



29 de octubre al 9 de noviembre de 2008

INSERCIÓN DE MARCAS DE AGUAS DIGITALES PARA PROTEGER LA PROPIEDAD INTELECTUAL DE LOS MATERIALES DIDÁCTICOS USADOS EN LA EDUCACION A DISTANCIA

Eje temático: Calidad y materiales Educativos y Herramientas Tecnológicas en Educación a Distancia

Autores: Lic. Maria Valeria Poliche - Mgter. Luis Arturo Segura
Facultad de Tecnología y Ciencias Aplicadas – Facultad de Humanidades
Universidad Nacional de Catamarca
Catamarca- Argentina
Maximio Victoria N°55
e-mail: vpoliche@hotmail.com; lsegu38@gmail.com

Resumen

Con el auge de las nuevas tecnologías de la información y comunicación (NTICs) hacen que áreas de conocimientos como la Educación a Distancia (ED) sean más aceptadas por la sociedad, convirtiéndose en uno de los pilares de la nueva sociedad del conocimiento. Dentro este contexto, los derechos de autor y la propiedad intelectual toman protagonismo, pues la enseñanza va a requerir del soporte indispensable de obras educativas protegidas por el derecho de autor y que se presentaran en formato multimedial o bien requerirán de su digitalización para que el alumno pueda acceder a ellas desde cualquier parte del mundo. Ante este riesgo se debe hacer uso de otros mecanismos que aseguren y protejan estos derechos fundamentalmente. El Watermarking o Marcas de Agua Digital es una herramienta que se aplica tanto en imágenes, videos, audio como a algunas formas de texto que nos permite poner de manifiesto el uso ilícito servicio digital por parte de un usuario no autorizado. Esto lo realiza colocando señales o patrones en imágenes para de esta manera poder identificar el origen, autor, propietario, derechos de uso, distribuidor o usuario autorizado de un documento digital, incluso si el mismo ha sido procesado y/o distorsionado. El presente trabajo pretende analizar y mostrar diferentes particularidades que debe tenerse en cuenta en la selección de las técnicas de las marcas de agua, las cuales deben estar estrechamente relacionadas con las propiedades deseables de un sistema de marcas de agua, haciendo hincapié en los mecanismos empleados para insertar marcas de agua digitales en texto como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia.



29 de octubre al 9 de noviembre de 2008

Palabras Claves: Marcas de Agua Digital (Watermarking), Propiedad Intelectual, Educación a Distancia, NTICs, Derecho de autor.



29 de octubre al 9 de noviembre de 2008

INSERCIÓN DE MARCAS DE AGUA DIGITALES PARA PROTEGER LA PROPIEDAD INTELECTUAL DE LOS MATERIALES DIDÁCTICOS USADOS EN LA EDUCACIÓN A DISTANCIA

INTRODUCCIÓN

La demanda de la Educación a Distancia está creciendo cada día más, el destinar tiempo para la familia y el trabajo impiden dedicarse completamente a estudiar o asistir presencialmente a las instituciones educativas, de esta manera emerge el concepto de la “Universidad Virtual” como una alternativa para romper esta barrera de tiempo y espacio y así posibilitar que el estudiante pueda cumplir con sus anhelos de estudiar. La Universidad Virtual concede al estudiante la oportunidad de contar con un Campus Virtual, entorno de aprendizaje que ofrece los espacios necesarios para que el estudiante interactúe con materiales, tutores, compañeros, etc., quienes intervienen en su formación. Es aquí donde nos planteamos los interrogantes si estos materiales que han sido confeccionados por profesores y son utilizados por los alumnos ¿pueden ser utilizadas por otros particulares a los fines que se estimen necesarios? y si ¿pertenecen a la institución de educación o al profesor que la confeccionó?.

