ISSN 1870-4069

Mejora de un esquema de marca de agua aplicado a la gestión de imágenes médicas

María de Jesús Del Pilar Lagunas, Javier Molina García, Volodymyr Ponomaryov

Instituto Politécnico Nacional, ESIME Culhuacán, Ciudad de México, México

{delpilar.lagunas, javier.molina.21016,volodymyr.ponomar}@gmail.com

Resumen. En el presente trabajo se propone un método de marca de agua basado en la DWT que aborda los problemas de protección de datos personales y datos sobre los estudios clínicos de un paciente, recuperación de datos del médico que lleva a cabo los estudios y verificación de la integridad de las imágenes médicas. El esquema de marcado realiza la descomposición de una imagen médica en formato DICOM al dominio tiempo-frecuencia mediante la DWT, insertado bits empleados para detección de alteraciones en el primer nivel de descomposición de la sub-banda HL, posteriormente se inserta la información del paciente, identificación del médico e información adicional empleada durante la extracción en la sub-banda de frecuencia LH. Los resultados obtenidos muestran que las imágenes protegidas no se degradan de manera significativa, ya que se obtiene un valor en términos de PSNR (dB) superior a 50dB; asimismo, se demostró que el esquema de marcado de agua es capaz de extraer la información insertada empleando ataques no intencionales como compresión. Finalmente, se mostró experimentalmente la eficiencia del método propuesto para detectar alteraciones empleando ataques de adición de ruido y emborronamiento.

Palabras clave: marcas de agua, imágenes médicas, confidencialidad, detección de alteraciones, gestión de imágenes médicas.

Improvement of a Watermarking Scheme Applied to Medical Image Management

Abstract. In this paper we propose a watermark method DWT-based that addresses the problems of personal data protection and and data about the clinical studies of the patient, the recovery of data from the physician who conducts the studies and the verification of the integrity of medical images. The watermarking scheme performs the decomposition of an image in DICOM format to the time frequency domain by means of the Wavelet transform, where bits used to detect alterations are embedded in the first decomposition level of the HL sub-band, subsequently the information of the patient, identification of the physician and

additional information used during the extraction are embedded in the sub-band LH. Experimental results show that the watermarked images do not degrade significantly, since a value in terms of PSNR (dB) greater than 50dB is obtained, likewise it was demonstrated that the watermark scheme is capable of extracting the embedded information using unintentional attacks such as image compression. Finally, the efficacy of the proposed method to detect alterations using noise addition and blurring filters was experimentally demonstrated.

Keywords: watermarking, medical images, confidentiality, image tamper detection, medical image management.

1. Introducción

Debido a los avances en la tecnología de la información y las comunicaciones, ha aumentado la transferencia y almacenamiento de datos a través de las redes. La tecnología también se encuentra presente en los hospitales debido a que las imágenes médicas en formato DICOM [1] (*Digital Imaging and Communication in Medicine*, por sus siglas en inglés) son empleadas por profesionales de la salud y el uso va desde tele-diagnóstico hasta tele-cirugías, así mismo, estos archivos facilitan la gestión, el almacenamiento e impresión de los mismos [2]. Los archivos contienen datos clínicos de los pacientes que son la principal fuente de información para el diagnóstico y tratamiento de una gran cantidad de enfermedades y anomalías. Al mismo tiempo que existen estos beneficios también existen riesgos para los datos o registros electrónicos paciente o EPR (*Electronic Patient Record*, por sus siglas en inglés), por lo tanto, es una necesidad constante el mantener la seguridad de la información en imágenes médicas [3,4].

La protección de información médica en la mayoría de los países se deriva de una estricta regulación como la HIPAA de los Estados Unidos y la Directiva Europea de la CE 95/46 que aplica a los registros de información de un paciente, los cuales contienen un conjunto exámenes clínicos, anotaciones de diagnósticos y otros hallazgos e imágenes en los EPR [5], Así mismo se tiene la norma de protección de datos personales en salud en México: NOM-004-SSA3-2012 [6]. Debido a lo anterior, son necesarios métodos que se utilicen para la protección de datos del paciente, una solución a esto son las marcas de agua [9,12-14], las cuales son técnicas empleadas para insertar un mensaje o contenido digital dentro de otro archivo digital (denominado archivo *host*), estas técnicas son utilizadas para aumentar el nivel de seguridad y/o autenticidad del archivo *host* multimedia.

2. Estado del arte

Durante los últimos años se han implementado técnicas basadas en marcas de agua, las cuales son aplicadas a imágenes médicas [7-13]. En la presente sección se presentan los métodos más representativos los cuales aplican técnicas de marcado de agua en imágenes médicas.

En [7] se propone una técnica de marca de agua reversible basada en la Transformada de Wavelet Entera (IWT por sus siglas en inglés de *Integer Wavelet Transform*), este método logra incrustar marcas de agua con baja distorsión, adicionalmente utiliza programación genética (GP) para localizar los coeficientes Wavelet para inserción.

Trankkar [8] propone un esquema de marcado de agua combinando la Transformada Discreta de Wavelet (DWT por sus siglas en inglés de *Discrete Wavelet Transform*) y la Descomposición en Valores Singulares (SVD por sus siglas en inglés de *Singular-Value Decomposition*) además implementa códigos de corrección de errores (ECC por sus siglas en inglés de *Error-Correcting Code*), el autor propone el uso de dos marcas de agua, una como imagen y otra marca de agua como texto la cual contiene los EPR.

