Marcas de agua en el mundo real

Por Amalia Beatriz Orúe López

1. INTRODUCCIÓN

Las marcas de agua digitales han sido propuestas como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia, posibilitando la identificación de la fuente, autor, propietario, distribuidor o consumidor autorizado, de imágenes digitales, grabaciones de audio o video. La principal ventaja de estos sistemas consiste en que la marca es inseparable del contenido del archivo. Sin embargo, existen algunas cuestiones que necesitan ser resueltas, antes de que estas técnicas puedan ser eficazmente aplicadas en los escenarios de la vida real.

La marca de agua digital es un código de identificación que se inserta directamente en el contenido de un archivo multimedia (imagen, audio, video), de manera que sea difícil de apreciar por el sistema perceptual humano, pero fácil de detectar usando un algoritmo dado y una clave, en un ordenador. Es preciso aclarar que existen sistemas de marcas de agua visibles, los cuales no serán analizados en este trabajo.

Un sistema de marcas de agua involucra un proceso de marcado y otro de detección que, generalmente, requieren una clave de propósito similar a la clave utilizada en los sistemas criptográficos. El nivel de disponibilidad de la clave, determinará quién o quiénes podrán leer o detectar la marca de agua. En la práctica, la mayoría de las técnicas de marcas de agua pueden considerarse como sistemas criptográficos simétricos, en los que se emplea una sola clave, variando en ellos el nivel de acceso a esa clave.

Frecuentemente se utiliza el término marcas de agua de segunda generación para denominar a los sistemas que tienen en cuenta el comportamiento del sistema perceptual humano a la hora de incrustar la marca, de manera que la misma es incrustada con mayor amplitud (de forma más robusta) en aquellas zonas de los archivos en las que pasan desapercibidas, por ejemplo, las zonas de alta actividad de textura y bordes de las imágenes digitales.

En los últimos años se ha incrementado el interés de la comunidad científica, por el establecimiento de las definiciones preliminares de los requisitos de un sistema de marcas de agua eficaz, con vistas a su estandarización. Sin embargo, queda mucho por hacer antes de que pueda hablarse de la adopción definitiva de un estándar para algunas aplicaciones, en el caso de la música y el video se han experimentado diversas iniciativas con resultados positivos.

En este trabajo pretendemos analizar algunas particularidades de las técnicas de las marcas de agua que deben tenerse en cuenta a la hora de caracterizar los requisitos exigidos para cada aplicación particular.

2. PROPIEDADES EN LAS MARCAS DE AGUA

Existe un gran número de publicaciones en las que se discuten los requisitos que deben cumplir las marcas de agua ([COX97], [PIV98]). Es bueno destacar que la seguridad de estos sistemas no debe estar basada en la ocultación de los algoritmos utilizados, sino en la fortaleza de los mismos y en la seguridad de la clave.

Entre las propiedades deseables de un sistema de marcas de agua se encuentran la robustez, la resistencia a las manipulaciones, imperceptibilidad, el costo computacional y la baja probabilidad de error.

2.1 Robustez

Los archivos digitales de imágenes, audio y video, están expuestos a muchos tipos de modificaciones (o distorsiones): las pérdidas por compresión, los cambios producidos por el mejoramiento de imágenes, la amplificación de las señales de audio, etc. Una marca de agua se considera robusta si perdura después de esas operaciones y, en el caso de las marcas en imágenes y en video, también deben persistir después de las transformaciones geométricas (recortado, rotación, escalado). Esto quiere decir que la marca ha de estar presente en los archivos y que debe ser detectada después de las distorsiones ([EGG00], [BAR00]). Para consolidar su robustez, los sistemas de marcas de agua deben insertar la marca en las regiones perceptualmente significativas de los archivos multimedia ([COX97a]).

Existen diversas opiniones a la hora de definir la robustez de estos sistemas, nuestro punto de vista coincide con las formuladas en los trabajos de Jiri Fridrich ([FRI99]) entre otros, por tanto aclaramos que la valoración de esta propiedad de los sistemas de marcas de agua, no incluye los ataques basados en el conocimiento de los algoritmos de incrustado y detección de la marca, la robustez significa resistencia a ciegas frente a aquellas modificaciones producidas por las operaciones comunes a las que estarán expuestos los archivos multimedia.