Este problema está vinculado al reconocimiento del derecho de autor y la propiedad intelectual que con las nuevas tecnologías se ha puesto en peligro. Al hablar de Propiedad intelectual nos estamos refiriendo a cualquier material utilizado, así como todas las herramientas usadas en el proceso de aprendizaje a través de la Universidad Virtual. De igual manera el alumno, también, tiene el derecho propiedad intelectual sobre los trabajos que presente, evitando su difusión sin su previo consentimiento. Ante este riesgo, legislar resulta insuficiente, y por ello se debe hacer uso de otros mecanismos que aseguren y protejan estos derechos fundamentalmente. De este modo surgen técnicas conocidas como el Watermarking o Marcas de Agua. El objetivo de una Watermarking consiste en colocar “marcas” que permanezcan invisibles al ojo humano o que si resultan detectadas sean imposibles de eliminar sin deteriorar la calidad del objeto que las contiene. Su función no es evitar que el archivo pueda ser modificado, sino dar información sobre si ha sido modificado o sobre quién es el autor o titular del derecho de autor de la obra.

LOS DERECHOS DE AUTOR Y LA PROPIEDAD INTELECTUAL EN LA EDUCACIÓN A DISTANCIA

Es necesario resaltar que en el mundo existen dos grandes líneas jurídicas sobre propiedad intelectual: el copyright y el derecho de autor. El primero, prevalece en la zona de influencia del derecho angloamericano; el segundo, en la del derecho latino.

El copyright está orientado a lo comercial, a la explotación de las obras intelectuales y por lo tanto pone el acento en derechos empresariales, mientras que el derecho de autor deviene de una concepción personalista. Para éste último, el derecho se origina en un acto de creación individual, y por ende, protege la obra para que permanezca en la esfera de la personalidad del autor.

El sistema latino, al incluir en la legislación de cada país disposiciones expresas, protege ambos tipos de derechos mientras que el derecho anglosajón se inclina por



29 de octubre al 9 de noviembre de 2008

defender los aspectos patrimoniales del derecho de autor. La adhesión generalizada al Convenio de Berna (1886, enmendado y revisado en varias ocasiones, la última en 1979) ha tendido a acercar algo ambos derechos, aunque países como EEUU no han modificado su legislación para que mencione en forma expresa el derecho moral de los autores. Por el contrario, han impulsado y logrado imponer a nivel mundial tratados como el Acuerdo de Marrakech (1994) que establece la Organización Mundial del Comercio, y sus cuatro anexos, uno de los cuales es el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio, ADPIC (en inglés TRIP's). En nuestro país esta norma generó, luego de su aprobación mediante la ley 24.425 del 5/01/95, serios conflictos de orden constitucional que no es el caso tratar aquí.

MARCAS DE AGUA O WATERMARKING

La marca de agua digital es un código de identificación que se inserta directamente en el contenido de un archivo multimedia (imagen, audio, video, texto), de manera que sea difícil de apreciar por el sistema perceptual humano, pero fácil de detectar por la computadora usando un algoritmo dado y una clave, en un ordenador. Dicho código es un grupo de bits que contiene información sobre el autor o propiedad intelectual del objeto digital tratado.

En los últimos años se ha incrementado el interés de la comunidad científica, por establecer los requisitos fundamentales que debe poseer, con vistas a su estandarización.

CARACTERÍSTICAS DE LAS MARCAS DE AGUA

A una marca de agua digital se le suele exigir una serie de requisitos para considerarlas adecuadas en la protección de derechos de propiedad intelectual:

- Indetectabilidad: las marcas de agua no se deberían poder detectar por un observador casual. Nadie debería apreciar una degradación en la calidad de la señal a consecuencia de la presencia de la marca de agua.
- Resistencia a manipulaciones: debería ser muy costoso eliminar la marca de agua del archivo. Esta resistencia se debe plasmar en las siguientes cualidades:
 1. Imposible de localizar: la marca debe ser simple, aunque podría estar aleatoriamente distribuida entre los datos. No debe existir forma fácil de identificar qué píxeles o partes de los datos contribuyen a la marca, de manera que no resulte sencillo eliminarla.
 2. Imposible de eliminar: la información de la marca no debería poder eliminarse sin degradar la calidad de la obra de forma significativa. Por ejemplo, muchas de las técnicas de espectro extendido embeben la información en grandes porciones de los datos. La destrucción de la información de la marca implicaría cambiar estas