Sharma [9] propone marca de agua múltiple combinando las transformadas DWT y la Transformada Discreta del Coseno (DCT por sus siglas en inglés de *Discrete Cosine Transform*), además de los algoritmos de cifrado RSA (*Rivest, Shamir y Adleman*) y MD5 (*Message-Digest Algorithm 5),* y el ECC Hamming, en este proceso utiliza dos marcas de agua, una imagen (logo del centro hospitalario) y otra marca de agua como texto (EPR) los cuales son cifrados por el algoritmo RSA.

En [10] se propone un esquema de marca de agua basado en la DWT, el proceso de inserción se realiza en la sub banda de frecuencia baja LL para incrementar la robustez. Este sistema agrega un mapa logístico proporcionando mayor eficiencia y seguridad para el cifrado de las imágenes.

Badshah en [11] propone realizar un método de marcado de agua donde cada imagen se divide en ROI (*Region of Interest*) y RONI (*Region of Non-Interest*). La técnica de la marca de agua consiste en el método del Bits Menos Significativo (LSB por sus siglas en inglés de *Least Significant Bit*), donde la marca de agua a insertar es comprimida mediante el algoritmo LZW (*Lempel-Ziv-Welch*).

Singh [12] propone un esquema de marcado de agua empleando múltiples técnicas DWT, DCT, SVD, ECC (Hamming y BCH) y encriptación selectiva para la protección digital de contenido. La propuesta descompone la imagen host en tres niveles de descomposición Wavelet, donde las sub-bandas de frecuencia LH2 y LL3 son seleccionadas para la inserción de una imagen y los EPR, finalmente se emplea red neuronal de retro-propagación (BPNN por sus siglas en inglés de *Back Propagation Neural Network*) durante el proceso de extracción minimizando los efectos de distorsión en la imagen marcada.

Singh [13] propone la inserción de múltiples marcas de agua, combinando DWT, DCT y SVD, este método utiliza una imagen médica y los EPR como marca de agua. Este proceso se realiza descomponiendo la imagen hasta el segundo nivel de descomposición Wavelet, considerando la banda de frecuencia baja LL de la imagen portadora que se transforma mediante DCT y SVD, este mismo procedimiento se realiza a la imagen médica de marca de agua, insertando el valor singular de la marca de agua en el valor singular de la portadora, la marca de agua de texto se inserta en la banda HH del segundo nivel de descomposición Wavelet.

Giakoumaki et al. [14] propone un esquema de protección de datos personales del paciente y un esquema de detección de alteraciones en imágenes médicas, este método está basado en la DWT donde se insertan marcas de agua desde el primer nivel de descomposición hasta el cuarto nivel de descomposición. La desventaja de este método

es una reducida capacidad de inserción, así como una gran cantidad de información a insertar. La principal ventaja de este método es que puede ser implementado en diversas aplicaciones de imágenes médicas propiciando alta seguridad de los datos del paciente, así como la identificación de la autenticidad de la imagen.

El presente trabajo está basado en el método propuesto por Giakoumaki [14], donde en el método propuesto se realiza una mejora en la capacidad de inserción del archivo *host*, así mismo se realiza una mejora en el algoritmo de generación de marcas de agua reduciendo la cantidad de bits empleados como marca de agua, donde se reduce la cantidad de bits a insertar, los cuales son utilizados para proteger la información médica y personal del paciente. Esta información es insertada como marca de agua dentro de una imagen en formato DICOM, así mismo se inserta un identificador del médico, finalmente se inserta información para detectar alteraciones en la imagen y mantener así la integridad de la misma. El resto del artículo está organizado como sigue, la sección tres muestra el desarrollo del método propuesto, la sección cuatro expone los resultados obtenidos y finalmente, la sección cinco presenta las conclusiones generadas.

3. Método propuesto

El esquema propuesto consiste en un método aplicado a imágenes médicas en formato DICOM, el cual realiza la detección de alteraciones para comprobar la integridad de la imagen médica, adicionalmente realiza la protección de la información del paciente, así como la inserción un identificador del médico que trata el caso médico del paciente. Este sistema divide la imagen en dos regiones, una ROI (*Region of Interest*) y una ROE (*Region of Embedding*), así mismo, este sistema está basado en técnicas de marcado de agua, donde la información para autenticación es insertada en el dominio de la DWT en toda la imagen, adicionalmente, la información del paciente y el identificador del médico es insertado en el mismo dominio, pero dentro de la ROE. Esto se realiza para no alterar significativamente la calidad de la ROI, ya que si esta es modificada de manera significativa podría llevar a una interpretación errónea por el médico o por parte de un sistema CAD. Finalmente, se inserta como marca de agua información adicional (coordenadas de la ROI y el total de bits que componen las marcas de agua), esta marca de agua es empleada para que el sistema de extracción sea un proceso a ciegas.

Una característica importante del método propuesto es que se realiza un análisis automático sobre la capacidad de inserción soportada por el sistema, tomando en consideración la ROI seleccionada por el médico y el tamaño de las marcas de agua a insertar, esto se realiza con el fin de insertar redundancia de las marcas de agua.

