REVISTA FCEFyN

Marcas de agua: una contribución a la seguridad de archivos digitales

Laura M. Vargas[1], Elizabeth Vera de Payer[2] y Alejandra Di Gionantonio[3]

[1]*Departamento de Computación, Facultad de Ciencias Exactas, Físicas y Naturales, Universidad Nacional de Córdoba, Córdoba, Argentina*

[2]*Departamento de Matemática, Facultad de Ciencias Exactas, Físicas y Naturales, Universidad Nacional de Córdoba, Córdoba, Argentina*

[3]*Departamento de Sistemas, Facultad Regional Córdoba, Universidad Tecnológica Nacional, Córdoba, Argentina*

Fecha de recepción del manuscrito: 18/08/2015
Fecha de aceptación del manuscrito: 16/12/2015
Fecha de publicación: 15/03/2016

Resumen— En las últimas dos décadas ha resurgido el arte de almacenar y transmitir información encubierta debido a los avances en las tecnologías de generación, almacenamiento y comunicación de contenidos digitales. El objetivo actual de este embebido de información, llamado marcado de agua digital, es proteger los archivos anfitriones y detectar adulteraciones. El marcado siempre produce una degradación del objeto contenedor (llamado host) de modo que en las técnicas que no permiten recuperar el original se ve afectada su utilidad y el daño causado es irreversible. Por esta razón, en los últimos años se ha enfocado la investigación en el desarrollo de marcas reversibles en las que los legítimos usuarios pueden extraer la marca embebida y recuperar el archivo original, si es necesario. El propósito de este trabajo es difundir el conjunto de estos métodos que contribuyen a la seguridad informática por sí solos o, en la mayoría de los casos, reforzando técnicas criptográficas. Se pondrá énfasis en el caso de imágenes digitales con valor legal, sean médicas, forenses o militares, las que utilizan marcas reversibles.

Palabras clave— marcas de agua, seguridad informática, autenticación, integridad, esteganografía.

Abstract— During the last two decades, the art of storing and transmitting covert information has gained importance due to technological advances in generation, storage and communication of digital content. The current purpose of the embedded information, called digital watermark, is to protect files and detect tampering. The watermarking always degrades the container object (called host), therefore the techniques that don't allow the recovery of the original file decreases its usefulness and produces an irreversible damage. For this reason, in recent years researchers have focused on reversible watermarking techniques; these techniques allow legitimate users to extract the embedded watermark and to restore the original file as needed. The aim of this article is to spread these methods that contribute to information security by themselves or, in most cases, reinforcing cryptographic techniques. Emphasis will be put on the case of digital images with legal value, whether medical, forensic or military, which use reversible watermarks.

Keywords— watermarking, information security, authentication, integrity, steganography.

INTRODUCCIÓN

En las últimas dos décadas, debido al auge de las redes e Internet, el marcado de agua digital, más conocido en la literatura como *digital watermarking* o simplemente *watermarking*, ganó un lugar como método para solucionar problemas de seguridad tales como la pérdida de integridad o la autenticación de los archivos digitales. También permite detectar adulteraciones e incluso ubicar en el archivo la posición donde se produjeron. Solo o con más frecuencia en combinación con técnicas criptográficas se aplica en contenidos digitales multimedia tales como textos, audio, software, imágenes o videos.

Dirección de contacto:
Laura Mónica Vargas, Avda. Vélez Sarsfield 1611 Ciudad Universitaria, X5016 CGA. Tel.:29050, Int. 50, lvargas@efn.uncor.edu

El marcado de agua digital es la técnica de embeber información en un contenido digital conocido como "host" o "anfitrión" con el objetivo de protegerlo contra la manipulación o uso ilegal. Contrasta con los métodos criptográficos puesto que en este caso la información secreta se embebe y es imperceptible, mientras que en la criptografía la información se ve, pero es incomprensible. Se diferencia de la esteganografía (información encubierta) en que la información incrustada está relacionada con el objeto que la embebe (Cox *et al.*, 2002).

