**Protección**
**Seguridad**

# Marcas de agua digitales. A vueltas con la protección de nuestros derechos

# Marcas de agua digitales. A vueltas con la protección de nuestros derechos

José Antonio Labodía Bonastre
*Director de Seguridad*
joseantonio.labodia@securitas.es
*(Todos los nombres comerciales están registrados por sus propietarios)*

A modo de continuación del artículo titulado: "Adobe Acrobat 3.01. Edición electrónica segura", que se publicó en el Manual formativo de ACTA Nº 16, y con el animo de tratar de informar a los autores de obras técnico-científicas y académicas de otras posibilidades de protección de sus derechos que brindan las modernas tecnologías informáticas, puesto que – cada vez más – la creación de sus obras, en un momento u otro, pasa por algún tipo de proceso informático, se ha confeccionado este artículo en el que se pretende informar de otras posibilidades de protección que ya se están utilizando en determinados programas y que tienen como misión fundamental la de garantizar la autoría de unos datos determinados.

El concepto de propiedad intelectual está claro: Una obra es de su autor, desde el mismo momento de su creación, y no puede ser manipulada por ninguna otra persona distinta de este. El autor, por su parte, sí puede realizar una cesión de derechos, pero la autoría de la obra sigue siendo suya.

Pero cuando se habla de proteger una obra que se encuentra en formato digital, y a pesar de lo que la Ley indica nos encontramos con una serie de problemas importantes.

Si pensamos en cómo proteger la información digital – la presente en un ordenador o la generada a través de cualquier proceso informático - automáticamente pensamos en la utilización de técnicas de cifrado y en los algoritmos que hacen posible su utilización. Pero realmente, las posibilidades de protección que brinda el cifrado, no sirven para proteger nuestros intereses como autores. Afortunadamente existen otras técnicas, como por ejemplo la esteganografía (en inglés *steganography*), que sí pueden sernos útiles.

Vamos a intentar conocer está técnica que puede ser de gran ayuda para la protección de los derechos de las obras generadas por los autores. Y la primera pregunta que surge es obvia: ¿Por qué existe y en que consiste la esteganografía?

La estenografía no nació con la intención de proteger el copyright, ni mucho menos. Su utilidad básica no es otra que la de proteger la información. Cuando se trata de proteger la información, esta se puede cifrar. El problema que se presenta es que es evidente que la información está cifrada – independientemente de la dificultad que presente el lograr su descifrado -. Si se quiere enviar esta información a determinados países en los que los derechos humanos se ven como algo inexistente, ponemos en peligro a nuestro interlocutor, que puede acabar en una prisión por el hecho de recibir esta información cifrada, aunque no se conozca su contenido. Esto es; el cifrado garantiza la confidencialidad e integri-

dad de la información remitida, pero no concede el anonimato, ni la discreción, que a veces es necesaria.

Esa es la utilidad real de la estenografía: Cifrar esta información y enviarla camuflada dentro de un archivo de otro tipo, como puede ser una imagen, un fichero de sonido o un texto. De esta forma, la información distribuida dentro de ese archivo pasará desapercibida para cualquiera que acceda al fichero soporte que contenga esa información. En el caso de que sospeche que esa imagen gráfica que se ha remitido oculte algo en su interior, no podrá acceder a la información introducida, dado que esta información a la que se pretende acceder puede estar cifrada.

En definitiva la función principal de la estenografía es ocultar una información dentro de otra totalmente diferente.

Bien, todo esto es muy interesante, pero ¿qué tiene que ver todo esto con la protección de nuestros derechos de autor?

Vayamos por partes.

## PROTECCIÓN DE LOS DERECHOS DE AUTOR

Si la estenografía permite el ocultar una información dentro de otra, ¿no se pueden utilizar estas técnicas para autentificar imágenes, sonidos, textos...? La respuesta es sí. De hecho ya se está realizando, y se denomina *watermarking* (marca de agua).

Fuera del mundo digital las marcas de agua se utilizan de forma similar y es bastante común su uso. Como ejemplo sirva la marca de agua del papel moneda – esa marca que se "*imprime*" por presión cuando se está fabricando el papel -, y que tiene como misión fundamental la autenticación del papel moneda ante cualquier duda que surja sobre su legitimidad.