El Sistema de autenticación y protección de información del paciente en imágenes médicas está dividido en dos etapas, las cuales son mostradas en la Figura 1:

1. *Generación e inserción de marcas de agua*: En esta etapa, se lleva a cabo la generación de bits de las marcas de agua a insertar (información médica del paciente, identificación del médico, información para detección de alteraciones en la imagen e información para extracción de las marcas de agua antes mencionadas),

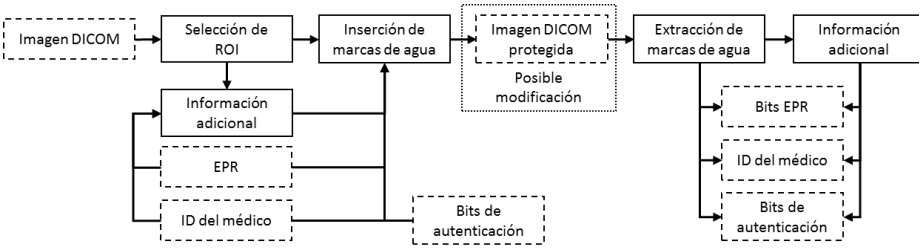


Fig. 1. Diagrama a bloques general del Sistema propuesto.

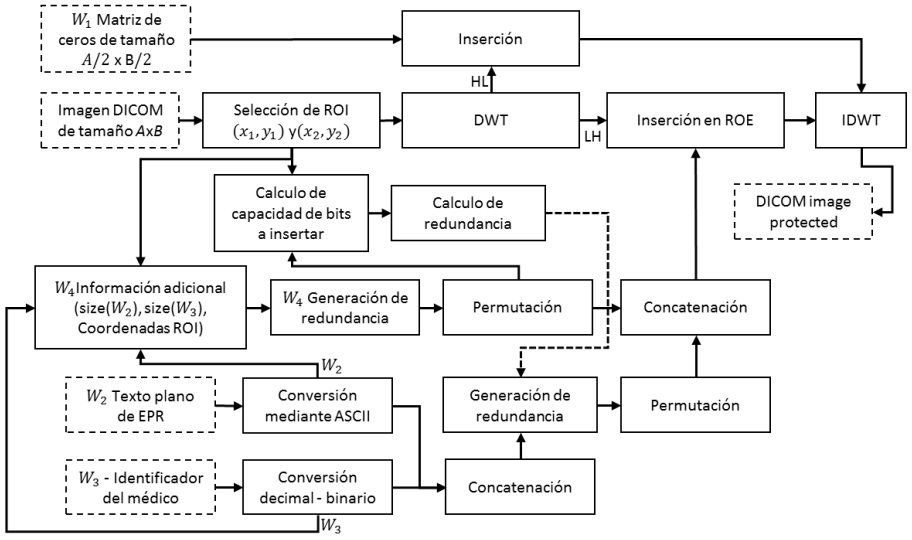


Fig. 2. Diagrama a bloques del proceso de *generación e inserción de marcas de agua.*

posteriormente la imagen médica es transformada al dominio de la frecuencia mediante la DWT, donde cada marca de agua es insertada.

2. *Extracción de marcas de agua y detección de alteraciones*: En esta etapa se realiza la extracción de las marcas de agua empleando el primer nivel de descomposición de la DWT, donde son extraídas la información de autenticación, marcas de agua de información del paciente e identificación del médico. Empleando las marcas de agua de autenticación se realiza el proceso de detección de alteraciones, donde en caso de detectar modificación en la imagen DICOM, las marcas de agua restantes podrían no ser extraídas y la imagen DICOM podría considerarse invalida para realizar el diagnóstico médico.

Las etapas mencionadas anteriormente son explicadas a continuación, donde los procesos de generación e inserción de marcas de agua y extracción de marcas de agua y detección de alteraciones son mostrados en Figura 2 y 3 respectivamente.

3.1. Generación e inserción de marcas de agua

Esta etapa se divide en dos sub-etapas: a) *generación de marcas de agua* y b) *inserción de marcas de agua*. Antes de realizar este proceso la ROI debe ser seleccionada por el médico, la cual es representada empleando las coordenadas (x_1, y_1) y (x_2, y_2), donde $x_1 < x_2$ y $y_1 < y_2$; x_1, y_1 son números impares y x_2, y_2 son números

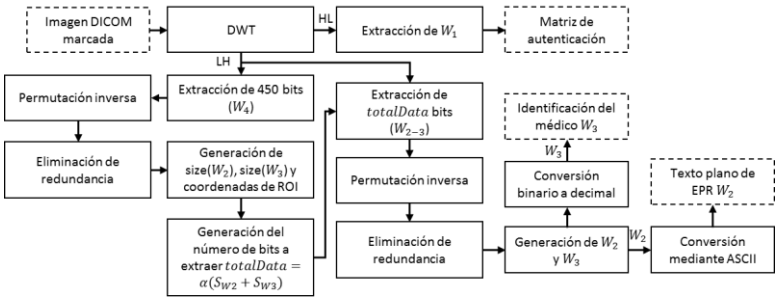


Fig. 3. Diagrama a bloques del proceso de *extracción de marcas de agua y detección de alteraciones.*

pares, estas coordenadas representan la esquina superior izquierda y la esquina inferior derecha respectivamente de la ROI sobre la imagen DICOM a proteger.

