "RESGUARDAR", extrae de las imágenes en disputa los metadatos y los valores resumen (HASH y MAC). El módulo 3, "PREPROCESAMIENTO", muestra los teléfonos registrados en la base de datos. El módulo 4, "ACTUALIZAR BASE DE DATOS", permite, en caso necesario, registrar un nuevo dispositivo de captura y sus imágenes de referencia asociadas. El módulo 5, "IDENTIFICADOR", procesa la imagen digital en disputa, y el módulo 6, "REPORTE TÉCNICO FINAL", genera un informe con la opinión sobre la identificación del dispositivo de captura de la imagen digital en disputa.

## Casos de estudio

En este trabajo se definieron dos casos de estudio que se construyeron con imágenes digitales descargadas de la base de datos de imágenes de Dresden propuesta en 2010 por Gloe & Bhôme (2010). El primer caso de estudio define la línea base de comparación de este trabajo, y fue preparado para mostrar el uso del algoritmo de Goljan *et al.* (2009). En este primer caso se seleccionaron 31 imágenes por cada uno de los  $C = 8$  dispositivos de captura diferentes del apartado *Flatfield frame*. Para cada dispositivo de captura, de las 31 imágenes, se consideraron  $S = 30$  como imágenes de referencia y se usan para construir la huella digital del dispositivo de captura; la imagen restante se considera como imagen en disputa, esto es  $N = 1$ . De esta manera, en total se usaron 240 imágenes de referencia y ocho imágenes en disputa. Las características del caso de estudio se pueden ver en la Tabla 1.

Tabla 1. Características del caso de estudio 1.

Fuente de Captura	Nemotécnico	Resolución	Imágenes de Referencia	Imágenes en Disputa
Casio Ex-Z150	CE50	3264x2448	30	1
Canon Ixus-55	CI55	1944x2592	30	1
Canon Ixus-70	CI70_1	2304x3072	30	1
Canon Ixus-70	CI70_2	2304x3072	30	1
Nikon S710	NS71	3264x4352	30	1
Olympus Mju	OM10	3648x2736	30	1
Praktica Dcz-5.9	PD59	2560x1920	30	1
Rollei 7325xs	RO73	3072x2304	30	1

Fuente: Elaboración propia.

El segundo caso de estudio fue preparado ampliando el primer caso y se aplica para mostrar el uso del método propuesto. Es más amplio que el primer caso, ya que no considera una imagen en disputa, sino 20 por cada dispositivo de captura. Las imágenes digitales adicionales usadas para este segundo caso de estudio también se tomaron de la base de datos de Dresden. De esta forma, se seleccionaron 50 imágenes digitales por cada uno de los  $C = 8$  dispositivos de captura. De cada dispositivo se tomaron  $S = 30$  imágenes de referencia y  $N = 20$  imágenes en disputa. En total se usaron 240 imágenes de referencia y 160 imágenes en disputa. Las características de este caso de estudio se encuentran en la Tabla 2. Es importante hacer notar que este segundo caso de estudio es el mismo usado en Quintanar-Reséndiz *et al.* (2021) para cuando se evaluó el algoritmo de Goljan *et al.* (2009) y el método ahí propuesto.

Tabla 2. Características del caso de estudio 2.

Fuente de Captura	Nemotécnico	Resolución	Imágenes de Referencia	Imágenes en Disputa
Casio Ex-Z150	CE50	3264x2448	30	20
Canon Ixus-55	CI55	1944x2592	30	20
Canon Ixus-70	CI70_1	2304x3072	30	20
Canon Ixus-70	CI70_2	2304x3072	30	20
Nikon S710	NS71	3264x4352	30	20
Olympus Mju	OM10	3648x2736	30	20
Praktica Dcz-5.9	PD59	2560x1920	30	20
Rollei 7325xs	RO73	3072x2304	30	20

Fuente: Elaboración propia.