El nombre de marcas de agua lo toma de los procedimientos de marcado de billetes cuyo objetivo inicial era probar su autenticidad y esta fue la designación elegida por Emil Hembrooke quien ideó y patentó en 1954 un método de embebido de códigos inaudibles en señales de música para verificar propiedad (Cox y Miller, 2002). El auge del watermarking digital comenzó unos años después, en la

década de 1990, siendo uno de sus precursores más conspicuos Ingemar Cox (Cox *et al.*, 1995).

Este trabajo se centrará en particular en métodos aplicables a imágenes digitales.

OBJETIVOS DE LAS MARCAS DE AGUA

Según el objetivo de la marca inserta en objetos digitales, se consideran tres grandes grupos:

a. Marcas para proteger derechos de autor o autenticar.
b. Marcas para comprobar la integridad del objeto digital, es decir verificar que este no cambió.
c. Marcas para insertar metadatos, es decir datos sobre el objeto en el que están embebidas.

La autenticación asegura que el objeto digital proviene de una fuente autorizada. Actualmente existen dos herramientas para autenticar objetos digitales: la firma digital y el watermarking. Un sistema de firma digital de clave pública consiste en el cálculo mediante una función matemática de un resumen casi unívoco de los datos de un archivo el que convenientemente encriptado constituye la firma digital. Esta, mediante un adecuado esquema de claves, cumple varios objetivos: autentica, no permite que quien generó el archivo lo repudie y asegura integridad (Tanembaum, 2003). La firma digital se almacena concatenada a los datos que protege de modo que puede ser separada o bien perderse si el archivo es abierto y convertido en otro formato. Las técnicas de watermarking tratan a la imagen como un canal de comunicación. La información de autenticación que puede consistir en un identificador o códigos especiales, se embebe en el archivo (en general en forma imperceptible) y sobrevive a los cambios de formato. La combinación de ambas estrategias, es decir el embebido de la firma digital fortalece este último método.

Una característica propia del watermarking es la posibilidad, variable según las distintas técnicas, de detectar la región que se modificó, algo que no permite la firma digital. En el caso de imágenes médicas o legales como información militar o policial, por ejemplo, en las cuales existe una ROI (Región de Interés) es importante decidir que esta no fue alterada, más allá de lo que haya sucedido con el resto.

El embebido de metadatos protege a estos del recorte que puede producirse si son agregados concatenadamente al archivo original. Este es un objetivo útil en imágenes médicas, por ejemplo, donde es conveniente insertar los datos del paciente y la fecha en que se hizo el estudio.

Un caso especial de watermarking es el *fingerprinting*, equivalente a la introducción de números de serie en productos. El propietario de los archivos digitales inserta diferentes marcas de agua en las copias entregadas a los distintos clientes. Así se puede hacer un rastreo y conocer quién permitió copias ilegales.

CLASIFICACIÓN DE MARCAS DE AGUA

Las marcas de agua se clasifican siguiendo diferentes criterios.

1) Según su reacción ante los ataques, sin importar si los ataques son intencionales o no, las marcas se clasifican en:

a. Robustas
b. Frágiles
c. Semifrágiles

Las marcas de agua robustas deben resistir todo tipo de ataques, detectándoselas incluso después de producidos los mismos. Sirven para proteger los derechos de autor. En el caso de imágenes, no se puede tolerar la eliminación de la marca por deformaciones geométricas, rotación, escalado o compresión, por ejemplo.

Las marcas de agua frágiles son aquellas que quedan eliminadas o modificadas y dejan de cumplir su función en caso de ataque. La incapacidad de recuperarlas, revela que se produjo algún cambio y ese es el objetivo buscado. No toleran ninguna transformación, ni siquiera las más comunes en procesamiento de datos. Se utilizan fundamentalmente para asegurar integridad ya que a través de ellas se conoce si el objeto fue alterado.

Las marcas de agua semifrágiles sobreviven a cierto tipo de alteraciones, como compresión sin pérdidas, pero deben destruirse ante cambios importantes, no reversibles. Una marca de este tipo puede consistir en extraer información de la ROI a la que se dividió en bloques y luego embeberla en la Región de No Interés (RONI). Si posteriormente se prueba que algún bloque de la ROI fue modificado se puede recuperar la información con los datos embebidos en la RONI, e incluso determinar qué bloque fue alterado.