La robustez no debe exigirse incondicionalmente, ya que un sistema de marcas de agua puede necesitar ser robusto respecto a determinados procesos y frágil respecto a otros. Si un sistema de marcas de agua requiere que ciertas modificaciones de los archivos dañen la marca se le denomina sistema de marcas de agua frágiles y es muy importante en determinadas aplicaciones como veremos más adelante.

2.2 Resistencia a manipulaciones

La resistencia a manipulaciones de un sistema de marcas de agua es un aspecto que puede relacionarse con la seguridad del mismo; se refiere a su resistencia frente a los ataques hostiles basados en el total conocimiento de los algoritmos de incrustado y detección y de los archivos marcados, excepto de la clave utilizada. Se incluyen aquí los ataques a los protocolos y los ataques basados en la estimación del sistema. Según la aplicación de que se trate,

unos ataques serán más importantes que otros; en general, un ataque efectivo deberá eliminar la marca de agua sin cambiar la calidad perceptual del archivo en cuestión; sin embargo, existen varias aplicaciones en las que la resistencia a determinadas manipulaciones es un aspecto indeseable. A continuación se revisan algunos de los ataques básicos a los sistemas de marcas de agua.

2.2.1 Ataques activos

Se trata de eliminar la marca o de hacerla indetectable, algo crítico para muchas aplicaciones incluyendo la identificación de propietarios, pruebas de propiedad, etc. En otro tipo de aplicaciones, como las de autenticación (cuyo objetivo es comprobar la integridad del archivo) el ataque activo consistiría en la restauración de una marca dañada por una manipulación no autorizada. Entre los ataques activos pueden catalogarse los siguientes:

- Ataques por promediación estadística que, en general, intentan estimar la marca y extraerla del archivo marcado.

- Ataques al detector de la marca, el intruso intentará por diversos medios deducir el comportamiento del detector, encontrando las posibles regiones donde se inserta la marca y tratando de eliminarla. Existen diversas versiones de este tipo de ataque.

- Ataques al dispositivo insertador de la marca, en un sistema donde el usuario tiene acceso a éste (aplicaciones de control de copias donde se requiere de un sistema de administración de la generación de las copias). Este puede hacerse, por ejemplo, en los sistemas de DVD donde el usuario tiene acceso a un disco original con una marca que permite una sola copia. Una vez que ésta se realiza, el dispositivo insertador incrustará una nueva marca que prohibirá efectuar más copias. El ataque necesita el acceso al archivo original (con la primera marca) y a su versión marcada (no más copias), con lo cuál se puede estudiar el comportamiento del insertador y crear un archivo diferencia restando el archivo original del marcado, de manera que podría predistorsionarse el archivo original con la finalidad de deshacer la adición de la nueva marca que haga el insertador.

- Ataque por Confabulación: Es otro tipo de ataque activo en el cual se utilizan varias copias de los datos marcados con diferentes marcas (dentro de un mismo sistema) para construir una copia que no contenga la marca ([KSU00]). La resistencia a estos ataques es crítica en las aplicaciones de marcas de agua transaccionales explicadas posteriormente ya que estos sistemas incrustan marcas diferentes sobre un mismo original del producto, cuando este va dirigido a varios destinatarios.

- Falsificación: Se trata de insertar una marca falsa que pueda ser reconocida como válida. Es un ataque crítico cuando utilizamos las marcas de agua para autenticar.

Es preciso aclarar que existe una gran variedad de ataques a los sistemas de marcas de agua que evidentemente no hemos mencionado aquí, un estudio detallado del estado del arte de los mismos puede encontrarse en [VOL01a].

Una herramienta de ataque a los sistemas de marcas de agua ([PET98]) y que ha servido como estándar de referencia para determinar su robustez, es el Stirmark; sin embargo, para obtener la evaluación completa de un sistema de marcas de agua, robustez y seguridad, deben aplicarse también otros estándares de comparación que tomen en cuenta el resto de ataques como, por ejemplo, los basados en la estimación ([VOL01b]).

La carencia de un estándar de referencia que evalúe y certifique oficialmente a los sistemas de marcas de agua, es uno de los problemas más importantes a resolver por la comunidad de científica dedicada al tema, recientemente los investigadores involucrados en el proyecto Europeo Certimark (CERTIfication for waterMARK) han dado a conocer una aplicación orientada a la evaluación de los software de marcas de agua denominada Checkmark, que incluye nuevas funcionalidades que no se habían tenido en cuenta en el Stirmark.