## Resultados

Con la finalidad de ilustrar cómo funciona el método propuesto, se usaron los dos casos de estudio descritos en la sección anterior. Para el primer caso, la Tabla 3 muestra los valores de correlación obtenidos utilizando el algoritmo propuesto en Goljan *et al.* (2009). En este primer caso, los dispositivos de captura fueron numerados del 1 al 8, al igual que se hizo con las imágenes en disputa, de manera que se sabe con seguridad que la imagen en disputa  $j = 1, 2, 3, \dots, 8$  corresponde al dispositivo de captura  $j$ . En la Tabla 3, las filas corresponden a los dispositivos de captura y las columnas a las imágenes en disputa. Cada celda corresponde al valor de correlación que genera el algoritmo de Goljan *et al.* (2009) cuando se contrasta la imagen en disputa  $D_j$  con el dispositivo de captura  $C_j$ , considerando que  $j = 1, 2, 3, \dots, 8$ . Note que en la diagonal principal de la Tabla 3 existe un valor relativo de referencia que corresponde a los valores máximos por columna de todos los valores de correlación. Estos valores máximos corresponden a la posición en la que coinciden una imagen en disputa con su dispositivo de captura. Además, debe resaltarse también que en todos los casos analizados las identificaciones son positivas, ya que cada imagen en disputa genera el valor máximo de correlación con el dispositivo de captura que la capturó. Pero se selecciona aquella cuyo valor es el más grande de todos. De esta forma, la Tabla 4 expresa la razón de similitud calculada a partir de los resultados de la Tabla 3. Nótese que se conserva el criterio de que las filas corresponden a los dispositivos de captura y las columnas a las imágenes en disputa. En este caso, el valor máximo de la razón de similitud es del 100%, lo que quiere decir que la imagen en disputa está totalmente correlacionada con el dispositivo de captura correspondiente. El valor mínimo de la razón de similitud es 0% y quiere decir que no hay absolutamente ninguna correlación entre la imagen en disputa y el dispositivo de captura correspondiente. Es importante resaltar que en la diagonal principal de la Tabla 4 se encuentra el valor máximo de la razón de similitud. Así, los resultados reportados confirman que el algoritmo propuesto por Goljan *et al.* (2009) asocia correctamente cada imagen en disputa con su respectivo dispositivo de captura.

Tabla 3. Resultados de correlación cuando se implementa el algoritmo de Goljan *et al.* en el caso de estudio 1.

		Imágenes en Disputa							
		CE50	CI55	CI70_1	CI70_2	NS71	OM10	PD59	R073
Dispositivos de Captura	CE50	29123	-0.108	-0.093	-0.032	-0.329	-	-1.288	0.683
	CI55	0.224	96244	-0.974	0.003	0.895	0.003	2.761	-0.500
	CI70_1	-0.004	0.856	21095	0.840	-2.062	1.369	-0.000	0.476
	CI70_2	0.047	1.362	0.001	46477	-0.695	-	0.229	0.513
	NS71	0.006	-0.327	-2.922	-1.043	6450	0.110	-1.106	2.532
	OM10	1.572	0.023	0.521	-1.275	0.008	12280	-0.053	0.747
	PD59	-0.019	0.651	0.066	3.946	1.140	-	48217	-0.039
	R073	-0.085	-0.193	-1.524	-0.849	0.165	-	3.392	39152
							0.205		

Fuente: Elaboración propia.

Tabla 4. Similitud en porcentaje cuando el algoritmo de Goljan *et al.* se aplica al caso de estudio 1.

		Imágenes en Disputa							
		CE50	CI55	CI70_1	CI70_2	NS71	OM10	PD59	R073
Dispositivos de captura	CE50	100	0.000	0.000	0.000	0.005	0.001	0.003	0.002
	CI55	0.001	100	0.005	0.000	0.014	0.000	0.006	0.001
	CI70_1	0.000	0.001	100	0.002	0.032	0.011	0.000	0.001
	CI70_2	0.000	0.001	0.000	100	0.011	0.017	0.001	0.001
	NS71	0.000	0.000	0.014	0.002	100	0.001	0.002	0.007
	OM10	0.005	0.000	0.003	0.003	0.000	100	0.000	0.002
	PD59	0.000	0.001	0.000	0.009	0.018	0.002	100	0.000
	RO73	0.000	0.000	0.007	0.002	0.003	0.002	0.007	100

Fuente: Elaboración propia.