2) Según la necesidad de poseer información original para decidir si un archivo es auténtico o no, las técnicas de marcado se clasifican en:

a. Ciegas
b. No ciegas o informadas
c. Semiciegas

En un comienzo la marcación era informada. Cuando el dueño de un archivo debía decidir si una copia era ilegal o no, comparaba la misma con el original extrayendo la marca que probaba la propiedad del objeto digital.

En las ciegas, preferidas actualmente, no se precisa contar con la información original para determinar la autenticidad del archivo.

En las semiciegas se precisan algunos datos del original para recuperar la marca, por ejemplo, en el caso de imágenes, su histograma.

3) Según el dominio en el que es insertada una marca. En las técnicas más populares para imágenes, las marcas pueden embeberse:

a. En el dominio espacial
b. En el dominio de transformadas matemáticas, ya sea modificando los coeficientes de la Transformada de Fourier, la DCT (Transformada Discreta de Coseno), o bien de alguna de las Transformadas Wavelet.

En un comienzo se utilizó el dominio espacial, cambiando el LSB (Least Significant Bit/ Bit Menos Significativo) por un bit de la marca según una clave. Esta técnica pronto se reveló ineficiente porque aunque produce una distorsión relativamente baja (a lo sumo cambia la

intensidad de cada píxel en una unidad) es de baja capacidad y tiene poca resistencia ante ataques. Por esto se comenzó a emplear el embebido en los coeficientes de transformadas a pesar de su mayor complejidad computacional. Las técnicas más populares se desarrollaron en el dominio DCT y DWT (Discrete Wavelet Transform) utilizando distintas variantes para lograr baja distorsión (Barni *et al.*, 1998), (Kundur y Hatzinakos, 1999). La Fig. 1 muestra un esquema de embebido en el dominio de la transformada.

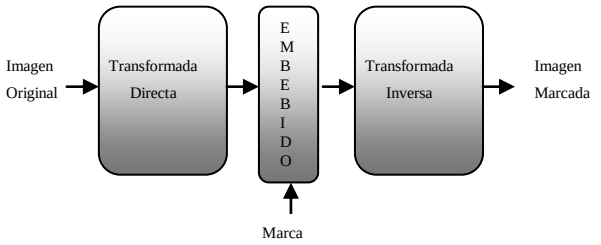

Fig. 1: Esquema de Embebido en el Dominio de la Transformada

El marcado en el dominio de la transformada DCT es resistente a la compresión JPEG, ya que esta se realiza aplicando esta transformada (Sayood, 2005). Embebiendo la marca en los coeficientes que son preservados por este método de compresión el watermarking se vuelve robusto a este.

REQUISITOS DE LAS MARCAS

Los requisitos que deben cumplir los esquemas de marcado, tanto robustos como frágiles son:

a. Imperceptibilidad
b. Capacidad

En el caso de imágenes, la imperceptibilidad se mide objetivamente, a través del MSE (Mean Square Error/ Error Medio Cuadrático) y el PSNR (Peak Signal Noise Relation/ Relación Pico Señal Ruido) indicados en ec. (1) y ec. (2) donde M y N son la cantidad de filas y columnas respectivamente de las imágenes I e I_w (original y marcada), e $I(i,j)$, $I_w(i,j)$ son las intensidades de los píxeles ubicados en la fila i, columna j de cada una de ellas.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} (I_w(i,j) - I(i,j))^2}{MN} \quad (1)$$

$$PSNR = 10\log \frac{(I_{Pico})^2}{(MN)^{-1}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_W(i,j) - I(i,j))^2}\ dB \quad (2)$$

Un alto PSNR indica una imagen de más calidad, lo mismo que un bajo MSE. La experimentación indica que un PSNR aceptable debe superar los 30 dB. También la imagen marcada debe ser evaluada subjetivamente por observadores.

