With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission - Directorate-General Justice, Freedom and Security

Cómo encontrar una imagen, aunque haya sido modificada.

Autores

Diego García Ordás – ULE
Laura Fernández Robles – ULE
María Teresa García Ordás – ULE
Óscar García-Olalla – ULE
Enrique Alegre Gutiérrez – ULE

Resumen

La manipulación de imágenes es una práctica muy común y fácil de realizar por cualquier persona. Manipular una imagen puede resultar muy útil para corregir defectos, embellecerla o crear arte pero también puede tener fines maliciosos. Por esta razón, la manipulación de imágenes, ya sea voluntaria (ocultación de rostros, añadido de marcos o de marcas de agua) o involuntaria (cambios de formato, de compresión) se ha convertido en un problema a la hora de identificar y buscar imágenes en grandes bases de datos. Para contrarrestar este problema se utiliza la técnica llamada *búsqueda por similitud* mediante el uso de hashes perceptuales pero desafortunadamente no es válida para todo tipo de modificaciones. La Universidad de León en el marco del proyecto europeo ASASEC está trabajando, entre otras cosas, en proporcionar una solución mediante hashes perceptuales que resuelva este problema mejorando las técnicas existentes.

Contenido

Dicen que una imagen vale más que mil palabras y esto nos ha llevado al interés por modificar las imágenes a nuestro antojo con fines muy diversos. La manipulación de imágenes nació casi a la par que la propia fotografía y se ha usado en incontables ocasiones a lo largo de la historia, unas veces con fines estéticos (Figura 1) y otras muchas con fines políticos (Figura 2). Modificar imágenes está al alcance de cualquiera, ya no se necesitan grandes habilidades ni potentes programas informáticos. Prueba de ello son los muchos adolescentes con conocimientos básicos de informática que retocan sus fotografías antes de compartirlas en redes sociales. Con la cantidad de software existente hoy en día se pueden crear falsificaciones muy creíbles.

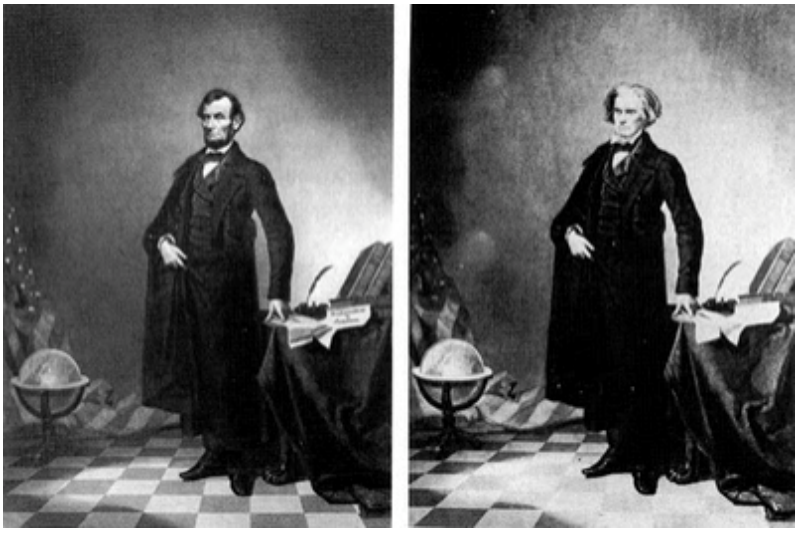

Figura 1: Cabeza de Abraham Lincoln sobre el cuerpo de John Calhoun (1860).

