Marcas de Agua

El Propietario de Derechos de Autor de un documento digital necesita, para obtener una justa remuneración por la información que produce, de medios técnicos adecuados que permitan la autenticación de dicha información (esto también es exigido por el usuario que disfruta de la misma), así como el seguimiento de copias ilegalmente distribuidas.

El uso de marcas de agua ("watermarks") como sistema de protección es casi tan antiguo como la fabricación de papel. Durante cientos de años, cualquiera que poseyera o fabricase un documento u obra de arte valioso/a lo marcaba con un sello de identificación o marca de agua (visible o no), no sólo para establecer su propiedad, origen o autenticidad, sino para desalentar a aquellos que pudieran intentar robarlo.

La posibilidad de digitalización de cualquier tipo de información (imágenes, vídeo, audio, texto, etc.) junto a la interconectividad global permite realizar copias perfectas de la información digitalizada.

Los procesos criptográficos permiten proteger la adquisición legal de la información, pero una vez obtenida la información se puede revender copias exactas. Por lo tanto, surge la necesidad de un sistema de seguimiento de las copias para la protección de los Derechos de Autor, que también se utilice en el caso de adquisición legal para distribución fraudulenta (copias ilegales).

La no disponibilidad de dichos sistemas ha frenado (y sigue frenando) la implantación de servicios multimedia donde la información "tiene un precio".

Las propias características de la información digital (facilidad de éplica, facilidad de transmisión y uso múltiple, facilidad de tratamiento y modificación,

equivalencia de las copias digitales, etc.) facilitan la agresión contra los Derechos de Autor del propietario de dicha información, lo que hace necesaria la existencia de un sistema de protección potente.

Por todo esto se ha expandido el concepto de marcas de aguas al mundo digital, incluyendo impresiones digitales inmateriales utilizadas para autentificar la propiedad de una información digital y servir en la defensa de los intereses de dicha propiedad.

Las técnicas de marcas de agua son utilizadas para la autenticación (tanto del distribuidor o propietario legal, como de que el original no ha sido falsificado) de la información, así como para el seguimiento de copias, ya que permiten la identificación del autor, propietario, distribuidor y/o consumidor autorizado de un documento digital.

Esta técnica de protección requiere básicamente dos herramientas:

* Introducción de la firma o marca en la información a proteger.

* Extracción e identificación de la marca.

Una marca de agua es un código de identificación, perceptible (visible y/o audible) o preferiblemente imperceptible, que se encuentra permanentemente "incrustado" en la información (no desaparece después del descifrado) y que puede contener información acerca del propietario, de los derechos de autor, el creador, el usuario autorizado, el número de copias o reproducciones autorizadas, el terminal autorizado, etc.

El desarrollo de un sistema de marcas de aguas digitales requiere la particularización a un tipo de señal determinado (imagen, audio, etc.), pues el diseño de un sistema de estas características logra mucho mejores resultados si se realiza en función de la respuesta humana

al medio a percibir.

En orden de efectividad, una marca de agua debe ser robusta, no ambigua e imperceptible.

La robustez se refiere a que debe ser difícil de eliminar o de ser distorsionada hasta el punto de hacerse indetectable.

En particular, una marca de agua debe ser robusta frente a: Análisis estadísticos como, por ejemplo, un filtro de Kalman (para imágenes), procesamientos comunes de la señal, como por ejemplo conversiones A/D, D/A, remuestreo, recuantificación, compresión, etc., distorsiones geométricas: rotación, traslación, recortes y cambios de escala (para imágenes); y colusión y falsificación, esto es, ante la combinación de copias de un mismo documento. La clave fundamental para hacer que una "marca de agua" sea robusta es introducirla en las componentes perceptiblemente más significativas de la señal o de su espectro.

La ambigüedad se refiere a que la probabilidad de un falso positivo en la detección de la marca ha de ser muy baja.

La imperceptibilidad dependerá del sentido receptor (vista, oído), y se referirá siempre a la comparación con la original (no se trata de medir la calidad).

La mayoría de los actuales sistemas de marcas de aguas digitales para imágenes se basan en introducir la marca en las componentes espectrales perceptiblemente significativas de una imagen, que son las bajas frecuencias. Ahora bien, la modificación de dichas componentes ha de ser lo suficientemente pequeña como para que no se pueda percibir a simple vista (característica de invisibilidad de la "marca de agua").

Lo mismo ocurre para señales de audio, si bien la respuesta perceptual sigue otros patrones.

La introducción de marcas de agua en documentos digitales se puede abordar también como un problema de comunicaciones digitales.

En paralelo con la creciente sofisticación en el modelado y explotación de las propiedades de los sistemas visual y auditivo humanos, se ha impulsado el desarrollo correspondiente en técnicas de comunicación de banda ancha.