Existe otro parámetro para medir la calidad. Se trata de una medida de la similaridad entre dos imágenes, una de referencia I y otra modificada, que en este caso será la marcada I_w: el SSIM (Similarity Structural Index / Índice de Similaridad Estructural) (Wang *et al.*, 2004). Este tiene en cuenta las particularidades del SHV (Sistema Humano Visual) considerando tanto la pérdida de correlación como las distorsiones de luminancia y de contraste entre una imagen y su modificada. SSIM es definido mediante ec. (3) y ec. (4), donde $l(I,I_w)$ compara las luminancias de ambas imágenes a través de sus valores de luminancia media μ, $c(I,I_w)$ compara el contraste utilizando la desviación estándar σ de ambas imágenes y finalmente $s(I,I_w)$ las estructuras mediante la correlación o producto interno entre ambas imágenes, indicado en ec. (5). Las constantes C indicadas se fijan de modo de conseguir que el denominador no se haga cero.

$$SSIM(I, I_w) = f(l(I, I_w)c(I, I_w)s(I, I_w)) \quad (3)$$

$$l(I, I_w) = \frac{2\mu_I\mu_{I_w} + C_1}{\mu_I^2\mu_{I_w}^2 + C_1}$$

$$c(I, I_w) = \frac{2\sigma_I\sigma_{I_w} + C_2}{\sigma_I^2\sigma_{I_w}^2 + C_2} \quad (4)$$

$$s(I, I_w) = \frac{\sigma_{I,I_w} + C_3}{\sigma_I\sigma_{I_w} + C_3}$$

$$\sigma_{I,I_W} = \frac{1}{MN-1}\sum_{i=1}^{MN}(I_i - \mu_I)(I_{w_i} - \mu_{I_w}) \quad (5)$$

Wang combina las ecuaciones dadas en la (6), indicando que $C_1=(k_1L)^2$ y $C_2=(k_2L)^2$ estabilizan la división, siendo L el rango dinámico de intensidad de los píxeles ($2^{\text{bits/píxel}}$-1), k_1=0,01 y k_2=0,03 por defecto.

$$SSIM(I, I_w) = \frac{(2\mu_I\mu_{I_W} + C_1)(2\sigma_{I,I_w} + C_2)}{(\mu_I^2 + \mu_{I_w}^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} \quad (6)$$

Los valores de SSIM pertenecen al intervalo [0, 1], donde el 1 indica absoluta coincidencia entre las imágenes, caso en el que MSE es igual a 0 y PSNR tiende a infinito.

Por otra parte, la capacidad del marcado se refiere a la cantidad de información que un archivo es capaz de embeber. En imágenes se indica en bpp (bits por píxel).

En las marcas robustas interesa la persistencia de la marca, que debe permanecer luego de ataques intencionales o daños colaterales.

Imperceptibilidad, capacidad y robustez guardan relación entre sí, al aumentar una de ellas disminuye necesariamente otra. Así, si se inserta más información, disminuye la imperceptibilidad, puede volverse detectable y la marca es más fácil de atacar. La Fig. 2 ilustra esta situación.

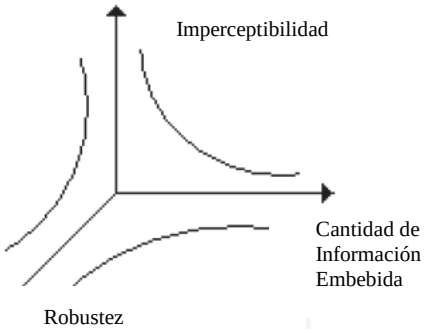

Fig. 2: Parámetros del Watermarking

En los primeros métodos de marcado desarrollados se le concedió extrema importancia a la imperceptibilidad. Luego, con las marcas reversibles para imágenes de valor legal, forenses, médicas o militares, dado que en estas se recupera el archivo original, comenzó a despertar interés el aumento de la capacidad del método. En el marcado reversible se necesita embeber carga extra para poder revertir el proceso. Esto hace que la carga útil sea solo una parte de la carga total que se debe insertar, lo que exige un método de mayor capacidad. Por otro lado. en imágenes médicas o legales es de interés insertar metadatos para lo que se precisa una capacidad acorde a la cantidad de bits a incrustar.

ETAPAS DE MARCADO

En las técnicas de ocultamiento de información se reconocen dos pasos:

1. Embebido de un mensaje en el host.
2. Detección o extracción del mensaje.

En el segundo paso, se puede recuperar archivo original (en el caso de las técnicas de embebido reversibles) y mensaje, o bien simplemente detectar la presencia del mensaje (en el caso de técnicas irreversibles).