2.2.2 Ataques pasivos.

En este caso, el intruso no pretende eliminar la marca, su intención es detectarla solamente. En la mayoría de las aplicaciones este ataque no tiene mayor trascendencia, en todo caso, serviría como fuerza disuasoria frente a la intención de sustraer el material informático; en realidad es un ataque válido para la aplicación de las comunicaciones encubiertas, ya que su razón de existir se basa en ocultar la comunicación que se está efectuando.

2.3 Imperceptibilidad e indetectabilidad

La imperceptibilidad y la indetectabilidad de las marcas de agua son dos conceptos que tienden a confundirse frecuentemente, aunque son muy distintos y no están relacionados entre sí.

La imperceptibilidad o transparencia de la marca tiene como base el comportamiento del sistema perceptual humano. Una marca de agua es imperceptible (transparente), si la degradación que causa en los archivos donde se ha insertado es muy difícil de apreciar. Este concepto se contrapone al de la robustez, si tenemos en cuenta que un sistema robusto debe insertar la marca en las regiones perceptualmente significativas del archivo. En algunas aplicaciones se puede aceptar una pequeña degradación de los datos, a cambio de lograr mayor robustez o menor costo del sistema.

La indetectabilidad está relacionada con el modelo estadístico del archivo antes y después de ser marcado. Se dice que la marca es indetectable si después de haberla insertado, el archivo marcado conserva las mismas propiedades estadísticas que su original. Lo que quiere decir que una persona no autorizada no podrá detectar la presencia de la marca utilizando métodos estadísticos. Esta propiedad es muy deseable en el caso de las comunicaciones encubiertas en las que el principal objetivo es ocultar la presencia del mensaje incrustado en el archivo.

2.4 Viabilidad del sistema

Toda tecnología que pretende ser comercializada, debe tener en cuenta varios aspectos, entre ellos: el coste computacional, el coste económico y la escalabilidad del sistema. En muchos sistemas, tales como los de audio y video, la marca debe ser insertada y/o detectada en tiempo real, lo que requiere una gran capacidad computacional de los equipos.

En algunas aplicaciones el número de equipos que insertan la marca de agua difiere de la cantidad de detectores, lo que marcará la diferencia de precio entre unos y otros de acuerdo a la aplicación concreta.

Los requerimientos computacionales exigen a los sistemas de marcas de agua simplicidad, pero ésta puede significar la reducción de la resistencia a las manipulaciones. Sin embargo, hay que tener en cuenta que la velocidad de los ordenadores se dobla anualmente, de manera que un algoritmo que hoy no nos parezca razonable, podrá rápidamente convertirse en algo factible; es muy deseable diseñar sistemas de marcas de agua que sean escalables con cada generación de ordenadores.

2.5 Baja probabilidad de error

En la mayoría de los sistemas de marcas de agua es muy importante distinguir entre los archivos que contienen una marca y los que no.

La probabilidad de error al detectar una marca debe ser muy pequeña. Se denomina probabilidad de falso negativo a la probabilidad de que, habiendo estado presente una marca en determinado archivo, el detector asuma que no hay tal marca. Por otro lado, la probabilidad de falso positivo es la probabilidad de que no estando la marca presente en un archivo, el detector asuma que la marca está presente.

En algunas aplicaciones interesará minimizar la probabilidad de falsos positivos. Por ejemplo, en el caso de las restricciones de copias en los DVD, si un equipo de éstos detecta la existencia de una marca falsa no leerá la pista y le dará muy mala reputación a las firmas que lo comercializan.

Este requisito debe ser debidamente probado a priori, con independencia de la aplicación, si se quiere que el sistema pueda ser utilizado en disputas legales.

Cuando se habla de razón de falso positivo, se refiere a la relación entre el número de detecciones que pueden resultar falsos positivos y el número total de detecciones realizadas en un sistema dado. El consenso general sobre los detectores de marcas de agua para video DVD, ha determinado que la razón de falso positivo debe ser de 1 por cada 1012 imágenes.

2.6 Marcas de agua múltiples

Los discos de video DVD pueden contener una marca que indique la posibilidad de realizar una sola copia del mismo; una vez que esta copia se ha realizado es necesario alterar la marca para prohibir copias posteriores. En general, es recomendable insertar una segunda marca de manera que ambas sean igualmente detectables y no interfieran entre sí.