La marca de agua digital admite la introducción de información referente al autor, fecha de creación, etc., permitiéndose de esta forma identificar y autenticar al verdadero autor. La marca de agua no impide la copia de un determinado fichero, pero si puede establecer, sin ninguna duda, quien es el autor. El cifrado puede impedir el acceso a una información determinada, pero una vez desprotegida esta información, el uso de técnicas de cifra no tiene ninguna utilidad.

En nuestro caso lo que deseamos es ejercer un control sobre las obras que hemos creado y que pueden encontrarse en cualquier tipo de soporte: gráficos, vídeo, texto, audio, etc. Para conseguir esta finalidad, así como la de controlar la existencia de copias – legitimas o no -, solamente podremos materializarla a través de la utilización de la estenografía y de las marcas de agua digitales, ya que la información existente en soporte digital es susceptible de ser copiada, modificada, tratada, distribuida – sin perdida de calidad - etc., por personas distintas de los autores o legítimos detentadores de los derechos pertinentes.

Antes de continuar hay que ser conscientes de que la estenografía es una técnica relativamente reciente, por lo que aún no se ha desarrollado completamente.

## MÁS SOBRE LAS MARCAS DE AGUA

Para conseguir su finalidad, las marcas de agua, desde la vertiente de la protección de los derechos de autor, deben existir – necesariamente - dos herramientas. La primera de ellas, debe poder permitir introducir y/o cifrar en el fichero la firma o la marca deseada. La segunda herramienta debe tener la posibilidad de extraer e identificar y/o descifrar la información introducida en los datos objeto de protección. Actualmente esto se consigue introduciendo la marca de agua digital en los canales espectrales significativos en el caso de las imágenes.

Para conseguirlo se utilizan:

- Técnicas en el dominio del espacio: La introducción de la marca de agua digital modifica directamente tanto los valores de luminancia como los de crominancia de los puntos (*pixel*) que componen la imagen digital.

- Técnicas en el dominio de la frecuencia: La introducción de la marca de agua modifica directamente el valor de los coeficientes espectrales de la imagen.

Estas dos técnicas se pueden resumir en la utilización de tintas invisibles, distorsión de caracteres, diferencias de escritura, nivel bajo de cambio de bits, etc.

Para que las marcas de agua cumplan con su función, deben presentar una serie de características:

- Deben ser robustas, entendiendo como tal la dificultad de que la marca de agua pueda ser totalmente eliminada o parcialmente distorsionada. La mejor forma de conseguir esta característica es hacer que la marca de agua sea lo más invisible posible, de forma que sea imperceptible frente a ataques estadísticos, procesamientos de señal (conversiones analógico/digital y viceversa), distorsiones geométricas, utilización de filtros, o cualquier otro tratamiento que tenga la finalidad de hacer desaparecer la marca.

- Deben ser ambiguas, es decir, la probabilidad de dar un falso positivo en la detección de la marca ha de ser muy baja, para que no parezca que existen datos acerca de la autoría, cuando esto no es así.

- Deben de ser imperceptibles en condiciones normales, mostrándose únicamente cuando sea necesario, no teniendo constancia de su existencia hasta ese momento.

Un ejemplo de las marcas de agua digitales seria el siguiente: Decidimos ocultar una información en un gráfico. Para ello utilizamos un programa que lo que hace es cambiar bits para que leyendo el nivel bajo de cada 8 bytes se obtenga un carácter, lo que permite ocultar la información deseada en un archivo de sonido o un gráfico. El hecho de ocultar esta información solo añade un pequeño bit de ruido que pasa totalmente desapercibido.

Dicho de otra forma: La marca de agua consiste en variar – levemente – el tono de los puntos (píxel) que componen la imagen, distribuyendo estos puntos que han cambiado de forma aleatoria por toda la imagen. Al no estar en ningún lugar en concreto, la marca de agua no se verá afectada cuando se aplican filtros, variaciones de color o cualquier otro tipo de tratamiento de imagen.