En un comienzo se desarrollaron esquemas robustos, los que introducen siempre degradación en el objeto anfitrión. Por esta razón se empezó a priorizar la investigación y desarrollo de métodos reversibles, donde si bien el objeto marcado se degrada, los usuarios finales (por ejemplo profesionales médicos) acceden al archivo original (Fridrich *et al.*, 2002). La Fig. 3 muestra un esquema completo de marcado reversible donde se recuperan tanto el archivo original como la marca.

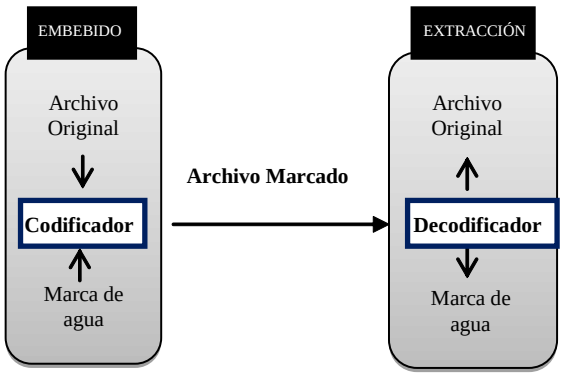

Fig. 3: Esquema de Marcado Reversible

Para valorar los algoritmos de marcado interesan especialmente la complejidad computacional y el tiempo requerido por el embebido.

UN EJEMPLO DE MARCADO REVERSIBLE EN IMÁGENES

Uno de los primeros algoritmos de marcado reversible en el dominio de la transformada wavelet, en particular de la transformada Cohen- Daubechies- Feauveau (2,2), fue desarrollado por Xuan *et al.* (Xuan *et al.*, 2002). Se lo presentará como ejemplo, dada su sencillez.

Una vez calculados los coeficientes de la transformada cdf(2,2) el algoritmo desecha la banda de aproximación, ya que embeber en ella afecta la imperceptibilidad, y comprime en forma reversible uno de los planos de bits de las subbandas de detalle (horizontales, verticales y diagonales). Un método de compresión posible es el aritmético. En el espacio ganado se insertan los bits de la marca. Para agregar seguridad se pueden embeber los bits de la marca según una clave.

Ya embebida la marca en la transformada de la imagen, se calcula la antitransformada para obtener la imagen marcada. Un inconveniente de este método es que puede producirse desbordamiento, es decir que en una imagen común de 8 bpp, se pueden obtener valores de intensidad fuera del rango [0 255]. En estos casos se debe realizar un preprocesamiento que consiste en la compresión del histograma.

Para recuperar la imagen original, emisor y receptor deben conocer el plano en que se efectuó la compresión. Además, deben adicionarse a la marca útil los datos necesarios para realizar la decompresión una vez extraída la marca, lo que se conoce como sobrecarga del método.

Para lograr mayor compresión, el plano de bits a comprimir debe ser medio. Si fuera el plano de LSBs, se tendría poca capacidad, y si se usara un plano muy alto se perdería mucha información lo que provocaría una mayor degradación de la imagen. En imágenes de 8 bits por píxel una elección habitual es el plano 4.

Los métodos de marcado arrojan resultados diferentes en diferentes escenarios. En general, los investigadores desarrollan su experimentación en un conjunto de imágenes típicas, a las cuales pertenecen las mostradas en la Fig. 4 (‘lena’ y ‘baboon’) que tienen 512x512 píxeles, y como marcas generan secuencias de bits pseudoaleatorias.

En la Fig. 5 se aprecian las bandas de aproximación y detalle de ‘lena’, para la transformada cdf(2,2). En la Fig. 6 se presentan la capacidad y calidad del método de Xuan explicado aplicado en las imágenes seleccionadas. Se observa que para la compresión del plano 4 de bits de los coeficientes de las bandas de detalle, la imagen ‘lena’ arroja un PSNR de más de 30 dB, para una capacidad máxima de 0,45 bpp, es decir para una marca de 117964 bits, mientras que ‘baboon’ no supera los 0,2 bpp, es decir 52428 bits, con un PSNR ligeramente inferior a los 30 dB. Repetida la experiencia comprimiendo el tercer plano de bits en ‘baboon’ se alcanza una capacidad de 0,4 bpp, pero con un PSNR de 25 apenas dB. Los resultados de la experimentación se muestran en la Tabla 1.