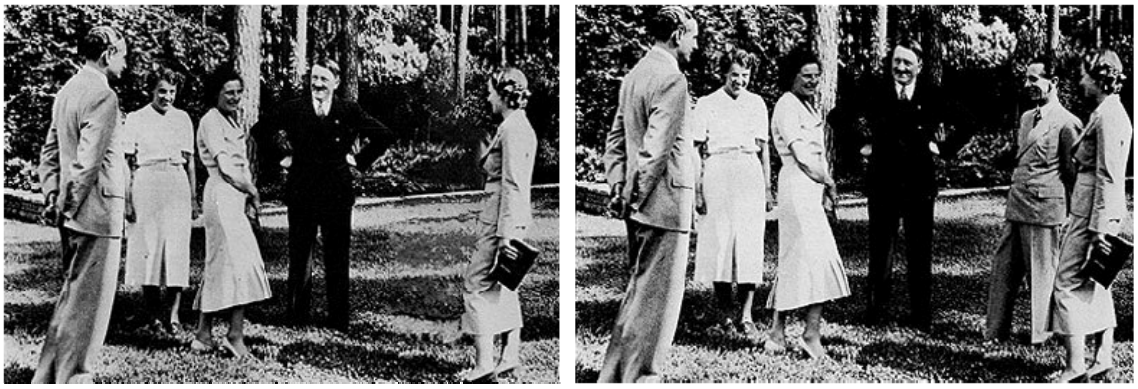

Figura 2: Ministro de propaganda nazi eliminado de una fotografía.

De esta manera, la manipulación de imágenes se ha convertido en un problema en algunos ámbitos como la lucha contra la pornografía infantil, objeto de nuestro estudio. Una de las principales pistas a seguir por los cuerpos de policía cuando investigan estos delitos, es la detección de imágenes ilegales. En los comienzos de la lucha contra la pornografía infantil, una imagen sospechosa se comparaba con bases de datos de imágenes ilegales y si existía alguna coincidencia era catalogada como ilegal. Sin embargo, las nuevas imágenes confiscadas pueden no ser idénticas, solo visualmente parecidas, ya que han sufrido algún tipo de manipulación (compresiones, cambios de tamaño, cambios de brillo y contraste, ocultación de rostros, etc). Este es un serio obstáculo pues la imagen no sería catalogada como ilegal y los delincuentes aprovecharían esta deficiencia. Para contrarrestar este fenómeno se utiliza un proceso llamado *búsqueda por similitud* que es capaz de encontrar no solo imágenes idénticas, si no también imágenes muy parecidas. Uno de los métodos más utilizados a la hora de realizar *búsqueda por similitud* es el *hashing robusto* o *hashing perceptual* del que hablaremos más adelante.

ASASEC (Advisory System Against Sexual Exploitation of Children) es un proyecto europeo de investigación que tiene como objetivo proporcionar una solución tecnológica para ayudar en la lucha contra la pornografía infantil. El proyecto es desarrollado por un consorcio de entidades públicas y privadas, especialistas en tecnología y, en su mayoría, con un acentuado carácter innovador, entre los que se incluyen el INTECO (Instituto Nacional de Tecnologías de la Comunicación), la

Universidad de León, la Asociación de Ingenieros e Ingenieros Técnicos en Informática, la Brigada de Investigación Tecnológica de la Policía Nacional y la Universidad Politécnica de Madrid.

Por su parte, la Universidad de León contribuye con el desarrollo y prueba de una de las tareas más innovadoras de ASASEC, la aplicación de técnicas de visión artificial para el análisis de evidencias en bases de datos de pornografía infantil.

En concreto, la Universidad de León está trabajando en varios métodos de visión artificial, entre los que destacan los siguientes:

- **Detección de entidades en diferentes escenas**. Las imágenes delictivas a veces contienen formas o pistas que la policía, con su experiencia, puede reconocer de otras escenas pasadas. Por lo tanto, se pueden rastrear escenarios y enlazar evidencias manualmente. La Universidad de León está creando un sistema automático de detección de formas mediante el cual, se pueda realizar esta tarea de manera automatizada.
- **Catalogación de escenas y detección de manipulaciones mediante el uso de hashes perceptuales.** Como se comentaba anteriormente, es muy habitual que las imágenes delictivas sean manipuladas (ocultación de rostros, inserción de marcas de agua, etc.) dificultando su catalogación mediante el uso actual de hashes criptográficos. La Universidad de León está desarrollando un método de hashing perceptual robusto contra todas estas modificaciones que sustituirá a los sistemas actuales.