Por otro lado, para el segundo caso de estudio, los resultados de las comparaciones se encuentran en la Tabla 5; para este caso,  $C = 8$ ,  $S = 30$  y  $N = 20$  y el grado de pertenencia de una imagen en disputa, con cada dispositivo de captura considerado, se determina a través de la razón de similitud definida en la ecuación 8. Por lo tanto, cada celda contiene el valor de razón de similitud,  $SIM_{k,d}$ . Nótese que la diagonal principal de la Tabla 5 contiene el valor máximo de similitud, lo que quiere decir que el método propuesto identifica correctamente el dispositivo de captura para cada imagen en disputa. Es importante resaltar que  $SIM_{k,d} \in [0,100]$ , siendo que si  $SIM_{k,d} = 100$  entonces la imagen en disputa analizada corresponde con el dispositivo de captura en un 100%, y si  $SIM_{k,d} = 0$  entonces la imagen en disputa analizada no corresponde con el dispositivo de captura en cuestión. Con estos resultados es posible asociar la imagen en disputa analizada con aquel dispositivo de captura que genere la razón de similitud máxima.

Tabla 5. Similitud en porcentaje obtenida cuando el algoritmo propuesto se aplica al caso de estudio 2.

	Imágenes en Disputa							
	CE50	CI55	CI70_1	CI70_2	NS71	OM10	PD59	R073
Dispositivos de Captura	CE50	100.00	0.00	0.00	0.00	0.00	0.00	0.00
	CI55	0.00	100.00	0.00	0.00	0.00	0.00	0.00
	CI70_1	0.00	0.00	96.33	0.50	0.00	0.00	0.00
	CI70_2	0.00	0.00	3.67	99.50	14.33	0.00	0.00
	NS71	0.00	0.00	0.00	0.00	85.67	0.00	0.00
	OM10	0.00	0.00	0.00	0.00	0.00	100.00	0.00
	PD59	0.00	0.00	0.00	0.00	0.00	0.00	100.00
	RO73	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Fuente: Elaboración propia.

Dado que el segundo caso de estudio es el mismo que el presentado en Quintanar-Reséndiz *et al.* (2021), la comparación de la Tabla 5 puede hacerse de manera directa contra las tablas de resultados expresadas en aquel trabajo. La Tabla 6 permite comparar los resultados aplicando tanto el método de Goljan *et al.* como el de Quintanar-Reséndiz *et al.* a través de la efectividad del proceso de identificación de los tres algoritmos considerados. Esta tabla resumen se construye a partir de los resultados reportados en Quintanar-Reséndiz *et al.* y los resultados presentados en este trabajo.

Tabla 6. Comparación entre métodos para la identificación de dispositivos de captura cuando se comparan las huellas digitales insertadas en las imágenes en disputa contra la huella digital de su dispositivo de captura.

Objetos de Comparación	Porcentaje de similitud para identificación		
	PCE (Quintanar- Reséndiz, et al., 2021)	KLD (Quintanar- Reséndiz, et al., 2021)	HLD Algoritmo propuesto
N_CE50 vs C_CE50	100.00	100.00	100.00
N_CI55 vs C_CI55	100.00	100.00	100.00
N_CI70_1 vs C_CI70_1	100.00	95.00	96.33
N_CI70_2 vs C_CI70_2	100.00	99.82	99.50
N_NS71 vs C_NS71	100.00	100.00	85.67
N_OM10 vs C_OM10	100.00	100.00	100.00
N_PD59 vs C_PD59	100.00	100.00	100.00
N_RO73 vs C_RO73	100.00	100.00	100.00
Precisión	100.00	99.35	97.68

Fuente: Elaboración propia.

Adicionalmente, las Tablas 7 y 8 presentan los dos algoritmos fundamentales del método propuesto para el proceso de discriminación. El algoritmo 1 (HLD) estima la divergencia de Hellinger que existe entre dos funciones de densidad de probabilidad. El algoritmo 2 (maxSIM) encuentra el valor máximo de similitud en la matriz de confusión que contiene los valores promedio de similitud. Aquellos dispositivos de captura cuyos valores promedio de similitud son los valores máximos se consideran como los dispositivos de captura de las imágenes en disputa.

Tabla 7. Primer algoritmo fundamental del método propuesto para el proceso de discriminación.