Durante la sub-etapa de *generación de marcas de agua* se generan cuatro marcas de agua, suponiendo que la imagen en formato DICOM a proteger es de tamaño AxB filas y columnas respectivamente, la primera marca de agua (W_1) consiste en una matriz de ceros de tamaño $A/2$ x$B/2$, la cual es utilizada para la detección de alteraciones. La segunda marca de agua (W_2) consiste en la información del paciente, la cual es representada en texto plano mismo que es convertido a una cadena binaria mediante código ASCII. La tercera marca de agua (W_3) consiste en un ID del médico el cual es conformado con un total de siete dígitos numéricos, estos dígitos son transformados a formato binario, representándose con un total de 24 bits.

Finalmente, la cuarta marca de agua es representada mediante $W_4 = [S_{W2}\ S_{W3}\ x_1\ y_1\ x_2\ y_2]$ donde S_{W2} y S_{W3} representan el tamaño de las marcas de agua dos y tres respectivamente, cada valor de este vector es representado con 15 bits, obteniéndose un total de 90 bits para la marca de agua W_4, posteriormente W_4 es repetida cinco veces, obteniéndose un total de 450 bits, esto se realiza con el fin de insertar redundancia de la información adicional para tener una mayor probabilidad de recuperar esta marca de agua en caso de un ataque no intencional (ej. compresión). Finalmente se genera $W_{2-3} = [W_2\ W_3]$ la cual representa la concatenación de las marcas de agua W_2 y W_3.

Después de generar cada marca de agua, se realiza el proceso de *inserción de marcas de agua*, en el cual se aplica el primer nivel de descomposición de la DWT a la imagen DICOM a proteger, obteniéndose las sub-bandas de frecuencia LL, LH, HL y HH. Posteriormente se realiza el proceso de inserción como en [13], donde W_1 es insertado dentro de la sub-banda de frecuencia HL, para realizar esto se genera un patrón binario $Q(f)$ mediante la función de cuantización (ecuación (1)):

$$Q(f) = \begin{cases} 0, & if \left\lfloor \frac{f}{\Delta} \right\rfloor = odd \\ 1, & if \left\lfloor \frac{f}{\Delta} \right\rfloor = even \end{cases}, \quad (1)$$

donde f representa cada coeficiente de detalle de la sub-banda de frecuencia y Δ representa el parámetro de cuantización, el cual es un número positivo. Una vez que se genera el patrón binario, se analiza la *i,j-esima* posición de *Q(f)*, si el valor es igual a la *i,j-esima* posición de W_1 entonces el coeficiente *f* no se modifica, en caso contrario se aplica la siguiente ecuación (2):

$$f = \begin{cases} f + \Delta, & if\ f \leq 0 \\ f - \Delta, & if\ f > 0 \end{cases}. \quad (2)$$

Las marcas de agua restantes son insertadas en la sub-banda de frecuencia LH dentro de la ROE, antes de insertar estas marcas de agua se analiza la capacidad de inserción para ver si es posible insertar redundancia de información. Este proceso se realiza de la siguiente manera, se genera una imagen de tamaño AxB rellena de ceros I_{ROI}, se coloca la ROI delimitada por las coordenadas (x_1, y_1) y (x_2, y_2) y todo el contenido de la ROI es seleccionado con el valor de 1. La imagen obtenida es re-escalada al tamaño $A/2$ x$B/2$, esto se realiza debido a que el tamaño de la sub-banda de frecuencia LH es $A/2$ x$B/2$. El cálculo del total de bits que se pueden insertar es el siguiente (ecuación (3)):

$$totbits = \frac{AB}{4} - \left(\sum_{j=1}^{\frac{A}{2}} \sum_{j=1}^{\frac{B}{2}} I_{ROI\,i,j} \right) - S_{W4}, \quad (3)$$

donde S_{W4} representa el tamaño de la marca de agua W_4, el cual es 450.

Una vez que se obtiene el valor de la capacidad de bits a insertar, se calcula la cantidad de copias que se pueden insertar las marcas de agua W_2 y W_3, esto se realiza mediante la operación $\lfloor totbits/(S_{W2} + S_{W3}) \rfloor$, el valor obtenido indica la cantidad de veces que W_{2-3} es concatenado para la inserción. Las marcas de agua W_4 y W_{2-3} son permutadas mediante una llave de usuario y son concatenadas. El proceso de inserción de $[W_4\ W_{2-3}]$ se realiza mediante Eq. (1) y Eq. (2) en la sub-banda de frecuencia LH dentro de la ROE delimitada por I_{ROI}. Finalmente se realiza el proceso inverso de la DWT empleando las sub-bandas de frecuencia LL, HH y las sub-bandas marcadas LH y HL, obteniéndose así la imagen protegida.

3.2. Extracción de marcas de agua y detección de alteraciones

Esta etapa está dividida en dos sub-etapas: a) *Detección de alteraciones* y b) *extracción de marcas de agua*. Antes de realizar ambos procesos se aplica la DWT a la imagen DICOM marcada, posteriormente se aplica el sub-proceso de *detección de alteraciones* el cual consiste en tomar la sub-banda de frecuencia HL y aplicar la Eq. (1) obteniéndose el patrón binario *Q(f)*, este patrón representa con valores 0 las regiones auténticas de la imagen médica y con valor 1 las regiones que son sospechosas de alteración.