29 de octubre al 9 de noviembre de 2008

- porciones significativas, que pueden degradar seriamente la calidad de la obra.
3. Imposible de mezclar: se podría montar un ataque sencillo si se dispusiera de más de una copia de la imagen. Si existen dos copias con marcas distintas, entonces sería posible bien promediar ambas o bien entremezclarlas de manera que los bits de marca de ambas copias se destruyan. Muchas de las técnicas de espectro extendido pueden evitar este ataque y revelan a menudo las marcas de las dos copias, de forma que ambas fuentes pueden ser identificadas.
 4. Resistente a errores: algunas señales podrían alterarse ligeramente debido a errores o perturbaciones en el canal de transmisión y muchas más son alteradas por sistemas de compresión como JPEG (imágenes), MP3 (música) o MPEG (vídeo). Un buen sistema de marcas de agua conservará los datos incluso después de que la imagen haya sido comprimida y reconstruida.
 5. Segmentable: tanto las señales visuales como audio pueden ser cortadas o segmentadas. Un buen esquema de marcas de agua será capaz de reproducir los datos aun después de haber sido fragmentada la información.
 6. Resistente a la distorsión: las señales de vídeo y de audio pueden ser distorsionados por motivos estéticos. Los ingenieros de sonido podrían añadir cualidades como la reverberación. Las imágenes visuales podrían ser distorsionadas en el proceso por alguna transformación afín. También se podrían cambiar los datos debido a ciertas técnicas de mezclado y corrección de colores. Operaciones geométricas como la rotación, traslación y cambio de escala tampoco deberían afectar a la marca. Un esquema de marcas excelente sería capaz de resistir estos procesos.
 7. Universalidad: el mismo esquema de marcas de agua debería ser aplicable a los tres medios básicos (música, vídeo e imágenes) para la protección económica de productos multimedia, puesto que se podría utilizar un único hardware común para los algoritmos de marcas de agua.
 8. No ambigüedad: la recuperación de la marca de agua no debería ofrecer ninguna duda respecto a la identidad del autor y/o propietario. Más aún, la posibilidad de identificar al autor debería mantenerse incluso ante ataques.

Ninguno de los esquemas de marcado que se han creado hasta la fecha posee todas las características anteriores, aunque la mayoría satisfacen varios de los requisitos, al menos siempre uno. Normalmente, el compromiso se presenta entre producir marcas que sean muy resistentes y marcas que sean indetectables, ya que ambos requisitos entran en conflicto, pues cuanto más resistente sea la marca, más evidente se hará su presencia y cuanto mayor sea su invisibilidad, más sencillo será eliminarla, accidentalmente o no. En la práctica se le exige que una marca de agua digital o watermarking sea:



29 de octubre al 9 de noviembre de 2008

1. Ambigüedad
2. Robustez
3. Imperceptibilidad.

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

GENERACIÓN Y DETECCIÓN DE UNA MARCA DE AGUA DIGITAL

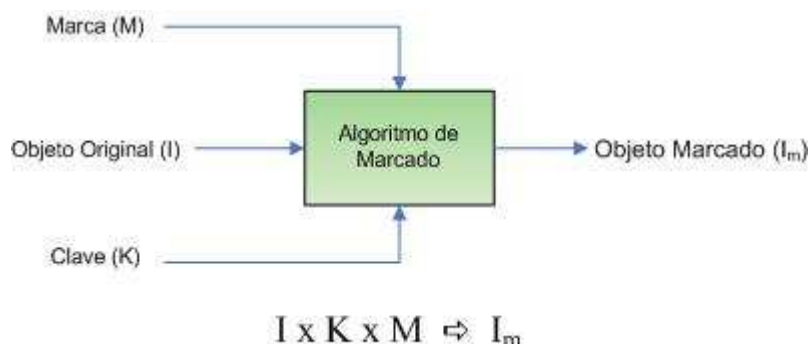
Un sistema de marcas de agua estándar está compuesto por dos módulos principales, que realizan los procesos de codificación (o inserción) de la marca y decodificación (o extracción e identificación) de la misma. El módulo codificador realiza la inserción de la marca de agua X en la información original I para crear la información marcada I' , que debe ser visualmente y/o auditivamente similar a I . La introducción de una marca de agua suele requerir tres tipos de informaciones:

- I : La información que albergará la marca de agua (imagen, sonido, texto, etc.)
- W : La marca de agua.
- K : La clave.

Mientras que la información de la que desea comprobarse si contiene la marca se denominará I'

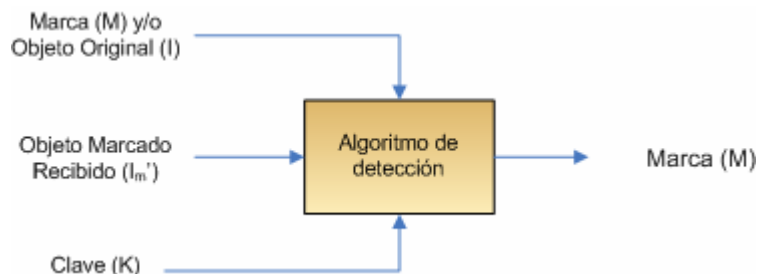
Un sistema de marcas de agua involucra un proceso de marcado y otro de detección que, generalmente, requieren una clave de propósito similar a la clave utilizada en los sistemas criptográficos. El nivel de disponibilidad de la clave, determinará quién o quiénes podrán leer o detectar la marca de agua.

El diagrama de generación de un objeto marcado será el siguiente



29 de octubre al 9 de noviembre de 2008

Asimismo, el proceso inverso, para saber si un objeto está marcado o no, y por lo tanto obtener la información almacenada en dicha marca será:



TIPOS DE MARCAS DE AGUA DIGITALES

Por esto una marca de agua se puede definir según los siguientes requisitos:

- Deber ser invisible a la percepción del ojo humano y no debe afectar a la calidad de la imagen.
- La marca recuperada debe identificar de forma unívoca al propietario de la misma.
- No debe ser detectada mediante pruebas estadísticas.
- Debe ser difícil, tanto que sea imposible, de eliminar excepto por el propietario.
- La marca debe ser robusta a los diferentes algoritmos de procesado de imagen

como pueden ser filtros, compresiones, etc.

A medida que se ha ido avanzando en la investigación sobre Watermarking se han ido descubriendo nuevas técnicas y métodos por los que se han definido distintas clases de marcas de agua, estas son:

- Marcas visibles frágiles.
- Marcas visibles robustas.
- Marcas invisibles frágiles.
- Marcas invisibles robustas.

Marcas visibles frágiles

Las características que deben cumplir este tipo de marcas son:

- Que sea fácilmente visible.
- Discreta.
- Difícil de eliminar.
- Insertada automáticamente a lotes de imágenes diferentes.

A pesar de la sencillez relativa para conseguir los tres primeros requisitos, el cuarto es mucho más complejo, ya que la misma marca se puede aplicar a distintas imágenes muy diferentes, pero esto puede provocar que en unas imágenes ésta sea claramente visible y en otras no llegue a verse.

II. Marcas visibles robustas

Este tipo de marcas tiene mucho menor interés ya que afectan a la calidad de la imagen y pueden considerarse como logotipos. Por ello no vamos a hablar de ellas.



29 de octubre al 9 de noviembre de 2008

III. Marcas invisibles frágiles

Los requisitos de éstas son:

- Invisible para el humano.
- Alterada en cuanto se aplican las técnicas más comunes de procesado de imagen.
- No puede ser insertada por personas no autorizadas.
- Debe poder ser extraída de forma rápida por las personas autorizadas.
- Debe permanecer aunque se recorte la imagen.
- La marca extraída debe indicar dónde se han producido las alteraciones.

