

Discurso de aceptación

19 de junio de 2025

Anil K. Jain, galardonado en la categoría de Tecnologías de la Información y la Comunicación (XVII edición)

Con profunda gratitud y humildad, acepto el Premio Fundación BBVA Fronteras del Conocimiento de la XVII edición en la categoría de Tecnologías de la Información y la Comunicación por mis contribuciones al reconocimiento de patrones, con aplicaciones en el reconocimiento de huellas dactilares.

Si examinamos atentamente las yemas de nuestros dedos, veremos un hermoso patrón de crestas y valles intercalados. Estos patrones de crestas y valles —llamados «patrones de crestas de fricción»— también los tenemos en las palmas de las manos y en las plantas de los pies. La curiosidad de los humanos por ellos es muy antigua; de hecho, en artefactos arqueológicos se han encontrado huellas de pulgar de los artesanos, y en muchos países las huellas de pulgar siguen aceptándose como firma en documentos legales.

El reconocimiento de huellas dactilares es el acto de acreditar la identidad de alguien por sus huellas dactilares. El impulso inicial de esta idea vino dado por necesidades de las fuerzas del orden. La Ley sobre Delincuentes Habituales de 1869 formalizó la identificación de delincuentes reincidentes partiendo de la premisa de que las huellas dactilares son *únicas* y *permanentes*. Scotland Yard adoptó la identificación por huellas dactilares en 1905, y el FBI lo hizo en 1924; expertos cualificados realizaban manualmente la identificación.

El uso de ordenadores para el reconocimiento de huellas dactilares no llegó hasta 1980, cuando aparecieron los primeros sistemas automatizados de identificación de huellas dactilares. En 1990 se me presentó la oportunidad de explorar el tema del reconocimiento automatizado de huellas dactilares. Cuando acepté este reto, nadie habría imaginado que esa investigación ayudaría a crear el campo de la biometría: la tecnología que identifica a las personas basándose en rasgos corporales como la cara, las huellas dactilares y el iris de los ojos. Hoy en día, la biometría ya es algo habitual y miles de

millones de personas la utilizan cada día con fines diversos, desde desbloquear el teléfono móvil hasta efectuar pagos o embarcar en un vuelo.

Lo que en realidad ha cambiado en los últimos treinta años es la proliferación y la escala de los sistemas biométricos. Hoy en día, el archivo de huellas dactilares de delincuentes del FBI contiene unos 90 millones de registros. Todos los países del mundo mantienen también una base de datos de este tipo, en la que buscar a quien sea en cada caso. En el trágico 11 de septiembre de 2001, Estados Unidos se enfrentó a su peor atentado terrorista. A raíz de ello, el Congreso de los Estados Unidos promulgó la Ley de Mejora de la Seguridad Fronteriza y Reforma de las Visas de 2002, que permitía el uso en Estados Unidos del reconocimiento de huellas dactilares para la entrada y salida de visitantes. La mayoría de los países siguieron su ejemplo, y hoy en los aeropuertos internacionales los viajeros han de pasar por algún tipo de identificación biométrica para mejorar la seguridad.

El reconocimiento biométrico también se ha aplicado para prevenir el fraude y aumentar la comodidad del usuario. Ejemplos de ello son su uso en los parques Disney para impedir que las entradas se compartan, el programa de identificación biométrica Aadhaar en la India —que tiene una escala de miles de millones de usuarios y ha mejorado la situación de los desfavorecidos— y los sistemas Touch ID y Face ID de Apple para desbloquear teléfonos y permitir pagos móviles. Las siguientes cifras son espectaculares: Aadhaar procesa más de 80 millones de autenticaciones biométricas cada día, y en 2024 se despacharon alrededor de 1000 millones de teléfonos móviles con autenticación biométrica incorporada.

Afortunadamente, ciertas contribuciones de mi investigación han sido muy importantes a la hora de hacer posible esta enorme transformación. Por ejemplo, para reconocer de forma fiable a miles de millones de personas, hay que recopilar la información crucial de sus huellas dactilares y buscarla eficientemente. A estos efectos, hemos desarrollado una técnica con la que representar imágenes de huellas dactilares de cientos de kilobytes de información utilizando un conjunto compacto de rasgos prominentes equiparable a un PIN de 24 caracteres, que permite realizar búsquedas rápidas en bases de datos de cientos de millones de huellas dactilares en cuestión de segundos.

También hemos desarrollado sensores y métodos para recoger y reconocer huellas dactilares de bebés a fin de obtener una identificación fiable con vistas a su atención médica y su vacunación.

El reconocimiento de huellas dactilares parte de la premisa de que las huellas dactilares son únicas y permanentes, pero tal afirmación no era más que una conjetura hasta que nuestros modelos matemáticos la confirmaron científicamente.

No es de extrañar que, debido a su amplio despliegue, los sistemas de reconocimiento de huellas dactilares hayan empezado a atraer la atención de los piratas informáticos y que la privacidad de los datos sea motivo de preocupación. Así, debemos asegurarnos de que el dedo presentado en un

sistema de autenticación sea real, y no una copia artificial de una huella dactilar o una huella dactilar mutilada deliberadamente para evadir la identificación, como se ve en la película *Hombres de negro*. Al objeto de contrarrestar estas amenazas, hemos desarrollado algoritmos de cotejo de huellas dactilares que preservan la privacidad y métodos para detectar las huellas dactilares artificiales y alteradas.

Como puede verse en la serie televisiva sobre la investigación de escenas de crímenes *CSI*, las huellas dactilares parciales y borrosas halladas en escenas de crímenes constituyen una de las pistas más valiosas para identificar al sospechoso. Hemos conseguido realizar muchas aportaciones algorítmicas para añadir precisión a la búsqueda por huellas y minimizar así las detenciones erróneas.

En todas estas aplicaciones de mi investigación, uno de los aspectos más gratificantes ha sido ver cómo las contribuciones han salido del laboratorio para surtir efectos en el mundo real. Dado el aumento del desorden mundial, las amenazas a la seguridad, el fraude financiero y la desigualdad económica, el reconocimiento biométrico seguirá siendo necesario para identificar de forma fiable a las personas.

Una vez más, es un gran honor para mí recibir este premio.