Posteriormente se aplica la sub-etapa de *extracción de marcas de agua*, la cual se realiza mediante los siguientes pasos, primero se extrae un total de 450 bits de la sub-banda de frecuencia LH mediante Eq. (1), los cuales corresponden a W_4, se aplica el proceso inverso de permutación mediante la llave de usuario (empleada durante la sub-etapa *inserción de las marcas de agua*) obteniéndose así cinco copias del vector $W_4 = [S_{W2}\ S_{W3}\ x_1\ y_1\ x_2\ y_2]$, se genera una matriz *M* de tamaño 90x5 en la cual cada fila contiene la información extraída de cada copia de W_4, finalmente, con el fin de generar una copia fiel de W_4 se aplica la siguiente ecuación:

$$W_{N_i} = \frac{2}{B}\sum_{j=1}^{\frac{B}{2}} M_{i,j}\,,\ \ 1 \le i \le 5, \tag{4}$$

donde W_{N_i} representa la *i-esima* posición de la copia fiel extraída de W_4.

Para realizar la extracción de las marcas de agua restantes se procede a calcular la cantidad de bits a extraer de la imagen marcada, este valor se obtiene mediante el siguiente cálculo (ecuación (5)):

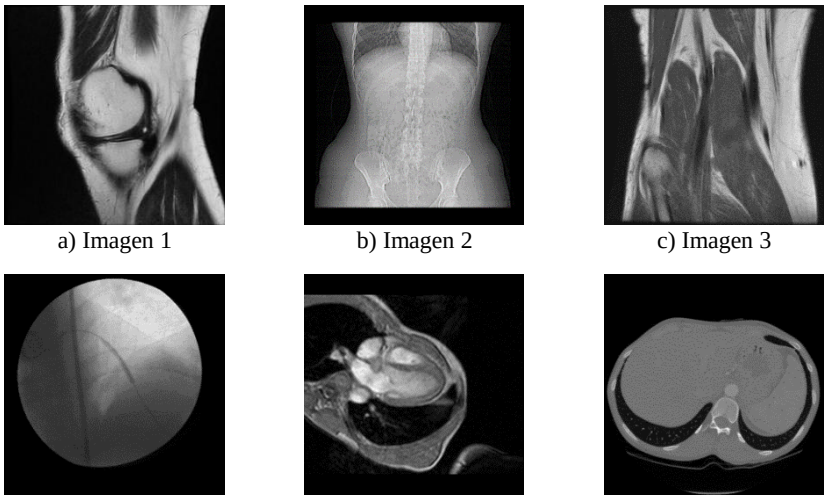
$$totalData = \alpha(S_{W2} + S_{W3}), \tag{5}$$

donde α representa la cantidad de copias que se insertaron, este valor es obtenido mediante $\lfloor totbits/(S_{W2} + S_{W3}) \rfloor$ donde $totbits$ es obtenido mediante la ecuación (3), empleando las coordenadas extraídas en la copia fiel de W_4. Una vez extraído $totalData$ bits, se aplica el proceso inverso de permutación mediante la llave de usuario, obteniéndose la concatenación de W_{2-3}, se genera una matriz *M* de tamaño αx$(S_{W2} + S_{W3})$ y se copia la información de W_{2-3}, donde cada fila contiene la información de una copia de S_{W2-3} y finalmente se aplica la ecuación (4) para obtener una copia fiel de S_{W2-3}. Empleando esta copia, se sabe que contiene dos vectores de marca de agua de tamaño S_{W2} y S_{W3} respectivamente, estos vectores son generados, donde el primero es transformado mediante código ASCII a texto y el segundo vector el cual contiene 24 bits es transformado de binario a decimal. Estas marcas de agua extraídas representan los EPR y el ID del médico respectivamente.

4. Evaluación y resultados

Durante el desarrollo del sistema propuesto se emplearon dos valores distintos de Δ, el primero Δ_1 fue empleado para insertar los bits de autenticación en la sub-banda de frecuencia HL, el segundo Δ_2 fue empleado para insertar los bits de marca de agua en la sub-banda de frecuencia LH. El sistema propuesto fue evaluado tomando en consideración tres características importantes:

1. Calidad de la imagen en formato DICOM marcada empleando diversos valores de Δ_2 durante la inserción de la marca de agua.



a) Imagen 1 b) Imagen 2 c) Imagen 3

d) Imagen 4 e) Imagen 5 f) Imagen 6

Fig. 4. Imágenes empleadas durante las pruebas realizadas.

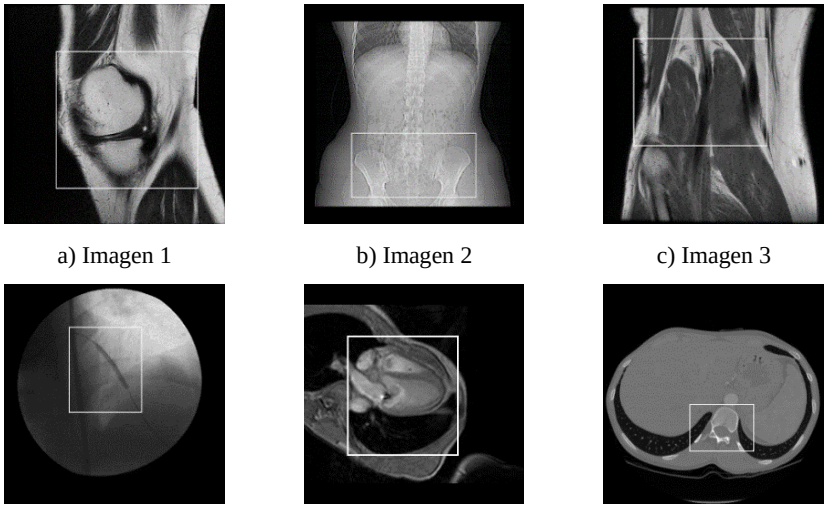
Tabla 1. Características de las imágenes utilizadas.