El hecho de que puedan coexistir múltiples marcas de agua facilita también el seguimiento de un archivo multimedia desde su punto de confección hasta sus distribuidores y compradores, pudiendo cada uno de ellos insertar su propia marca. En este escenario, el hecho de que las marcas insertadas no interfieran entre sí, significa que cada usuario autorizado podrá detectar su marca.

Un parámetro de especial interés a tener en cuenta aquí es la tasa de bits de la marca de agua (data payload), es decir, la cantidad de información que ésta contiene y se expresa en número de bits. Este parámetro brindará información acerca de cuántas marcas de agua distintas podrán insertarse en un archivo dado. En general, el diseño de sistemas de marcas de agua que permitan la inserción de múltiples marcas debe ser extremadamente cuidadoso para evitar los riesgos de un ataque por confabulación.

Como hemos explicado anteriormente, la mayoría de los sistemas de marcas de agua, involucran un compromiso entre la robustez deseada, la tasa de bits de la marca y la imperceptibilidad. Es evidente que estos requerimientos no pueden optimizarse al mismo tiempo, y que el tipo de compromiso entre ellos dependerá rigurosamente de la aplicación.

3. APLICACIONES DE LAS MARCAS DE AGUA

Los requisitos que deben cumplir en la práctica los algoritmos de marcas de agua deben analizarse dentro del entorno de trabajo del sistema y de acuerdo con la aplicación donde será utilizado, dicho esto consideraremos algunas de las posibles aplicaciones de las marcas de agua y sus peculiaridades.

3.1 Marcas de agua como Firmas

Las marcas pueden utilizarse para firmar archivos multimedia. El propietario de uno de estos archivos insertará una marca de agua que lo identifique como tal. Esta aplicación puede verse en los siguientes escenarios:

a) Identificación de propietario

La forma usual de informar sobre el derecho de propiedad, tanto en libros, fotografías o cualquier tipo de documentos, como en las cajas de CD de música y los créditos de las películas, es una nota de copyright colocada en forma visible. Evidentemente estas notas no garantizan la protección de tales materiales, baste sólo nombrar lo fácil que resulta borrar los créditos de una película, o tirar la envoltura de un CD de música. Como complemento de las notas de copyright puede insertarse una marca de agua que formará parte del contenido del producto; pongamos por ejemplo, la información del copyright insertada dentro de una imagen fotográfica.

La compañía DCT (Digital Copyright Technologies), brinda servicios en este campo, entre sus productos para insertar marcas de agua en imágenes se encuentra el everSign Workstation.

La corporación Digimarc ha comercializado un sistema de marcas de agua en imágenes con estos propósitos. Así, las marcas creadas dentro de la imagen llevan información acerca del autor o distribuidor de la misma. Muchos de los productos de compañías líderes en aplicaciones de edición y mejoramiento de imágenes como son Adobe, Cerious Software, Corel, Jasc Software y Micrografx, utilizan el software de Digimarc; los usuarios pueden marcar sus imágenes y detectar su propia marca teniendo la opción de registrarse en línea en la base de datos central de Digimarc, accediendo a su sitio web para identificarse como propietarios de la marca que han creado (pagando una cuota por ello). Cuando el detector de marcas de agua encuentra una imagen marcada, contacta con la base de datos para identificar al propietario de la misma y señaliza que dicha imagen contiene información acerca de su propietario.

b) Prueba de propiedad

Los propietarios de archivos multimedia pueden usar las marcas de agua no sólo para identificar su copyright sino también para probar la propiedad que ejercen sobre estos archivos.

Entre los software de marcas de agua desarrollados con el objetivo de identificación de propietario para diversos archivos multimedia se encuentran: EIKONAmark (imagen), AudioMark, y VideoMark de la corporación Alpha Tec.

3.2 Marcas de agua transaccionales (fingerprinting)

Las marcas de agua también pueden utilizarse para identificar a los compradores de los archivos multimedia, lo que puede servir para la búsqueda del infractor en el caso de distribución de copias ilegales de un archivo dado.

En este caso, la marca de agua transaccional se incrusta de manera adicional (o efectuando una nueva copia de los archivos originales) y llevará los datos del propietario y los datos del comprador. Además de usar la marca de agua (firma), para demostrar la propiedad de sus datos multimedia, el propietario podría determinar a quién atribuir la distribución ilegal de las copias que ha vendido.

Es interesante recalcar que dentro de los requisitos de esta aplicación, el sistema ha de tener capacidad y permiso para insertar varias marcas de agua en un mismo archivo.