## UN CASO REAL

Imaginemos que estamos creando una imagen para ser colocada en una página Web, o para ser enviada a nuestro editor a través del correo electrónico, esto es, en formato digital para que sea utilizada en la confección de un articulo o de un libro. Así mismo, imaginemos que nuestro programa de dibujo (o de retoque fotográfico) es Adobe Photoshop 5.0. Creamos la imagen, la obtenemos a través de una tarjeta digitalizadora de vídeo, una cámara fotográfica digital o un escáner, y utilizamos este programa para mejorarla o retocarla de acuerdo con nuestros deseos.

Para añadir la información digital el programa utiliza la tecnología Digimarc PictureMarc, esto es la introducción de un código digital – que contiene los datos del creador - añadido como ruido a la imagen e inapreciable a simple vista. Este código permanece aunque en la imagen se inserten otras, se realicen conversiones de formato, o simplemente, se copien. En el ultimo caso, si se copia la imagen con una marca de agua, se copiara también la información asociada a esta.

*Tratamiento de imagen en Adobe Photoshop.*

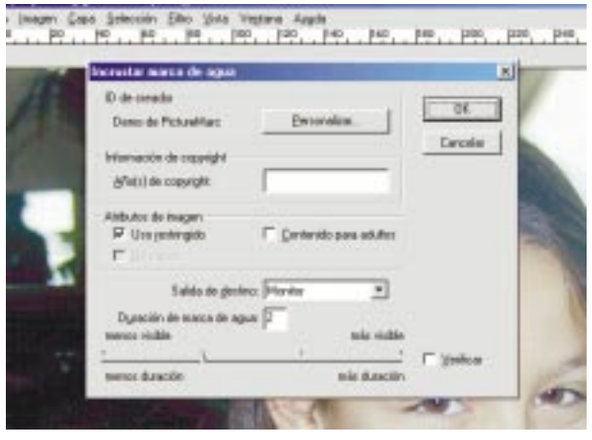
Una vez generada la imagen, y si queremos utilizar las posibilidades que se nos ofrecen para la inclusión de las marcas de agua digitales se debe tener en cuenta una serie de conceptos, que nos facilitaran su inclusión:

- Color: la imagen no puede estar formada por único color, aunque si puede utilizarse una imagen creada con gama de grises. Si alguien intenta transformar y copiar la imagen en formato monocromo (1 bits/canal) la marca de agua desaparece, pero cuando se vuelve a cambiar la imagen, por ejemplo a escala de grises (8 bits/canal), la marca de agua vuelve a aparecer.

- Dimensiones de los puntos (*píxel*): Las imágenes digitales están conformadas por puntos. Photoshop y su tecnología de marcas de agua (Digimarc) requiere tanto de un número, como de unas dimensiones mínimas de estos puntos, para que la marca de agua se incruste correctamente y prevalezca sin problemas aunque se trate la imagen. El

número mínimo de puntos – por defecto - es de 100x100.

- Compresión de archivos: Cuando se trabaja con imágenes es muy normal comprimirlos con algoritmos que presentan perdidas (Vg.: JPEG). Esto no afecta a la duración ni calidad de la marca de agua, aunque hay que tener en cuenta que habrá que escoger una mayor duración de la marca de agua para que esta prevalezca después de una compresión.

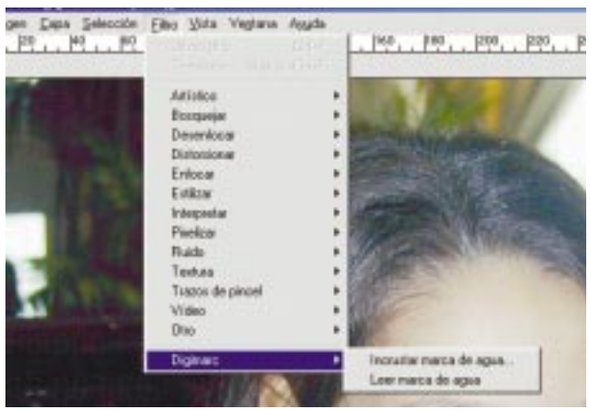



*Opciones de la marca de agua.*

## TRABAJANDO CON LA IMAGEN

La inclusión de la marca de agua digital debe ser la ultima operación realizada sobre la imagen que queramos enviar. Sobre la imagen hemos debido realizar todas las operaciones deseadas, hasta que esta haya quedado como teníamos previsto; redimensionamiento, correcciones de color, etc.