Encontrando imágenes mediante hashing percetual

Un hash es un identificador único asociado a un fichero, una especie de resumen del fichero basado en su contenido. Es decir, generar un hash de un fichero es algo así como convertir ese fichero en un fragmento de ``texto'' que lo represente. El hashing perceptual es un caso particular de hashing que se aplica a imágenes. Consiste en extraer una representación simple de la imagen, de manera que pequeños cambios sobre ella desde el punto de vista del sistema de percepción humano impliquen pequeños cambios en su hash perceptual, y del mismo modo, grandes cambios sobre la imagen hagan variar su hash perceptual de manera considerable (Figura 3)

Figura 3: Izquierda: imagen original, derecha: imagen manipulada mediante cambios de color. Hash MD5 extraído de la imagen original: *''bb4f0a96c77e8737d02755457c2e49c8*``, Hash MD5 extraído de la imagen manipulada: *''6d4d51dfc23becf3edb0019448f78c8c*``. Hash Perceptual (pHash dct) extraído de la imagen original: *''4e1e4967f518cec2''*, Hash Perceptual (pHash dct) extraído de la imagen manipulada: *''4e1e5d47b518cec0''*

Como podemos ver en las imágenes, ambas son muy parecidas desde el punto de vista humano, sin embargo un hashing criptográfico (MD5 como el mostrado en la figura) no es capaz de reflejar esta similitud. Podemos utilizar un hash criptográfico para verificar la integridad de una imagen, pero este tipo de hash no nos ofrece información sobre su estructura visual. Como se puede observar, sus hashes criptográficos no tienen ningún parecido, sin embargo los hashes perceptuales sí lo tienen, es decir, la distancia de sus hashes perceptuales es muy pequeña. Si las imágenes fuesen visualmente distintas, sus hashes perceptuales tendrían mucha distancia uno de otro, quedando reflejado de esta manera el parecido entre dos imágenes en las distancias entre sus hashes perceptuales.

Conociendo el hash perceptual de las imágenes de una base de datos se pueden realizar búsquedas y catalogaciones de imágenes. Si tenemos una base de datos con millones de imágenes y queremos buscar una imagen determinada, una búsqueda automática exhaustiva conllevaría mucho tiempo: habría que mirar imagen por imagen si se corresponden con la que estamos buscando. Además, si nuestra imagen ha sufrido alguna modificación (compresión a distinta calidad o formato, escalado, cambios de brillo y contraste…) es muy posible que una búsqueda exhaustiva no llegase a encontrarla, ya que no existiría en nuestra base de datos una imagen exactamente igual a la buscada. Este problema se puede solucionar haciendo uso del hash perceptual. De esta manera, cada imagen estaría asociada a un hash de un tamaño fijo (usualmente menor de 512 bits dependiendo del método utilizado), mucho más rápido de buscar y de comparar que una imagen completa y además robusto contra diferentes tipos de modificaciones.

En la práctica actual se están utilizando hashes criptográficos para la indexación de imágenes y vídeos de material pornográfico incautado. A diferencia del hash perceptual, el hash criptográfico no depende de la percepción que un humano tiene sobre una imagen, si no de la estructura binaria interna de la imagen, esto es, el código binario que se utiliza para representar dicha imagen en un ordenador. Por ese motivo, un simple cambio de un bit, prácticamente imperceptible para el ojo humano, haría que se generase un hash criptográfico completamente distinto al original que no nos permitiría discernir si ambas imágenes son la misma desde el punto de vista de la percepción humana. Como hemos dicho es muy común realizar modificaciones sobre las imágenes: correcciones de color, añadido de marcas de agua, rotaciones, escalados, compresiones, etc. por ese motivo, la Universidad de León propone el uso de hashes perceptuales robustos contra todos estos tipos de manipulaciones en el marco del proyecto ASASEC.

Propuestas actuales

Hoy en día, gracias a la utilización de hashes perceptuales, se puede detectar prácticamente cualquier manipulación sobre las imágenes que permita a la policía encontrar coincidencias. Alguno de esos métodos han sido ampliamente utilizados y muchos de ellos están siendo objeto de continuas mejoras. Por ejemplo, Yuenan Li et al.[4] obtienen un hash robusto contra rotaciones utilizando una modificación del filtro de Gabor ofreciendo un buen balance entre robustez y discriminabilidad. Longjiang Yu et al.[9] proponen un método fuerte contra compresiones y escalados haciendo uso de la Transformada Discreta del Coseno para extraer el hash a partir de las bajas frecuencias de una imagen, es decir, quedándose con su estructura perceptual básica. Otros artículos como los de Jinglong Zuo [10], Monga Vishal [6] o Chen Brenden [2] presentan métodos robustos contra compresiones, escalados y rotaciones. También existen métodos capaces de detectar manipulaciones maliciosas, Ahmed Fawad [1] Sujoy Roy [7] y Han-ling Zhang [5], que podrían utilizarse para la detección de tampering. En esta línea, Farid [3] analiza cambios de compresión en las imágenes

para detectar artefactos propios de regiones manipuladas. Así mismo, existen métodos más específicos que resuelven problemas concretos como el de Senel Kamil [8] aplicado al reconocimiento de caras para la autenticación biométrica mediante la extracción de hashes robustos de rostros.