Uno de los escenarios donde estas marcas de agua podrán jugar su papel es durante el rodaje de una película:

El resultado diario de las tomas de fotografía de una película se distribuye a todas las personas involucradas en su realización. Estas tomas tienen un carácter altamente confidencial y los originales de las mismas se guardan celosamente. En el caso de que se filtre la copia de una toma dada, los estudios cinematográficos necesitan identificar con prontitud al infractor; si cada copia distribuida contiene una marca que identifica a su poseedor, se descubre el culpable. En este entorno las marcas de agua, no necesitan ser totalmente imperceptibles ya que lo que se precisa es identificar a quién se le ha dado cada copia.

La vulnerabilidad de un sistema de este tipo a un posible ataque por confabulación debe estudiarse cuidadosamente y tenerse en cuenta en su diseño e implementación.

Con el objetivo de la identificación de propietario para diversos archivos multimedia en general y particularmente, para que los consumidores de tales archivos puedan acceder a un mercado legal de música digital, sin perjuicio para los derechos de las compañías discográficas, la corporación IBM ha presentado recientemente un sistema que utiliza diversas marcas de agua, entre otros métodos de protección, denominado EMMS (Electronic Media Management System). Este sistema cuenta con el apoyo mayoritario de la industria discográfica: propietarios de contenidos (EMC), proveedores de servicios (Sanity.com y Prisa), vendedores y distribuidores (MusicMaker, Supertracks, Amazon, CDNow), proveedores de sistemas de reproducción multimedia (LiquidAudio, RealNetworks, Reciprocal) y fabricantes de electrónica de consumo (Sony, Panasonic, Pioneer, AIWA, Sanyo y Sharp). Los propietarios de los archivos, por su parte, pueden predefinir las condiciones de uso de los mismos a lo largo de la cadena de distribución, asegurando la protección de sus derechos.

3.3 Marcas de agua para Autenticación

Existen muchas aplicaciones donde la veracidad de una imagen es crucial, tal es el caso de imágenes médicas y muchas otras. Las marcas utilizadas para la autenticación contendrán la información requerida que determinará la integridad de un archivo multimedia. La marca debe ser invisible y frágil (cualquier modificación de la imagen debe alterar la marca) y es muy deseable que pueda ofrecer información sobre los cambios ocurridos en las imágenes ([EGG01b]).

La corporación Mediasec ha comercializado varios productos que incrustan marcas de agua en archivos multimedia, entre los que se encuentran los

sistemas MediaSign y MediaLabel que realizan una marca de agua con el objetivo de la autenticación.

Supongamos otro escenario, una agencia de prensa que recibe imágenes capturadas por un reportero con una cámara digital; antes de usar las imágenes la agencia querrá tener la seguridad de que las mismas no han sido alteradas o editadas tras su captura.

Una de las primeras ideas aportadas para la creación de una cámara digital confiable fue Friedman ([FRI93]), su sistema añadiría una firma criptográfica asociada con la imagen captada, formando parte de los meta-datos localizados en la cabecera del formato de la misma, lo que supone el inconveniente de que dicha firma desaparece cuando la imagen se pasa a otro formato que no contenga este campo de cabecera.

Para resolver este problema y volviendo al ejemplo inicial, se incrusta durante la captura de la imagen una marca de agua invisible. Esta marca llevará información acerca del número de serie de la cámara digital, de manera que la agencia de prensa al detectarla determinará la veracidad de la imagen. Aquí, el uso de la marca posibilitará la detección de las manipulaciones ya que cualquier alteración aparecerá también en la marca.

Los laboratorios de investigación de IBM en Tokyo, asociados con Yasuda Fire & Marine Inc., han desarrollado el prototipo DataHiding que es un sistema seguro de transmisión e indexado de fotografías digitales desde la cámara digital al ordenador, cuyo propósito es verificar el origen y la integridad de las fotografías digitales.

Actualmente, se han propuesto varios sistemas que indican a groso modo la localización de los cambios realizados a la imagen y algunos de ellos admiten un mínimo de alteraciones o cambios en la misma, sin que se dañe la marca.

3.4 Monitorizado de las trasmisiones de radiodifusión

Al igual que en las firmas y las marcas transaccionales, las marcas de agua identificarán al propietario de los archivos multimedia y/o al comprador de una copia determinada de los mismos y serán detectadas por sistemas automatizados que rastrean las transmisiones de televisión y radiodifusión, las redes de ordenadores y otros canales de distribución para estar al tanto de cuándo y dónde se ha utilizado un archivo multimedia.