Para colocar la marca de agua primero es aconsejable grabar la imagen en el formato que deseemos y después ir al menú "Filtro" Digimarc.



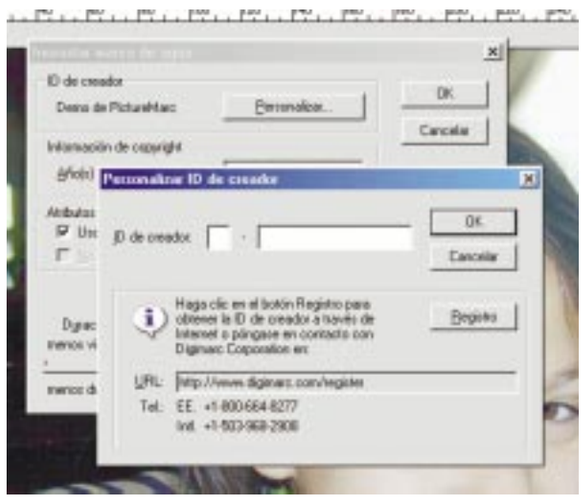

*Accediendo al menú de marca de agua.*

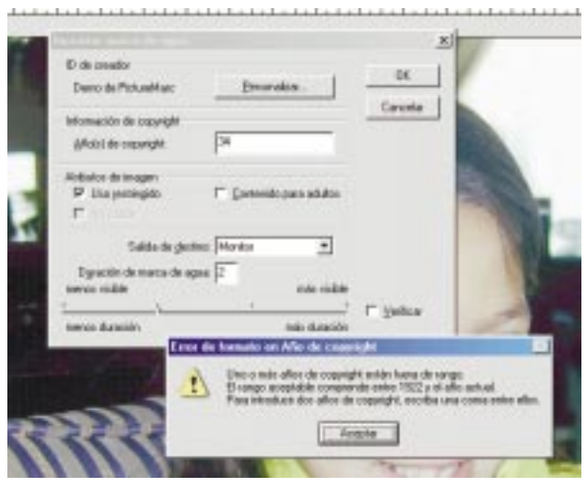
En el menú Digimarc aparecen dos opciones: "Incrustar" o "leer la marca de agua". Antes de continuar es necesario tener en cuenta que cuando pulsemos la primera opción se nos pedirá que incluyamos el ID de creador. Esto significa que previamente hemos debido acceder a la Web de Digimarc Corporation y darnos de alta en la base de autores de la misma.

Por defecto el programa únicamente admite la posibilidad de generar una Demo que permite hacerse una idea de cómo funcionan las marcas de agua.

Entre las opciones que se nos presentan en este cuadro nos encontramos con las siguientes:

"Personalizar". Si pulsamos en este botón automáticamente se abre otro cuadro de diálogo en el que se nos pide la ID del creador. Si no lo tenemos, otro botón (Registro) nos remitirá a Digimarc Corporation (http://www.digimarc.com/register) donde lo podremos solicitar. Esta información solamente se nos pedirá cuando utilicemos esta opción por primera vez.






*Campo de introducción de datos ID del autor y otras opciones: año copyright, atributos, densidad de la marca...*

La siguiente opción que tenemos es la de poner la "Información del copyriht", así como los "Atributos de la imagen" en los que podemos determinar si la imagen es de uso restringido (lo que limita la utilización de la misma), o si su contenido es para adultos.

A continuación debemos elegir la "Salida de destino", que puede ser monitor, Web o impresión (ya que si pretendemos imprimirla deberemos realizar previamente la separación de color), así como seleccionar la "Duración de la marca de agua" que oscila entre 1 (menos duración/menos visible) y 4 (más duración/más visible). Los valores de esta opción debemos elegirlos en función del formato y del uso final que se prevea para la imagen generada.