Algoritmo 1
<p>Nombre: HLD</p> <p>Descripción básica: Estimación de la divergencia de Hellinger para dos funciones de densidad de probabilidad</p> <p>Requiere: pdf_1; % huella digital estadística estimada para el dispositivo de captura estimada con las imágenes de referencia. Pdf_1 es el promedio de las funciones de densidad de probabilidad del PRNU de las imágenes de referencia</p> <p>Requiere: pdf_2; % huella digital insertada en la imagen en disputa por el dispositivo que la capturó. Pdf_2 es la función de densidad de probabilidad del PRNU de la imagen en disputa</p> <pre> longitud = size(pdf_1,1); HLDi = zeros(1, longitud); i ← 1; while i ≤ longitud hacer     HLDi(i) = sqrt(pdf_1(i) * pdf_2(i));     i = i + 1; end while HLD = 1 - sum(HLDi); Devuelve HLD; </pre>

Fuente: Elaboración propia.

Tabla 8. Segundo algoritmo fundamental del método propuesto para el proceso de discriminación.

Algoritmo 1
<p>Nombre: HLD</p> <p>Descripción básica: Estimación de la divergencia de Hellinger para dos funciones de densidad de probabilidad</p> <p>Requiere: pdf_1; % huella digital estadística estimada para el dispositivo de captura estimada con las imágenes de referencia. Pdf_1 es el promedio de las funciones de densidad de probabilidad del PRNU de las imágenes de referencia</p> <p>Requiere: pdf_2; % huella digital insertada en la imagen en disputa por el dispositivo que la capturó. Pdf_2 es la función de densidad de probabilidad del PRNU de la imagen en disputa</p> <pre> longitud = size(pdf_1,1); HLDi = zeros(1, longitud); i ← 1; while i ≤ longitud hacer     HLDi(i) = sqrt(pdf_1(i) * pdf_2(i));     i = i + 1; end while HLD = 1 - sum(HLDi); Devuelve HLD; </pre>

Fuente: Elaboración propia.

## Discusión

Ante la realidad de que el marco legal mexicano permite el uso de imágenes digitales como soporte en un juicio, se tiene la necesidad de contar con herramientas que faciliten el trabajo de un analista forense cuando se quiere saber cuál es la fuente de origen de una imagen digital. Es así como este trabajo presenta un método basado en la distancia de Hellinger, calculada entre la huella digital de los dispositivos de captura y la huella digital insertada en las imágenes en disputa para identificar su dispositivo de captura. Las huellas digitales se basan en la PDF de señales PRNU extraídas, por un lado, de imágenes de referencia capturadas con los dispositivos candidatos y, por otro, de las imágenes en disputa. El criterio de asociación

que el método propuesto utiliza es el valor máximo de similitud encontrado entre los valores promedio de similitud de cada dispositivo de captura candidato. Entonces, el método propuesto permite asociar unívocamente cada imagen en disputa con su respectivo dispositivo de captura, ya que cuando se comparan las imágenes de disputa contra los dispositivos de captura el porcentaje para cinco de los ocho teléfonos se obtuvo una similitud del 100% cuando la imagen en disputa proviene del ese dispositivo. En los otros tres casos se alcanzó una similitud de 96.33%, 99.50% y 85.67%; se asume siempre que en cada caso la imagen en disputa no fue manipulada.

Al comparar, para el mismo caso de estudio, los resultados obtenidos del método propuesto contra los de Goljan *et al.* y Quintanar-Reséndiz *et al.*, se encuentra que el método de Goljan *et al.* es mejor en cuanto a que el porcentaje de similitud alcanza el 100% para la identificación de dispositivos de captura desde una imagen digital no manipulada; pero, como lo menciona Quintanar-Reséndiz *et al.*, el método de Goljan *et al.* requiere más tiempo para la identificación, ya que es 3.23 veces más lento. Por el contrario, el método de Quintanar-Reséndiz *et al.* es más rápido, pero menos preciso, ya que su porcentaje de similitud promedio es de 99.35%. Además, para su implementación, se debe considerar y evitar las posibles indeterminaciones de la función KLD, cuando  $P = 0$  o  $Q = 0$ . En esos casos, sin el debido cuidado de implementación, ocurriría una división por 0 o el cálculo del logaritmo de 0. Por otra parte, el tiempo de identificación para el método propuesto es semejante al de Quintanar-Reséndiz *et al.* debido a que, además de procesar recortes y no imágenes completas, utiliza la comparación entre PDF. El método propuesto se basa en la función de HLD que, contrariamente a la función de KLD usada en el método de Quintanar-Reséndiz *et al.*, no presenta problemas de indeterminación en su implementación, ya que cuando se utiliza la función HLD ocurre que  $0 \leq HLD^2 \leq 1$ ,  $HLD^2 = 0$  si y solo si  $P = Q$  y  $HLD^2 = 1$  si  $P = 0$  o  $Q = 0$ .