Como se puede observar, no existe un hash perceptual que resuelva a la perfección todos los tipos de modificaciones que puede tener una imagen. Unos hashes son buenos contra unos tipos de ataques como escalados y compresiones mientras que otros obtienen buenos resultados contra rotaciones y manipulaciones u otro tipo de modificaciones.

El proyecto ASASEC necesita una solución robusta contra todos los tipos de ataques y manipulaciones que sufren habitualmente las imágenes con contenido pornográfico infantil. La Universidad de León se ha volcado en esta tarea ardua y compleja buscando mejorar y combinar varios métodos existentes, con el fin de suplir sus carencias y adaptarlos a la solución requerida.

Conclusiones

Los métodos de hashing criptográficos utilizados hoy en día en la catalogación de imágenes no son adecuados para efectuar la *búsqueda por similitud* requerida en bases de imágenes de pornografía infantil. Por este motivo, la Universidad de León propone el uso de hashes perceptuales. Este tipo de hashes, se basan en el contenido o en la estructura perceptual de una imagen desde el punto de vista de un observador humano, en lugar de generarse a partir de la estructura binaria de la imagen. Sin embargo, existen muchas técnicas diferentes para generar hashes perceptuales, cada una con sus ventajas y limitaciones, por lo que es necesario desarrollar nuevas soluciones que se ajusten al problema concreto. La Universidad de León está activamente trabajando en la búsqueda de estas soluciones en el marco del proyecto europeo ASASEC y en colaboración con multitud de entidades de carácter público y privado.

Una vez se desarrollen estas técnicas de hashing de propósito general, no se limitarán a las necesidades exclusivas de este proyecto, si no que podrán ser utilizadas en diferentes ámbitos como la protección de autoría de contenido en portales de vídeos como YouTube o la búsqueda de imágenes por contenido en gestores de imágenes.

Referencias

[1] F. Ahmed and M.Y. Siyal. A secure and robust hashing scheme for image authentication. In Information, Communications and Signal Processing, 2005 Fifth International Conference on, pages 705 –709, 0-0 2005.

[2] B. Chen and V. Chandran. Robust image hashing using higher order spectral features. In Digital Image Computing: Techniques and Applications (DICTA), 2010 International Conference on, pages 100 –104, dec. 2010.

H. Farid. Exposing digital forgeries from jpeg ghosts. Information Forensics and Security, IEEE Transactions on, 4(1):154 –160, march 2009.

[4] Yuenan Li, Zheming Lu, Ce Zhu, and Xi- amu Niu. Robust image hashing based on random gabor filtering and dithered lattice vector quantization. Image Processing, IEEE Transactions on, 21(4):1963 –1980, april 2012.

[5] Han ling Zhang, Cai qiong Xiong, and Guang zhi Geng. Content based image hashing robust to geometric transformations. In Electronic Commerce and Security,

2009. ISECS ’09. Second International Symposium on, volume 2, pages 105 –108, may 2009.

[6] V. Monga and M.K. Mhcak. Robust and secure image hashing via non-negative matrix factorizations. Information Forensics and Security, IEEE Transactions on, 2(3):376 –390, sept. 2007.

[7] Sujoy Roy and Qibin Sun. Robust hash for detecting and localizing image tampering. In Image Processing, 2007. ICIP 2007. IEEE International Conference on, volume 6, pages VI –117 –VI –120, 16 2007-oct. 19 2007.

[8] K. Senel, M.K. Mihç andak, and V. Monga. A learning framework for robust hashing of face images. In Image Processing (ICIP), 2010 17th IEEE International Conference on, pages 197 –200, sept. 2010.

[9] Longjiang Yu and Shenghe Sun. Image robust hashing based on dct sign. In Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP ’06. International Conference on, pages 131 –134, dec. 2006.

[10] Jinglong Zuo and Delong Cui. Retrieval oriented robust image hashing. In Industrial Mechatronics and Automation, 2009. ICIMA 2009. International Conference on, pages 379 –381, may 2009.