El grado 1 es poco visible en la imagen pero representa el problema de que su duración es más corta y puede presentar problemas en el caso de aplicar filtros o realizar algunas operaciones (edición, impresión o uso del escáner). El valor 4, en cambio, es más duradero, pero puede generar ruido en la imagen. Este valor es el aconsejable en el caso de imágenes en formato JPEG (comprimidas).

Una vez realizadas estas operaciones únicamente nos queda grabar la imagen de nuevo y comprobar como ha quedado la marca de agua.

Para ello volvemos al menú "Filtro", "Digimarc", "Leer marca de agua". En nuestro caso, al no tener ID, la información generada se corresponde con la Demo de la marca de agua. Si pulsamos en "OK" de nuevo saldremos a la imagen. Si pulsamos el botón "Mirar Web", se nos remitirá a la Web de Digimarc. Este cuadro puede presentar otras opciones, como la de comprobar, mediante una barra de color la idoneidad, o no, de la marca que hemos generado, en el caso de que dispongamos de un ID de autor.


*ID del autor (demo), atributos de la imagen y URL.*

Si accedemos a la página Web, nos encontramos con que nos ofrece información sobre la empresa, sus productos, protección de derechos, comercio electrónico, etc., aparte de menús tan populares en las páginas Web de los Estados Unidos, como pueden ser oportunidades de empleo, contacto con la empresa, noticias, etc.

Entre esta información aparece un cuadro que determina cuales son los precios por disponer de un ID, y que están determinados en función del número de imágenes amparadas por un ID concreto, y que se abonaran anualmente.

Desde el momento en que detentemos un ID en la base de datos de la empresa, las imágenes que generemos y en la que coloquemos la marca de agua, con el citado ID, estarán indisolublemente unidas a nosotros, como sus autores, o a la información que conste en la base de datos de Digimarc.

ANNUAL FEE (SUS) BASED ON NUMBER OF IMAGES WATERMARKED

| Level | Number of Images | Watermarking | MarcSpider |
|---|---|---|---|
| 1 | 1-99 | FREE | 49 |
| 2 | 100-999 | 99 | 99 |
| 3 | 1,000-4,999 | 399 | 149 |
| 4 | 5,000-9,999 | 699 | 249 |
| 5 | 10,000-24,999 | 1,499 | 499 |
| 6 | 25,000-49,999 | 2,499 | 799 |
| 7 | 50,000-99,999 | 3,999 | 1,199 |
| 8 | 100,000-249,999 | 7,499 | 1,499 |
| 9 | 250,000-499,999 | 12,499 | 1,999 |
| 10 | 500,000-999,999 | 19,999 | 2,999 |
| 11 | Over 1,000,000 | Customized | Customized |

*Tabla de precios de Digimarc Corporation.*

## PARA FINALIZAR CON ADOBE PHOTOSHOP

El programa de retoque fotográfico ofrece –además– otra posibilidad de adjuntar datos. Esta opción pensada para incluir una serie de datos extra que se han diseñado de acuerdo con un estándar generado por la Asociación de Periodistas de América y el Consejo Internacional de Comunicación de Prensa.

Estos datos se pueden incluir de dos formas:

En la primera posibilidad – y desde el entorno Windows – se pueden asociar estos datos a un archivo que no tenga un formato nativo de Adobe Photoshop. En este caso y desde la ventana de menús que aparece al pulsar sobre el menú "Archivo", surge una nueva opción denominada "Obtener información". Si pulsamos en ella aparece un cuadro de dialogo que nos permite introducir información en diferentes secciones: Pie de ilustración, Palabras clave, Categorías, Créditos, Origen, Copyright y URL. A continuación podemos incluir el texto que deseemos, el nombre del autor, el titular, o instrucciones especiales.

Si pulsamos el botón de "Guardar" aparecerá un cuadro de diálogo que nos solicitará el nombre con el que queremos guardar los datos que acabamos de generar. Estos datos se guardaran en un archivo FFO, pudiéndose crear tantos de estos archivos como secciones hayamos rellenado.