Muchas comunidades están interesadas en la monitorización de las transmisiones de radiodifusión, cada una de ellas con diferentes intereses. Por ejemplo, los músicos y actores cuyas obras son retransmitidas en diversas cadenas de radio y televisión, así como los agentes publicitarios, desean asegurarse que el tiempo en el que realmente están en el aire, sea el que han pagado. En este contexto, la marca de agua insertada en cada video clip debe ser irremplazable.

Existen varios sistemas comerciales que utilizan esta tecnología. La agrupación Worldtrax Media de Lucent, ha implementado el servicio MediaTrace que realiza el monitorizado de cualquier tipo de archivo multimedia; el sistema ConfirMedia de la corporación Verance trabaja con los archivos de audio; para archivos de video y televisión, se ha adoptado como estándar la tecnología VEIL II, de la corporación VEIL. La aplicación MarcSpider de Digimarc, es un servicio que rastrea las imágenes marcadas en la web, reportándole a sus propietarios el sitio donde fueron encontradas y el estatus legal de las mismas, otros software y servicios de la corporación Digimarc pueden encontrarse en Digimarc MediaCommerce.

3.5 Control de copias

Las marcas de agua diseñadas para el control de copias, contendrán la información determinada por su propietario, acerca de las reglas de uso y copiado de los archivos en los que se insertan. A diferencia de las marcas de agua transaccionales, así como las marcas de aguas usadas para el monitorizado, identificación y pruebas de propiedad, que sólo sirven como herramienta para investigar a los transgresores del sistema, las marcas de agua usadas en el control de copias restringen la utilización de los archivos de acuerdo a las regla de uso y copiado que porten.

Actualmente, esta aplicación está evolucionando continuamente. En los DVD de video, uno de los sistemas implantados fue el DIVX con características del tipo pago por visión; sin embargo, esta iniciativa ha sucumbido ante la inconformidad de la mayoría de sus consumidores potenciales.

Muchas compañías se han asociado en la búsqueda de métodos más apropiados para los DVD, las corporaciones Macrovision, Philips y Digimarc se agruparon en el llamado Millennium Group Watermarking, para desarrollar un sistema que combina un procedimiento de marcas de agua con un sistema de control de reproducción de pistas y autenticación, con vistas a la protección de los contenidos de video grabados en videocasetes, DVDs y de las transmisiones hechas por cable o satélite. También se incluía el diseño de módulos dentro del hardware de los ordenadores que garanticen esta protección.

Paralelamente el proyecto del Galaxy Group, congregó a las compañías IBM, NEC, Pioneer, Hitachi y Sony, proponiendo un sistema basado en cuatro estados, que indicaban el modo de protección: copia permitida, una sola copia, no más copias y prohibido copiar, especificados por dos marcas de agua, que no interfieren entre sí, denominadas marca de agua primaria y marca de copia, que se insertan en el contenido del video.

Actualmente ambos grupos se han unificado formando el Video Watermarking Group, quedando excluida la compañía IBM.

Un software disponible con posibilidades de efectuar el control de copias para archivos de audio es AudioKey Personal.

3.6 Comunicaciones secretas

En esta aplicación, la marca incrustada en los archivos multimedia se utiliza por dos o más personas para comunicarse secretamente sin levantar la sospecha de terceros. Es la aplicación clásica de la esteganografía (ocultar una información dentro de otra) de comunicación por canales subliminales. Existen varios software de dominio público que pueden utilizarse con estos fines entre ellos Steghide.

4. CONCLUSIONES

En este trabajo se ha hecho una revisión general de los conceptos básicos de las marcas de agua y sus aplicaciones en el mundo real. Se ha intentado presentar la panorámica actual acerca de los requerimientos de diferentes sistemas y su nivel de introducción en el mercado.

Hemos podido comprobar que cada aplicación requiere diferentes compromisos entre las propiedades de robustez, resistencia a manipulaciones, imperceptibilidad y probabilidad de error. Un único sistema de marcas de agua no es adecuado para todas las aplicaciones.