Un sistema de marcas de agua estándar está compuesto por dos módulos principales, que realizan los procesos de codificación (o inserción) de la marca y decodificación (o extracción e identificación) de la misma.

El módulo codificador realiza la inserción de la marca de agua X en la información original 1 para crear la información marcada 1', que debe ser visualmente y/o auditivamente similar a 1.

Las técnicas de inserción existentes se pueden clasificar en dos grupos, en función del tipo de elemento de la imagen al que la marca de agua afecta de manera directa:

* Técnicas en el dominio del espacio: la marca modifica directamente el valor de luminancia y/o crominancia de los pixeles.

* Técnicas en el dominio de la frecuencia: la marca modifica directamente el valor de los coeficientes espectrales de la imagen.

La mayor parte de las técnicas desarrolladas en este dominio están inspiradas en métodos de codificación y compresión.

El módulo decodificador realiza en primer lugar la extracción de la marca X* de una información, cuyos derechos de propiedad se desean probar, I*, posiblemente manipulada o distorsionada, haciendo uso o no (esto depende de la técnica de extracción) de la información

original I.

A continuación establece el parecido entre la marca extraída X* y la marca original X, calculando el valor de un índice de similitud entre ambas.

Finalmente utiliza una función de comparación (e.g., un umbral T, un valor de relación señal a ruido) para determinar si la información test I* es una versión marcada de la información original I.

También las técnicas de decodificación de la marca de agua se pueden clasificar en dos grupos, según necesiten o no a la información original I para extraer la marca.

Los sistemas de marcas de aguas en que se utilizan la información original para la detección de la marca se denominan sistemas privados, en caso contrario reciben el nombre de sistemas públicos.

Para aplicaciones concretas puede resultar crucial el hecho de que la información original no esté directamente implicada en el proceso de detección.

Así, puede resultar interesante poder demostrar ante un tribunal que una determinada marca de agua está presente en una información sin mostrar públicamente el documento original.

Una vez que la marca de agua ha sido introducida en un documento digital, es susceptible de un amplio abanico de ataques que la distorsionarán, así como al documento en el que está inserta.

Según la causa y objetivo que los origina, éstos se pueden agrupar en ataques no intencionados e intencionados.

Los ataques no intencionados son aquellos a los que la marca de agua está sometida de manera casi inevitable.

Ejemplos claros son:

· El propio proceso de recuantificación del documento marcado antes de ser expedido.

· El ruido introducido por el canal de transmisión por el que se envía dicho documento marcado.

· Los ataques intencionados son las manipulaciones que realiza un pirata o "hacker" sobre el documento marcado con el fin de eliminar las protecciones de Derechos de Autor.

Los objetivos fundamentales son dos:

· **Manejar información libre de cualquier firma**. Estos ataques consisten en la manipulación del documento marcado con la finalidad de distorsionar la marca embebida en él, de forma que ésta se haga indetectable. Como se ha comentado, la marca de agua ha de ser más resistente que la información en sí, es decir, la degradación perceptible de dicha información ha de ocurrir antes de que el nivel de distorsión sufrido por la marca como consecuencia de las manipulaciones sea tal, que la marca deje de ser detectable. Algunos de estos procesos, como conversiones A/D, D/A, procesos de compresión, rotación, traslación, etc., podrían aparecer de igual modo como ataques no intencionados, pues pueden resultar necesarios para la transmisión o almacenamiento de la imagen o bien el usuario puede desear realizarlos, sin tener como objetivo la eliminación de los Derechos de Autor. Por lo tanto, una marca robusta es aquella que resiste a distorsiones como las descritas hasta ahora, sean o no intencionadas.

· **Poner su propia firma.** Estos ataques pueden dar lugar a confusión en la determinación de la propiedad de dichos derechos. El objetivo del agresor en este caso es introducir su firma en la imagen para reclamar que él es el propietario de la imagen original. Por lo tanto la robustez de una marca no es suficiente para garantizar una adecuada protección de los Derechos de Autor.

Las técnicas de marcas de agua actuales suelen resultar robustas frente a la mayoría de los ataques descritos hasta ahora. El verdadero "cuello de botella" de la robustez de las marcas de aguas son los ataques que dan lugar a una interpolación de la señal digital que representa la información. En el caso de imágenes estos ataques pueden realizarse mediante rotación, traslación de un número no entero de pixeles y cambios de escala.

Estudio realizado por el
Dr. José M. Martínez
Publicado en el Boletín del Criptonomicón Nº 64
Ingeniero de telecomunicaciones, del Grupo de
Tratamiento de Imágenes del Dpto de Señales
Sistemas y Radiocomunicaciones de la ETS
Ing. Telecomunicación de la Universidad
Politécnica de Madrid.