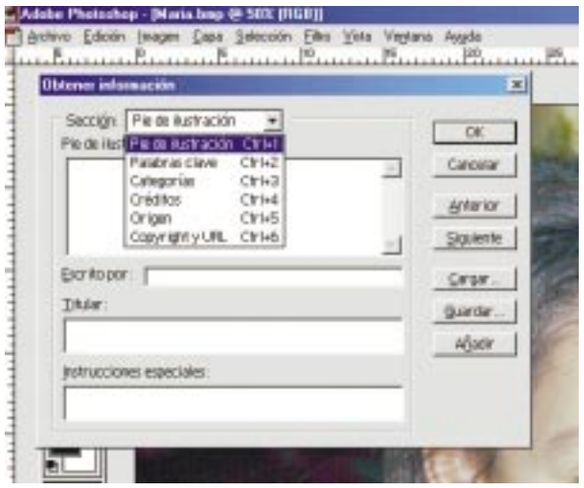
Si desde el Explorador de Windows pulsamos con el ratón sobre este archivo (*.FFO) automáticamente se lanzará Adobe Photoshop, aunque no aparecerá la imagen a la que está asociado. Para abrirla deberemos hacerlo desde el programa. Una vez la hayamos recuperado, pulsamos en "Archivo", "Obtener información", "Cargar" el fichero *.FFO, aparecerán los datos que en su momento incluimos en el mismo.

Los campos de Copyright y URL están interrelacionados con la marca de agua digital que generamos anteriormente, actualizándose automáticamente en función de los datos que tengan sobre el autor en la base de datos de Digimarc.

Pero ¿qué ocurre si borramos este fichero? Nada. Si se borra este fichero *.FFO, estos datos desaparecen. Esta opción – por lo tanto - carece de cualquier tipo de seguridad

La otra posibilidad que brinda el programa es la de guardar la imagen en un formato nativo de Adobe Photoshop (PSD, PPD, PDF, etc.). En este caso los datos se introducen de la forma anteriormente descrita para ficheros no nativos, con la salvedad de que no se genera un fichero FFO, si no que esta información queda incluida dentro del propio archivo gráfico, pudiéndose leerla al recuperarlo de nuevo con Adobe Photoshop.

Esta última posibilidad parece que dota a los datos de más seguridad que la primera que se ha visto, dado que esta información extra no está depositada en un archivo aparte. Pero siento decir que no es así. Basta leer el archivo gráfico con cualquier editor hexadecimal para localizar estos datos (que se almacenan en claro - de forma comprensible - al inicio del fichero) y borrarlos, sin que quede rastro alguno de su existencia. Posteriormente, el archivo se puede volver a editar sin ningún problema.




*Opciones de "Sección" dentro del menú "Obtener información".*

En cualquier caso, esta claro que la función de introducir estos datos, no es otra más que la de remitir una información extra junto con el archivo gráfico, que ayude a la colocación de la imagen en un texto determinado, por ejemplo, más que una medida que ofrezca seguridad.

A pesar de que a lo largo de estas líneas solamente se ha hablado de Digimarc Corporation, por ser la empresa que genera la marca de agua digital de Adobe Photoshop, existen otras compañías que ofrecen otras soluciones comparables, como el paquete WebSIte Totality de Auto F/X, que permite incluir – entre otras posibilidades - una contraseña propia y hasta 12 caracteres de texto que permanecen inalterables ante cualquier tratamiento que se de a la imagen protegida.

## OTRAS POSIBILIDADES (*CIRCUNSTANCIALES*) DE AUTENTICACIÓN

Pero además de la inclusión de una marca de agua digital, recogida en los párrafos anteriores, existen otras posibilidades de autenticar nuestros trabajos. Todo depende de lo que deseemos. Quizás deseemos solo autenticar el envío ante la persona que lo recibe, o bien tener un control de las copias que se generen.

En primer lugar nos encontramos con la opción de enviar nuestros trabajos en un archivo PDF (ver Manual Formativo de ACTA Nº 16 "Adobe Acrobat 3.01. Edición electrónica segura"), o simplemente firmados, esto es, unidos a un archivo SIG, a modo de firma electrónica. Este archivo permite únicamente – siempre que nuestro corresponsal tenga el programa de cifrado PGP (Manual Formativo de ACTA número 10) - comprobar nuestra firma, indicándole la validez (la no manipulación de los datos), o su invalidez, lo que demostraría que alguien ha manipulado el fichero que le remitimos. Lógicamente, esto no permite la protección de nuestros derechos de autor, puesto que este fichero SIG puede borrarse sin que se reciba ningún aviso de este hecho, y por lo tanto no protege el archivo.