A pesar del esfuerzo de la comunidad científica y de la industria en desarrollar y establecer una tecnología de marcas de agua, hay que decir que desde el punto de vista científico y tecnológico existen numerosas incógnitas que están por resolver, muchos de los fundamentos teóricos utilizados no son totalmente concluyentes y la mayoría de los sistemas se diseñan de forma heurística. Otro inconveniente, es la carencia de un conjunto completo de normas para evaluar los sistemas de marcas de agua, lo que puede conducir a establecer como estándar, un sistema que falle de manera espectacular, desacreditando a toda la tecnología basada en ellos.

Para ofrecer en breve una mayor garantía de la tecnología de las marcas de agua, la evaluación y certificación de las técnicas de marcas de agua, es uno de los objetivos de la iniciativa Certimark, que pretende desarrollar un estándar de comparación adecuado, y entre sus resultados cuenta con el software ya disponible Checkmark, con lo cual se incentiva la competencia entre los proveedores de sistemas y el avance hacia mejores algoritmos de marcas de agua.

Por estas razones hay que mirar el futuro de estos sistemas con los pies en la tierra. Hoy por hoy las marcas de agua se presentan como una herramienta que puede ayudar a combatir y en todo caso a entorpecer, la proliferación de los delitos informáticos. Las aplicaciones relacionadas con la protección de los derechos de copyright, así como las pruebas de propiedad, tienen que evolucionar mucho para brindar los servicios que se esperan de ellas. En otras aplicaciones como las de la industria de los DVD y las aplicaciones de monitorizado y protección de copias de archivos de audio y video distribuidos por Internet, la utilización de las marcas de agua promete satisfacer todas las expectativas y lograr los resultados esperados a corto plazo.

Agradecimientos

Este trabajo ha sido posible gracias al financiamiento brindado por el Programa de estancias de Científicos y Tecnólogos Extranjeros en España del MEC.

A Dolores de la Guía, Gonzalo Álvarez y Berta Soriano, por su colaboración en la revisión del mismo.

REFERENCIAS

[BAR00] M. Barni, F. Bartolini, R. Caldelli, A. Piva, Geometric-Invariant Robust Watermarking through Constellation Matching in the Frequency Domain, Proceedings of 7th IEEE International Conference on Image Processing ICIP 2000, Vancouver, Canada, September 10-13, 2000, Vol. II, pp. 65 -68.

[COX97] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[EGG00] J.J. Eggers, J.K. Su and B. Girod, Robustness of a Blind Image Watermarking Scheme, International Conference on Image Processing (ICIP 2000), Vancouver, Canada, September 2000.

[EGG01a] J. J. Eggers, J. K. Su and B. Girod, Performance of a Practical Blind Watermarking Scheme, Electronic Imaging 2001, San Jose, CA, USA, January 2001.

[EGG01b] J. J. Eggers, and B. Girod, Blind Watermarking Applied to Image Authentication, submitted to ICASSP 2001, Salt Lake City, Utah, USA, May 7-11, 2001.

[FRI93] L. Friedman, The trustworthy digital camera: restoring credibility to the photographic image, IEEE Trans. On Consumer Electronics, vol.39, pp 905-910, November 1993.

[FRI99] J.Fridrich, M. Goljan, Comparing Robustness of Watermarking Techniques. Proc. of SPIE Vol. 3657 (Security and Watermarking of Multimedia Content), San Jose, Jan 25-27, 1999.

[KSU00] J.K. Su, J.J. Eggers, and B. Girod, Capacity of Digital Watermarks Subjected to an Optimal Collusion Attack, European Signal Processing Conference (EUSIPCO 2000), Tampere, Finland, September 2000

[PET98] F. A. P. Petitcolas, R. J. Anderson, M. Kuhn. Attacks on copyright marking systems. II Int. Workshop on Information Hiding, 1998.

[PIV98] A. Piva, M. Barni, F. Bartolini. Copyright protection of digital images by means of frequency domain watermarking. Mathematics of Data/Image Coding, Compression, and Encryption, Proceedings of SPIE Vol. 3456, pp. 25-35, 1998.

[VOL01a] S. Voloshynovskiy, S Pereira, T. Pun, JJ. Eggers and J. K. Su. Attacks on Digital Watermarks: Classification, Estimation-based attacks and Benchmarks submitted to IEEE Communication Magazin, 2001.

[VOL01b] S. Voloshynovskiy, S Pereira, V. Iquise, T. Pun. Towards a second generation watermarking benchmark Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.

Amalia Beatriz Orúe López, profesora de la Facultad de Ingeniería Eléctrica en la Universidad de Oriente de Santiago de Cuba.