Uno de los puntos más complejos es determinar si la marca es estrictamente invisible, ya que en muchos casos esta invisibilidad dependerá del visualizador, de la imagen y de cómo es presentada. Para ayudar en la creación de la marca se emplean diversos tests que parten de imágenes preparadas en las que la marca tiene más posibilidades de ser visibles. El tercer requisito pretende evitar que se extraiga una marca de una imagen y se inserte en otra. Para ello debe cumplirse que es extremadamente difícil para terceros determinar si la imagen está marcada o no. Una de las propuestas más aceptadas es la utilización de las claves para realizar el proceso de extracción, de forma que éstas se almacenan de forma separada en una base de datos segura.

El quinto requisito es deseable en alguna aplicación en las que las imágenes son recortadas, y sin embargo puede no ser tan importante en aplicaciones que no ofrezcan esta opción. En cualquier caso es interesante que el proceso de extracción de la marca permita detectar si se han producido recortes o no.

IV. Marcas invisibles robustas

Para este tipo de marcas las características de las mismas son:

- Ser invisible para la percepción humana.
- Permanecer en la imagen marcada incluso si se realizan sobre ella operaciones de procesado.
- Difícil de detectar por personas no autorizadas.
- Debe poder ser extraída rápidamente por personas autorizadas.
- Debe permanecer en la imagen y debe ser extraíble tras su impresión y posterior escaneado.

Diseñar métodos de marcado para cumplir el tercer y el quinto requisito es una tarea ardua y costosa a la par que compleja, ya que la forma de crear marcas muy robustas es analizar todos los posibles ataques. Debido a esto se definen unos requisitos para que la marca sea resistente a las técnicas de procesado de imagen comunes como son edición, visualización, impresión o transmisión. Algunas son las siguientes:

- Recortes.
- Modificaciones de brillo y contraste.
- Operaciones de reducción, alargamiento y rotación.
- Compresión con pérdidas como es el caso del formato JPEG mencionado con anterioridad.



29 de octubre al 9 de noviembre de 2008

- Adición de ruido correlado o no, esto es un ataque intencionado.

Para la extracción de la información contenida en la marca (M) o para conocer si un objeto está marcado o no con una información concreta, necesitaremos unos datos u otros. En función de dichos datos y de lo que queramos obtener, tendremos diversos tipos de watermarking:

- **Marca Privada:** se necesita tener el objeto original (I)

- Tipo I: $I'_m \times I \times K \Rightarrow M$

- Tipo II: $I'_m \times I \times K \times M \Rightarrow \text{Marcado/NoMarcado}$

- **Marca Semiprivada:** se necesita tener la marca (M)

$$I'_m \times K \times M \Rightarrow \text{Marcado/NoMarcado}$$

- **Marca Pública:** no necesita ni de el objeto original (I) ni la marca (M)

$$I'_m \times K \Rightarrow M$$

- **Marca Visible:** en estos casos, la marca de agua es visible y deteriora el objeto digital, mediante la clave (K) podemos obtener la el objeto original sin pérdidas debido a la marca.

$$I'_m \times K \Rightarrow I$$

TÉCNICAS

Existen mecanismos o técnicas que han sido propuestas como una solución eficiente para la protección de los derechos de copia y propiedad de los archivos de datos multimedia. Estas tienen como objetivo principal poner en manifiesto el uso ilícito de un cierto servicio digital por parte de un usuario no autorizado. Su función no es evitar que el archivo pueda ser modificado, sino dar información sobre si ha sido modificado o sobre quién es el autor o titular del derecho de autor de la obra. Aunque no impide que el archivo sea modificado, eso no significa que se pueda eliminar esta marca, entre otras cosas, porque permanece oculta al usuario. La principal ventaja de estos sistemas consiste en que la marca es inseparable del contenido del archivo.

En este trabajo se pretende 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.

El watermarking se aplica tanto a imágenes, video, audio, como a algunas formas de texto, es decir en casi todos los formatos de archivos empleados en la actualidad, obviamente con técnicas diferentes para cada caso, pero con un objetivo en común.