*Comprobación positiva de un archivo gráfico JPG.*

Otra posibilidad que se nos presenta es la de utilizar un programa de esteganografía (por ejemplo S-Tools 4) que nos permite cifrar y ocultar mensajes en ficheros gráficos y de sonido, así como realizar una compresión mayor o menor de la información enviada. Como se puede comprender su finalidad principal es la de proteger y remitir información oculta, no proteger los derechos de autor.

Pero como solución "*de circunstancias*", puede utilizarse también para proteger el copyright. La idea es ocultar nuestros datos en el fichero que remitamos, cifrándolos con cualquiera de los algoritmos que admite el programa: IDEA, DES, Triple DES o MDC y protegerlos introduciendo una clave. Su utilización es muy sencilla, teniendo solamente que tener la prevención de guardar el fichero que contiene los datos cifrados (*hidden*) con el nombre del fichero gráfico o de sonido que deseemos proteger.

En el caso de que queramos confirmar la autoría de un grafico o fichero de sonido determinado, solamente deberemos arrastrar ese archivo a S-Tools, introducir la contraseña y el algoritmo que utilizamos para cifrar la información y automáticamente nos extraerá el fichero (la información que en su día ocultamos) donde le indiquemos.

Esta opción presenta las siguientes ventajas:

- Es gratuito.
- No aumenta demasiado el número de bits de la imagen (estamos hablando de datos mínimos: nombre del autor, fecha de creación, etc.)
- La información es prácticamente invisible.
- Los algoritmos de cifrado utilizados son bastante robustos.

Pero también presenta desventajas, algunas de ellas importantes:

- Para extraer la información oculta en el archivo, es necesario disponer – necesariamente - del programa que se ha utilizado para ocultarla.
- Solo trabaja con los formatos gráficos BMP y GIF, por lo que en el caso de que se transforme a otro formato, la información se pierde irremisiblemente, no pudiendo demostrar nuestra autoría. Si volvemos a pasar el archivo al formato BMP, S-Tools es incapaz de extraer la información.

La utilización de una aplicación de este tipo no ofrece la fortaleza suficiente como para ser utilizado con ninguna garantía. No hay que olvidar que su utilidad fundamental no es la protección del copyright.

Otra posibilidad, que no recomiendo a personas que no tengan profundos conocimientos informáticos, y que en realidad no tiene nada que ver con las marcas de agua digitales, consiste en que directamente – con un editor hexadecimal – escribamos los datos en el archivo que deseemos confirmar nuestra autoría. El riesgo que se corre es claro. El no poder abrir el archivo en el futuro, puesto que al escribir los datos directamente en el fichero lo hayamos dañado irremisiblemente. En este

caso, además, si se cambia el formato del fichero – y en función del lugar en el que los hayamos escrito – estos se perderán también.

Para finalizar, simplemente comentar que también existen programas estenográficos que permiten ocultar la información en ficheros de texto, de forma que esta información no sea visible al utilizar cualquier editor de texto. Para recuperar la información oculta, hará falta el programa que la ha ocultado.

## PARA SABER MÁS

PC ACTUAL: Marzo 2000. Artículo "La importancia del copyright", de Jorge Medina Beiro. En este articulo se somete a las marcas de agua de Adobe Photoshop a una serie de pruebas.

## ALGUNOS ENLACES DE INTERÉS

S-tools 4: Programa estenográfico.
http://linkbeat.com/files/s-tools4.zip

Sección de estenografía de Kriptopolis. http://www.kriptopolis.com/software/estego.html

Programas de esteganografía y su código fuente.
http://linkbeat.com/files/

Adobe.
http://www.adobe.es/products/acrobat/digsigs.html

Alakarga. http://www.geocities.com/Athens/Acropolis/6322/estega.doc

Digimarc. www.digimarc.com