Fig. 4: Imágenes de Prueba: ‘lena’ y ‘baboon’

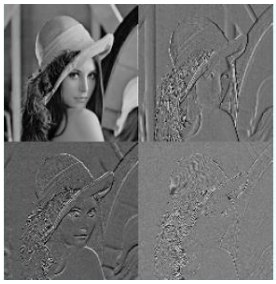

Fig. 5: Bandas de Aproximación y Detalle para 'lena' según cdf(2,2)

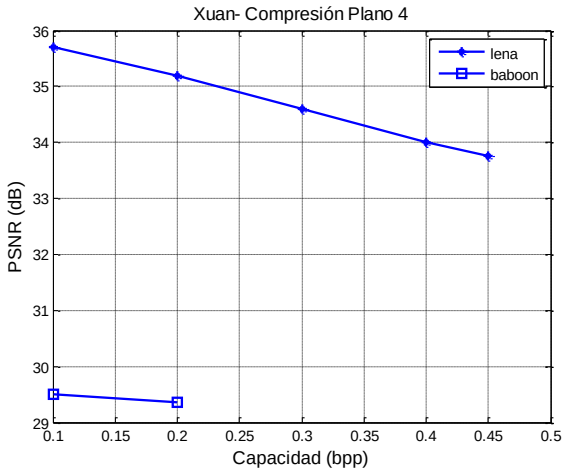

Fig. 6: Algoritmo de Xuan - Capacidad vs. Calidad

Tabla 1: Capacidad y Calidad – Algoritmo de Xuan

Imagen	Capacidad (bpp)	PSNR (dB)	MSE	SSIM
lena	0,10	35,71	1 7,44	0,9724
	0,20	35,17	1 9,76	0,9696
	0,30	34,55	2 2,81	0,9669
	0,40	33,97	2 6,07	0,9636
	0,45	33,85	2 6,79	0,9636
baboon	0,10	29,51	7 2,74	0,9683
	0,20	29.35	7 5,43	0,9679

Existen numerosos estudios que recopilan métodos reversibles aplicables en general a todo tipo de imágenes y algunos particulares para imágenes médicas, entre ellos los realizados por Caldelli *et al.*, Hisham *et al.* y Khan *et al.* (Caldelli *et al.*, 2010), (Hisham *et al.*, 2013), (Khan *et al.*, 2014).

ALGUNAS CONSIDERACIONES SOBRE PRESENTE Y FUTURO DEL WATERMARKING

Si bien en un principio fue discutida la aplicabilidad y efectividad del watermarking digital, en especial desde la criptografía clásica, su empleo fue defendido por investigadores (Barni, 2003). Las primeras técnicas recibieron críticas, en particular porque no eran reversibles y, por lo tanto, sometían a degradación el objeto anfitrión. La comunidad científica ha respondido desarrollando nuevos y mejores métodos y aún sigue siendo un tema abierto y activo.

Actualmente en telemedicina y en cloud computing el watermarking ha encontrado un amplio campo de aplicación. Cloud computing ha modificado la industria de la computación en los últimos años. La información se ha movido hacia la nube. También la de salud que antes se almacenaba en los centros médicos y a la que solo accedían los usuarios autorizados. Entre las razones que se tienen para migrar hacia la nube se encuentran la facilidad de comunicación, la posibilidad de efectuar trabajos colaborativos, la menor necesidad de tener personal especializado en tecnologías informáticas. Hoy, los protocolos de comunicación permiten una conexión a Internet confiable, con recuperación de desastres. Sin embargo, existe todavía un desafío a vencer: la seguridad, aunque se han registrado avances en el tema. Se debe impedir el acceso no autorizado a informaciones personales, y es necesario asegurar la integridad de los datos así como la no repudiación de los mismos. Como se dijo, si los metadatos o un resumen hash del archivo se almacenan aparte, pueden ser fácilmente recortados y reemplazados. Para vencer estos obstáculos se recurre a técnicas de watermarking. En el caso de imágenes médicas o críticas, se recomienda watermarking reversible, dadas las exigencias legales de las mismas. El watermarking va en general acompañado de técnicas criptográficas, así se realiza un resumen SHA (Secure Hash Algorithm) o MD5 (Message Digest Algorithm) del archivo el que luego se embebe y los metadatos insertados son previamente encriptados. De la combinación de técnicas propias de cloud computing, criptografía y watermarking surge un uso seguro de la nube (Singh y Singh, 2013).