Imágenes

La utilización de una técnica u otra para marcar una imagen dependerá en gran medida del uso que se vaya a hacer de la misma. Por lo tanto, para aceptar como



29 de octubre al 9 de noviembre de 2008

válido un método de marcado deberemos conocer previamente la finalidad del mismo. Algunos autores han realizado varias propuestas en este sentido, extendiendo el uso de las marcas de agua a otros escenarios además del clásico de protección de los derechos de autor.

De forma resumida los escenarios propuestos son los siguientes:

- Modificación del bit de menor peso (LSB: less significant bit) de algunos pixels de la imagen, elegidos mediante una secuencia pseudo-aleatoria (S. Walton). Al tratarse del bit de menor peso de un píxel, éste se ve sometido a un cambio imperceptible de color.
- Modificación de los coeficientes de la DCT (Discrete Cosinus Transformation o Transformada Discreta Coseno)
- Ensanchamiento del espectro frecuencial.

Audio

De la misma forma que en el caso de imágenes, es importante saber si la imagen se distribuye en papel y posteriormente se escanea o si procede directamente de soporte electrónico, en el caso de señales de audio hay que tener presente qué camino ha seguido desde su generación al destinatario. La señal puede transmitirse digitalmente o analógicamente, propagarse por un cable o por el aire, etc. Las características de la señal más robustas a la transmisión, y por tanto más adecuadas para el marcado, dependerán de las condiciones en que se ha ya transmitido la señal. Análogamente al caso de imagen, la cantidad de información que se podrá ocultar será tanto mayor cuanto mayor sea la velocidad de transferencia (mayor frecuencia de muestreo y /o mayor número de bits por muestra) En general, la transferencia de información oculta que se puede conseguir está comprendida entre 2 y 128 bits por segundo. Algunos de los métodos posibles para ocultar información en señales de audio son:

- Modificación del bit de menor peso de algunas muestras del archivo de sonido, elegidos mediante una secuencia pseudo-aleatoria.
- Ensanchamiento del espectro frecuencial.
- Ocultación de eco.

Texto

Si el texto está impreso y escaneado se trata de una imagen, por lo que es posible aplicar algunas de las técnicas que se aplican en imagen. Además, se pueden aprovechar las características particulares de este tipo de imagen para introducir información variando ligeramente la forma de las letras, distancias entre letras, posición de las líneas, etc. Sin embargo, usualmente los textos se distribuyen en formato electrónico (por ejemplo mediante ficheros ASCII, html, etc.) En este caso, la ocultación de información es ostensiblemente más difícil, dado que la redundancia presente es mucho menor, y una pequeña variación se detecta rápidamente. Existen tres grandes grupos de técnicas para ocultar información en textos:

- Modificación del espaciado entre líneas En este caso, las líneas de texto de un documento son desplazadas imperceptiblemente hacia arriba o hacia abajo.



29 de octubre al 9 de noviembre de 2008

E	s		e	l		v	o		q	u	e		e	l			
a	l		m	a		p	r	o	n	u	n	c	i	a		y	
q	u	e		t	o	d	o	s		s	a	b	r	e	m	o	s
c	u	m	p	l	i	r	.										

E	s		e	l		v	o		q	u	e		e	l					
a	l		m	a		p	r	o	n	u	n	c	i	a		y			
q	u	e		t	o	d	o	s		s	a	b	r	e	m	o	s		
c	u	m	p	l	i	r	.												

- Modificación del espaciado entre palabras: Aquí es alterado el espaciado entre palabras en una línea de texto justificado.

Codificación por desplazamiento de palabras
Codificación por desplazamiento de palabras

- Modificación de caracteres: Envuelve alteraciones menores a las formas de los caracteres. Una persona interesada en quebrar estos mecanismos de seguridad podría hacerlo simplemente reespaciando las líneas ya sea uniforme o aleatoriamente, el espaciado entre palabras o la forma de los caracteres.