Imagen	Tamaño	Capas	Profundidad en bits	ROI
Imagen 1	512x512	1	12	40.28%
Imagen 2	512x512	1	8	16.59%
Imagen 3	512x512	1	13	29.56%
Imagen 4	512x512	12	8	12.97%
Imagen 5	256x256	16	8	27.77%
Imagen 6	512x512	1	12	6.29%

2. Extracción de las marcas de agua bajo ataques no intencionales de compresión en la imagen en formato DICOM.
3. Detección de alteraciones bajo diversos ataques intencionales de modificación de la imagen DICOM.

Se emplearon diversas imágenes con distintos niveles de profundidad en bits. La Figura 4 muestra las imágenes empleadas durante las pruebas realizadas. Asimismo, se utilizaron algunas imágenes en formato DICOM con múltiples capas (véase Fig. 4 (d) y (e)).

La ROI seleccionada para cada imagen es mostrada en la Figura 5. Las características de las imágenes utilizadas se muestran en la Tabla 1, como se puede observar, las características de la imagen DICOM puede variar significativamente, obteniéndose distinto tamaño en filas y columnas, diversas capas de imágenes y una distinta profundidad en bits para representar las tonalidades de la imagen, la ROI seleccionada abarca distintos porcentajes de la imagen lo cual puede afectar a la calidad de la misma.



a) Imagen 1 b) Imagen 2 c) Imagen 3

d) Imagen 4 e) Imagen 5 e) Imagen 6

Fig. 5. ROI seleccionada para cada imagen.

Las marcas de agua empleadas durante las pruebas son las siguientes, W_2 consiste en un archivo de texto de tamaño 577 bytes, así mismo la marca de agua W_1 consiste en la serie numérica '1234567'.

4.1. Calidad de la imagen marcada

En esta etapa se evaluó la calidad de la imagen marcada en términos de PSNR (dB), obteniéndose esta métrica de calidad comparando la imagen protegida contra la imagen original. Para realizar esta prueba se utilizó un valor $\Delta_1 = 2$, esto debido a que los bits de marca de agua para autenticación requieren ser frágiles ante alteraciones, por otra parte, se realizó el proceso de inserción empleando diversos valores de Δ_2 analizando los valores óptimos para cada imagen. La Figura 6 muestra los resultados obtenidos durante la evaluación de la calidad empleando múltiples valores de Δ_2.

Como se puede observar, la calidad para cada imagen tiene un comportamiento similar empleando diversos valores de Δ_2, la diferencia radica en que de acuerdo a los bits de profundidad la calidad será mayor o menor. Esto significa que para imágenes con un mayor nivel de bits de profundidad se obtendrá una calidad mayor a diferencia de las imágenes que poseen un menor nivel de bits de profundidad.

Por lo tanto se establecieron los valores de Δ_2 para cada imagen utilizada, para imágenes con un nivel de bits de profundidad de 8 se seleccionó un valor $\Delta_2 = 4$, esto debido a que con este valor la calidad de la imagen obtiene un PSNR mayor a 38dB. Posteriormente, para imágenes con un nivel de profundidad superior a 12 bits se seleccionó un valor $\Delta_2 = 150$, ya que con este valor se obtiene una calidad superior a 40 dB.

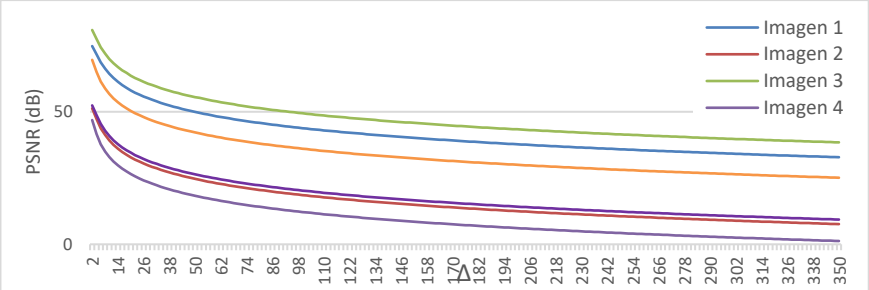


Fig. 6. Calidad de imagen DICOM marcada empleando diversos valores de Δ_2.

Tabla 2. Calidad (PSNR) de las imágenes marcadas para los valores de Δ_2 seleccionados.

Imagen	Δ_1	Δ_2	PSNR(dB) ROI	PSNR(dB) Toda la imagen	Redundancia insertada
Imagen 1	2	150	75.27	40.21	8
Imagen 2	2	4	50.23	47.22	11
Imagen 3	2	150	64.96	45.83	9
Imagen 4	2	4	45.90	39.77	12
Imagen 5	2	4	50.21	46.45	2
Imagen 6	2	150	69.24	32.44	13

La tabla 2 muestra a detalle los resultados para las imágenes de acuerdo a los valores de Δ_2 seleccionados anteriormente, es importante mencionar que la calidad para la Imagen 4 e Imagen 5 es el promedio de todas sus capas.

Como se puede observar la calidad de la ROI siempre se mantiene superior a la calidad de toda la imagen marcada, esto se debe a que la ROI únicamente es marcada con los bits de detección de alteraciones empleando un valor de Δ_1 mínimo, mientras que la ROE es marcada con los bits de detección de alteraciones y con las marcas de agua W_2, W_3 y W_4.