Por otro lado, el método propuesto encuentra su realización práctica a través de un programa de *software* desarrollado en Matlab™, el cual ofrece una solución sencilla e intuitiva para identificar el dispositivo de captura de una o más imágenes digitales no manipuladas. Además, esta herramienta incluye un módulo para la extracción de metadatos, el tratamiento de imágenes digitales (en disputa o de referencia) y la comparación de las huellas digitales de los dispositivos de captura registrados contra la huella digital insertada en cada imagen en disputa. La comparación se puede hacer utilizando alguno de los métodos de identificación habilitados. Esta herramienta al ser modular permite incluir otros algoritmos de identificación de dispositivo de captura, así como otras herramientas de verificación de integridad y autenticidad de las imágenes digitales.

La Figura 6 muestra un ejemplo del módulo de identificación del programa de *software* desarrollado. Este módulo menciona los tres métodos de identificación comparados en la sección de Resultados. Enfatizamos aquí que el algoritmo de Goljan *et al.* consta de dos módulos, uno relativo a la extracción de la señal PRNU y otro para la identificación de dispositivos de captura basado en la correlación tipo PCE que existe entre la señal PRNU de la imagen en disputa contra la huella digital de los dispositivos de captura, la cual se obtiene de la señal PRNU acumulada de las imágenes digitales consideradas como de referencia. Además, en la Figura 7 se muestra un ejemplo del informe que consta de dos páginas. Una primera versión de esta interfaz fue registrada ante INDAUTOR y su número de registro es 03-2021-021111590100-01.



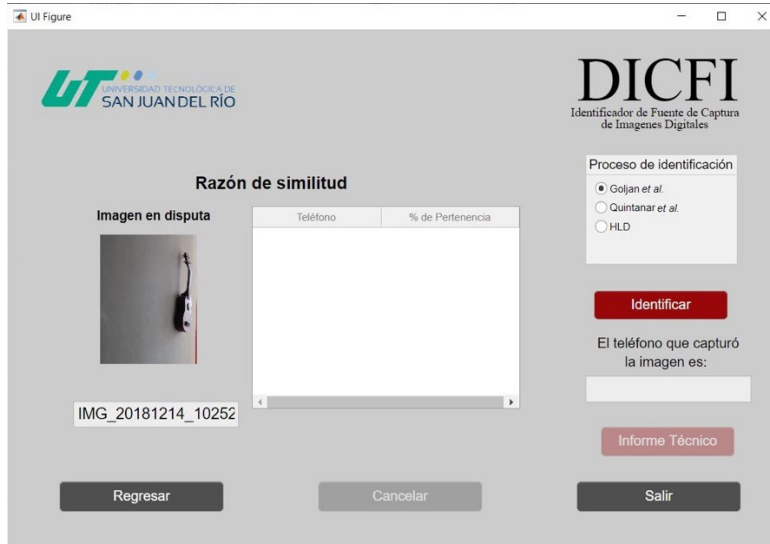


Figura 6. Vista del módulo IDENTIFICADOR para el programa de *software* desarrollado en Matlab™. Fuente: Elaboración propia.

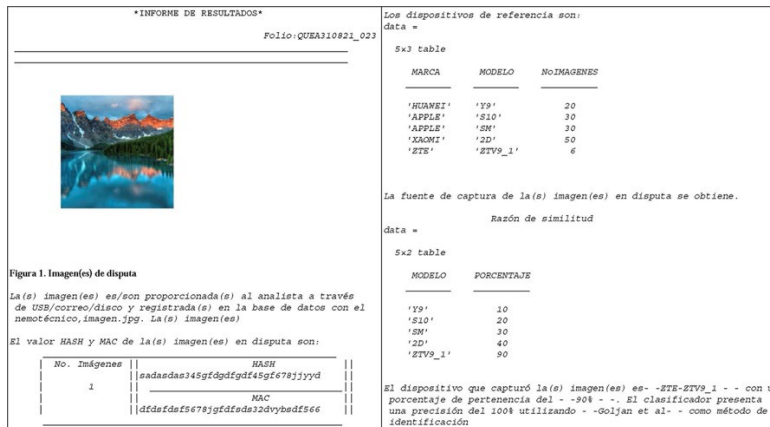


Figura 7. Ejemplo del reporte técnico obtenido del proceso de identificación en el programa de *software* desarrollado en Matlab™. Fuente: Elaboración propia.