CONCLUSIONES

Actualmente existen varios grupos de investigadores, tanto en universidades como en empresas comerciales, que se dedican a estudiar y desarrollar técnicas de DW (Digital Watermarking) o marcado digital de imágenes.

No hay una única aplicación para las marcas digitales, sino que este proceso es aplicable en una gran variedad de casos. Por lo tanto, no existe una única técnica que pueda ser utilizada en todos los casos, sino que existen distintos tipos de técnicas de marcas de aguas digitales cuyas propiedades varían de acuerdo al contexto de aplicación para el que fueron desarrolladas.

Existen en la actualidad hay aún varias barreras que evitan que esta tecnología se vuelva efectiva y de uso difundido. La misma se halla aún en sus desarrollos iniciales. El mayor desafío técnico es desarrollar una protección segura pero manteniendo las marcas ocultas. Con este trabajo se intentó dejar en claro el concepto de marca de agua digital o watermarking, los tipos y propiedades que debe poseer un sistema de marca de agua. Así mismo se mencionaron las técnicas más utilizadas en la inserción de marcas de aguas digitales dependiendo del contenido de un archivo de multimedia.

REFERENCIAS BIBLIOGRAFICAS

- A. TANENBAUM, "Computer Networks", Prentice Hall PTR New Jersey - 1996.
BRÜNNER, J. J. Educación e Internet. ¿La próxima revolución?, Fondo de Cultura Económica, Chile. 2004.
CASTELLS, Manuel. El desafío tecnológico. Alianza. Madrid. 1986.



29 de octubre al 9 de noviembre de 2008

- COX, I. J. AND MILLER, M. L. (2002): "The First 50 Years of Electronic Watermarking". EURASIP J. of Applied Signal Processing, 2, 126-132
- D. CHADWICK , A. YOUNG , "Merging and Extending the PGP and PEM Trust Models - The ICE-TEL Trust Model", IEEE Network , May/Jun-97.
- G. ALDEGANI., "La amenaza del Hacking" , Compu Magazine, Ago-97.
- GARCIA ARETIO, LORENZO. "Educación a Distancia Hoy". Volumen Nro 840.984, Colección Educación Permanente. Universidad Nacional de Educación a Distancia. Madrid, Febrero de 1998.
- H. BERGHEL, L. O'GORMAN, "Protecting ownership rights through digital watermarking", IEEE Computer , Jul-96.
- H. BERGHEL, "Watermarking Cyberspace", ACM Communications , Nov-97.
- J. BRASSIL, S. LOW, N. MAXEMCHUK, L. O'GORMAN, "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications, Oct-95
- J. BACH, "Good Enough Quality : Beyond the Buzzword", IEEE Computer , Ago-97.
- J. ZHAO, "Look, It's Not There", Byte, Ene-97.
- LEVIS, DIEGO, GUTIERREZ, MA. Hacia una herramienta educativa universal? Enseñar y aprender en tiempos de Internet, Ediciones Ciccus, Bs. As. 2000.
- LÓPEZ, C. (2002): "Watermarking of Digital Geospatial datasets: a review of Technical, Legal and Copyright issues", International Journal of Geographic Information Science, 16, 6, 589-607.
- N. JOHNSON, S. JAJODIA, "Exploring Steganography: Seeing the Unseen", IEEE Computer, Feb-98
- P. NEUMAN,"Crypto Key Management", ACM Communications, Ago-97.
- REY VALZACCHI, JORGE. "Internet y educación". Ed Horizonte . Argentina . 1999
- ROZENHAUZ, J, STEINBERG, S *Llegaron para quedarse: Propuestas de inserción de las nuevas Tecnologías en las aulas*, Miño y Dávila, Argentina. 2002
- S. GARFINKEL, "Public Key Cryptography", IEEE Computer, Jun-96.
- S. LOW, N. MAXEMCHUK, "Performance Comparison of Two Text Marking Methods", IEEE Journal on Selected Areas in Communications, May-98.