4.2. Extracción de marcas de agua bajo ataque de compresión

En esta etapa se evaluó la capacidad del sistema propuesto para extraer las marcas de agua bajo ataques de compresión. Estos ataques no modifican la información visual de la imagen DICOM, y tienden a mantener una calidad aceptable en la imagen comprimida. La tabla 3 muestra los resultados en términos de NCC para la calidad de la marca de agua W_2 extraída bajo distintos ataques de compresión. El proceso de compresión fue llevado a cabo mediante el software MatLab®.

Como se puede observar el sistema propuesto es capaz de extraer correctamente la marca de agua que contiene la información del paciente (W_2), únicamente existe una pequeña perdida con el proceso de compresión JPEG con perdida. Cabe destacar que la marca de agua W_3 se extrae en todos los casos de manera correcta (‘1234567’).

Tabla 3. Calidad de la marca de agua W_2.

Imagen	JPEG2000 'lossy'	JPEG2000 'lossless'	JPEG 'lossy'	JPEG 'lossless'	RLE
Imagen 1	1	1	0.9923	1	1
Imagen 2	1	1	0.9912	1	1
Imagen 3	1	1	0.9863	1	1
Imagen 4	1	1	0.9892	1	1
Imagen 5	1	1	0.9935	1	1
Imagen 6	1	1	0.9921	1	1

4.3. Detección de alteraciones bajo ataques intencionales

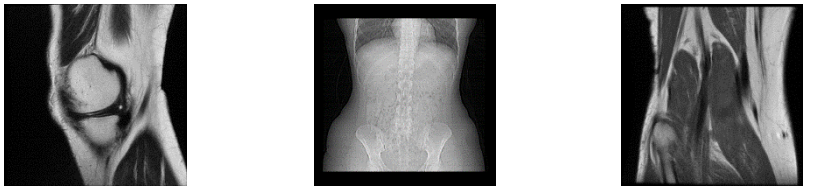
La última prueba realizada es la detección de alteraciones bajo distintos ataques de procesamiento de imágenes, específicamente se realizaron dos ataques: emborronamiento y adición de ruido Gaussiano. Debido a que este tipo de ataques

degradan significativamente la calidad de la imagen, después de realizar la fase de detección de alteraciones se observa que existe una gran cantidad de modificaciones en las imágenes, por lo tanto, las marcas de agua W_2, W_3 y W_4 se consideran sospechosas de alteración, por lo tanto, no son tomadas en consideración para evitar futuros diagnósticos médicos erróneos.

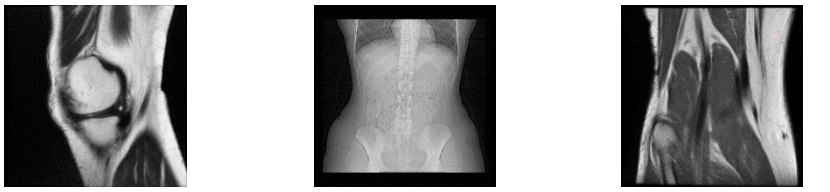
Las modificaciones fueron realizadas con el software Photoshop®. La Figura 7 y 8 muestran los resultados obtenidos para los ataques de *emborronamiento* y *adición de ruido* respectivamente empleando las imágenes 1-3. El tipo de emborronamiento es mediante una distribución Gaussiana con una ventana de 3 pixeles y el ruido insertado es mediante una distribución uniforme a una cantidad del 5%.

Como se puede observar, el método propuesto detecta correctamente las alteraciones que se llevaron a cabo para cada imagen, esto se debe al valor empleado en Δ_1, ya que los sistemas actuales en la literatura de detección de alteraciones en imágenes mencionan que es necesario el uso de marcas de agua frágiles para detectar alteraciones, en este método se empleó un esquema semi-frágil, el cual al asignarse un valor en Δ_1 muy pequeño, el comportamiento de la marca de agua de autenticación insertada es parecido al de un esquema de marcado de agua frágil.

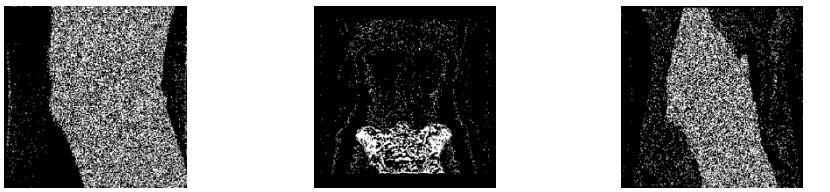
Finalmente se realizaron ataques intencionales para alterar de manera significativa el contenido de las imágenes médicas 4-6, estas modificaciones consisten en ataques de collage y emborronamiento a ciertas regiones de interés, finalmente se almacenó la imagen DICOM con compresión JPEG con perdida. La Figura 9 muestra los resultados para las detecciones realizadas en estas imágenes.