Empresas como IBM, Digimarc, Philips, Cinea, Verimatrix, han incorporado tecnologías de watermarking y se ha conformado en el año 2006 la DWA (Digital Watermarking Alliance), cuyo sitio en la Web es *http://www.digitalwatermarkingalliance.org*. La DWA es un grupo sostenido por un conjunto de compañías entre las que se incluyen algunas de las empresas nombradas y otras más que emplean y tienen interés en promover técnicas de watermarking, ofreciendo soluciones de este tenor para el problema de la seguridad en el mercado multimedia.

REFERENCIAS

[1] Barni M., Bartolini F., Cappellini V. y Piva A. (1998), "A DCT-domain System for Robust Image Watermarking". En *Journal on Signal Processing*, Vol. 66, Issue 3, pp. 357-372, Ed. Elsevier.

[2] Barni, M. (2003), "What is the future of watermarking?". En *IEEE Signal Processing Magazine*, Vol. 20, Issue 6, pp. 53-59.

[3] Caldelli R., Filippini F. and Becarelli R. (2010), "Reversible Watermarking Techniques: An Overview and Classification". En *Eurasip Journal on Information Security*, Vol. 2010, Art. ID 134546, 19 páginas.

[4] Cox I. y Miller M. (2002), "The first 50 years of digital watermarking". En *EURASIP Journal on Applied Signal Processing*, pp. 126-132.

[5] Cox I., Kilian J., Leighton T. y Shamoon T. (1995), "Secure Spread Spectrum watermarking for multimedia". *NEC Research Institute-Technical Report*.

[6] Cox I., Miller M. y Bloom J. (2002), "Digital Watermarking and Fundamentals". Ed. Morgan Kaufman, Series in Multimedia Information and Systems.

[7] Fridrich J., Goljan M. y Du R. (2002), "Lossless data embedding – new paradigm in digital watermarking". En *Proceedings of the SPIE Security and Watermarking of Multimedia Content* (2), pp. 185-196.

[8] Hisham S., Liew S. y Zain J. (2013), "A Quick Glance at Digital Watermarking in Medical Images". En *Biomedical Engineering Research*, Vol. 2, Issue 2, pp. 79-87.

[9] Khan A., Siddiqa A., Munib S. y Malik S. (2014), "A recent survey of reversible watermarking techniques". En *Information Sciences*, Vol. 279, pp. 251-272.

[10] Kundur D., Hatzinakos D. (1999), "Digital watermarking for telltale tamper proofing and authentication". En *Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information*, Vol. 87, pp.1167-1180.

[11] Sayood K. (2005), "Introduction to Data Compression". Ed. Morgan Kauffman Series in Multimedia Information and Systems, 3th Ed.

[12] Singh N. y Singh S. (2013), "The amalgamation of digital watermarking and cloud watermarking for security enhancement in cloud computing". En *International Journal of Computer Science and Mobile Computer, IJCSMC,* Vol. 2, Issue 4, pp. 333-339.

[13] Tanembaum A. (2003), "Redes de Computadoras". Ed. Pearson, 4ta Ed., pp. 755-762.

[14] Wang Z., Bovik A., Sheikh H. y Simoncelli E. (2004), "Image Quality Assurement: from Error Visibility to Structural Similarity". En *IEEE Transactions on Image Processing*, Vol. 13, N° 4, pp. 600-612.

[15] Xuan G., Zhu J., Chen J., Shi Y., Ni Z. y Su W. (2002), "Distortionless data hiding based on integer wavelet transform". En *Electronics Letters*, pp. 1646-1648.