## Conclusiones

El trabajo realizado presenta un método basado en la distancia de Hellinger, el cual permite discriminar a qué dispositivo de captura corresponde una imagen digital. La distancia de Hellinger se calcula entre la huella digital de cada dispositivo de captura candidato y la huella digital insertada en la imagen en disputa. En este trabajo se pone de manifiesto que el método aquí propuesto es más rápido que el método de Goljan *et al.* y no tiene los problemas de implementación práctica como los presentados por el método de Quintanar-Reséndiz *et al.*, basado en la función de KLD. El método propuesto se implementó en un programa de *software* que, además de utilizar el método propuesto, permite conectar diferentes métodos para la identificación del dispositivo de captura de imágenes digitales en formato JPEG, sin que el usuario tenga que ser un experto en la codificación de algoritmos para estos métodos. La comparación del método propuesto contra el método de Goljan *et al.* y el método de Quintanar-Reséndiz *et al.* se hizo a través de un caso de estudio que considera ocho dispositivos de captura, 240 imágenes de referencia (30 por dispositivo

de captura) y 160 imágenes en disputa (20 por dispositivo de captura). Los porcentajes promedio de similitud obtenidos fueron de 100%, 99.35% y 97.68%. Aunque el porcentaje promedio de similitud obtenido para el método propuesto es ligeramente menor que para los otros dos métodos, el método propuesto tiene las siguientes ventajas: es más rápido que el método de Goljan *et al.* y durante su implementación no requiere que se impongan condiciones para evitar alguna indeterminación como ocurre en el método de Quintanar-Reséndiz *et al.*, que está basado en la función KLD. El programa de *software* presentado genera un informe en formato PDF y al imprimirse queda prácticamente listo para que sea firmado por el analista y entregado al solicitante del servicio.

## Agradecimientos

A. L. Quintanar Reséndiz agradece al CONACYT por la beca otorgada para estudios de posgrado (CVU: 746317) y al Instituto Politécnico Nacional por el apoyo financiero recibido a través del Proyecto de Desarrollo Tecnológico o Innovación para alumnos del IPN 2019-2020 autorizado por la Secretaría de Investigación y Posgrado.

Los autores agradecen el apoyo recibido del CICATA unidad Querétaro del Instituto Politécnico Nacional, a la Universidad Tecnológica de San Juan del Río (UTSJR) y a los estudiantes del programa educativo de Tecnologías de la Información generación 2018-2020 de la UTSJR que participaron en el desarrollo de este proyecto.

## Conflictos de interés

Los autores declaran que no tienen intereses económicos conocidos ni relaciones personales que pudieran haber influido en el trabajo presentado en este artículo.

## Referencias

- Al-Ani, M., & Khelifi, F. (2017). On the SPN estimation in image forensics: A systematic empirical evaluation. *IEEE Transactions on Information Forensics and Security*, 12(5), 1067-1081. doi: <https://doi.org/10.1109/TIFS.2016.2640938>
- Balamurugan, B., Maghilnan, S., & Kumar, M. R. (2017). Source camera identification using SPN with PRNU estimation and enhancement. *2017 International Conference on Intelligent Computing and Control (I2C2)*, 1-6. doi: <https://doi.org/10.1109/I2C2.2017.8321801>
- Bellare, M., Canetti, R., & Krawczyk, H. (1996). Keying Hash functions for message authentication. En N. Kobitz (ed.), *Advances in Cryptology — CRYPTO '96. Lecture Notes in Computer Science* (pp. 1-15). Springer. doi: [https://doi.org/10.1007/3-540-68697-5\\_1](https://doi.org/10.1007/3-540-68697-5_1)
- Chang, H., Lee, M., Chen, N., Chien, C., & Lee, W. (2015). Feature extraction based hellinger distance algorithm for non-intrusive aging load identification in residential buildings. *2015 IEEE Industry Applications Society Annual Meeting*, 1-8. doi: <https://doi.org/10.1109/IAS.2015.7356778>
- Li, C. (2010). Source camera identification using enhanced sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 5(2), 280-287. doi: <https://doi.org/10.1109/TIFS.2010.2046268>
- Cooper, A. J. (2013). Improved photo response non-uniformity (PRNU) based source camera identification. *Forensic Science International*, 226(1-3), 132-141. doi: <https://doi.org/10.1016/j.forsciint.2012.12.018>
- Fridrich, J. (2009). Digital image forensics. *IEEE Signal Processing Magazine*, 26(2), 26-37. doi: <https://doi.org/10.1109/MSP.2008.931078>
- Gloe, T., & Bhôme, R. (2010). The dresden image database for benchmarking digital image forensics. *Journal of Digital Forensic Practice*, 3(2-4), 150-159. doi: <https://doi.org/10.1080/15567281.2010.531500>

- Goljan, M., Fridrich, J., & Filler, T. (2009). Large scale test of sensor fingerprint camera identification. *Proceedings Media Forensics and Security*, 7254, 170 -181. doi: <https://doi.org/10.1117/12.805701>
- Grunnet, P. (2021). *HMAC Hash message authentication code function*. MathWorks. <https://www.mathworks.com/matlabcentral/fileexchange/46182-hmac-hash-message-authentication-code-function>
- Jan. (2022). *DataHash*. MathWorks. <https://www.mathworks.com/matlabcentral/fileexchange/31272-datahash>
- Instituto Nacional de Estadística y Geografía (INEGI). (2019). [Demografía y Sociedad. TIC's en hogares]. INEGI. <https://www.inegi.org.mx/temas/ticshogares/>
- Long, M., Peng, F., & Zhu, Y. (2019). Identifying natural images and computer generated graphics based on binary similarity measures of PRNU. *Multimedia Tools and Applications*, 78, 489-506. doi: <https://doi.org/10.1007/s11042-017-5101-3>
- Lukas, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2), 205-214. doi: <https://doi.org/10.1109/TIFS.2006.873602>
- Mehrish, A., Subramanyam, A. V., & Emmanuel, S. (2018). Robust PRNU estimation from probabilistic raw measurements. *Signal Processing: Image Communication*, 66, 30-41. doi: <https://doi.org/10.1016/j.image.2018.04.013>
- Quintanar-Reséndiz, A. L., Rodríguez-Santos, F., Pichardo-Méndez, J. L., Delgado-Gutiérrez, G., Jiménez Ramírez, O., & Vázquez-Medina, R. (2021). Capture device identification from digital images using Kullback-Leibler divergence. *Multimedia Tools and Applications*, 80(13), 19513–19538. doi: <https://doi.org/10.1007/s11042-021-10653-1>
- Saito, S., Tomioka, Y., & Kitazawa, H. (2017). A theoretical framework for estimating false acceptance rate of PRNU-based camera identification. *IEEE Transactions on Information Forensics and Security*, 12(9), 2026-2035. doi: <https://doi.org/10.1109/TIFS.2017.2692683>
- Sandoval, A. L., Arenas, D. M., García, L. J., & Hernández-Castro, J. (2015). Analysis of errors in exif metadata on mobile devices. *Multimedia Tools and Applications*, 74, 4735-4763. doi: <https://doi.org/10.1007/s11042-013-1837-6>
- Seshadri, S., Akshatha, K. R., Karunakar, A. K., & Paul, K. H. (2020). A preliminary approach to using PRNU based transfer learning for camera identification. En K. Arai & S. Kapoor (eds.), *Advances in Computer Vision. CVC 2019. Advances in Intelligent Systems and Computing* (pp. 246-255). Springer. doi: [https://doi.org/10.1007/978-3-030-17798-0\\_21](https://doi.org/10.1007/978-3-030-17798-0_21)
- Zhao, Y., Zheng, N., Qiao, T., & Xu, M. (2019). Source camera identification via low dimensional PRNU features. *Multimedia Tools and Applications*, 78, 8247-8269. doi: <https://doi.org/10.1007/s11042-018-6809-4>