a) Imagen 1 sin alterar b) Imagen 2 sin alterar c) Imagen 3 sin alterar



d) Imagen 1 alterada e) Imagen 2 alterada f) Imagen 3 alterada



g) detecciones obtenidas h) detecciones obtenidas i) detecciones obtenidas

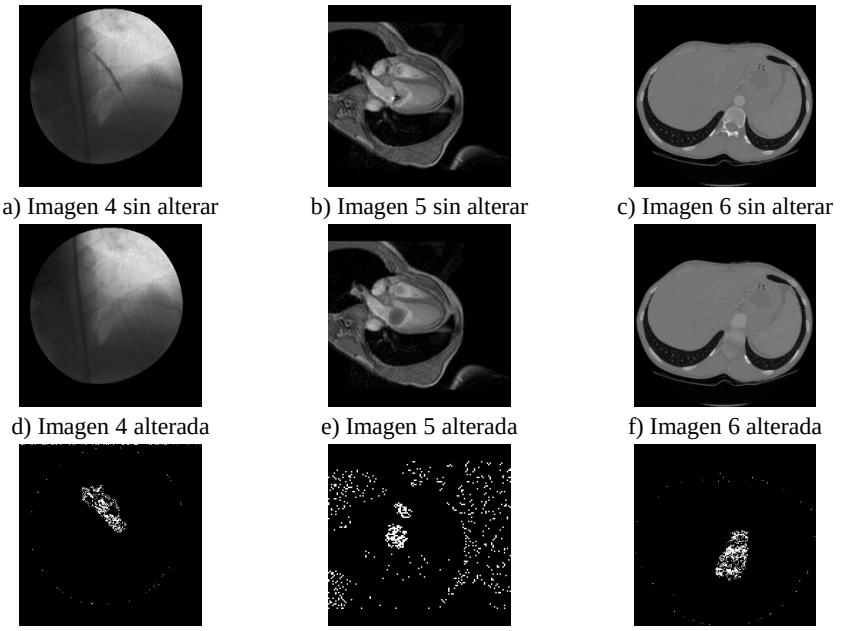
Fig. 7. Resultados durante la detección de alteraciones para ataques de emborronamiento.

a) Imagen 1 sin alterar b) Imagen 2 sin alterar c) Imagen 3 sin alterar

d) Imagen 1 alterada e) Imagen 2 alterada f) Imagen 3 alterada

g) detecciones obtenidas h) detecciones obtenidas i) detecciones obtenidas

Fig. 8. Resultados durante la detección de alteraciones para ataques de adición de ruido.



a) Imagen 4 sin alterar b) Imagen 5 sin alterar c) Imagen 6 sin alterar

d) Imagen 4 alterada e) Imagen 5 alterada f) Imagen 6 alterada

g) detecciones obtenidas h) detecciones obtenidas i) detecciones obtenidas

Fig. 9. Resultados durante la detección de alteraciones para ataques de adición de ruido.

5. Conclusiones

En el presente trabajo se propone un método para la protección de los datos personales de un paciente, los cuales son insertados como marca de agua dentro de una imagen médica en formato DICOM. Así mismo se realiza la inserción de un identificador del médico y una serie de bits empleados para detección de alteraciones, esto se realiza con el fin de verificar la autenticidad de la imagen medica durante el proceso de extracción de marcas de agua, ya que en caso de que se detecten alteraciones, el procedimiento de extracción podría considerarse incorrecto o poco confiable, así mismo se considera a la imagen como no apta para su análisis en algún diagnóstico médico.

El método propuesto está basado en marcas de agua en el dominio de la frecuencia, insertando la información mediante el uso de la DWT en el primer nivel de descomposición, donde los bits de marca de agua de detección de alteraciones son insertados en la sub-banda de frecuencia HL, mientras que la información de los datos del paciente y la firma del médico es insertada dentro de una ROE en la sub-banda de frecuencia LH.

Los resultados experimentales muestran que el sistema propuesto obtiene una calidad aceptable en las imágenes protegidas, superior a 40dB en la imagen completa y superior a 45 dB en la ROI, se tomó en consideración la evaluación por separado de la calidad debido a que es importante que la calidad de la ROI seleccionada por el médico

se degrade lo menos posible. Por otra parte, el sistema propuesto puede extraer de manera correcta la información insertada como marca de agua (datos del paciente e identificador del médico) ante ataques no intencionales como compresión, esto es una ventaja debido a que algunos de estos ataques no degradan de manera significativa la calidad de la imagen. Finalmente, se demostró que el esquema propuesto es efectivo al detectar alteraciones como adición de ruido o emborronamiento, a pesar de que estas modificaciones no degraden de manera significativa el contenido de la imagen médica.

Agradecimientos. Agradecemos al Instituto Politécnico Nacional (IPN), al Consejo Nacional de Ciencia y Tecnología de México (CONACyT, proyecto 220347), a la Comisión de Operación y Fomento de Actividades Académicas (COFAA) del IPN y a la Beca de Estimulo Institucional de Formación de Investigadores (BEIFI) del IPN por el apoyo otorgado para el desarrollo de este trabajo.

Referencias

1. DICOM Library: https://www.dicomlibrary.com/ (2018)
2. Gungal, B. L., Mali, S. N.: ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine. Int. J. of Comp. and Inf. Eng. 6(8), pp. 997–1002 (2012)
3. ISO: Health Information – pseudonymisation, Technical Report 25237, https://www.iso.org/obp/ui/#iso:std:iso:ts:25237:ed-1:1:en (2018)
4. Liu, Y., Qu, X., Xin, G., Liu, P.: ROI Based Reversible Data Hiding Schema for Medical Image with Tamper Detection. IEICE Trans. on Inf. and Systems, E98(4), pp. 769–774 (2015)
5. Coatrieux, G., Lecornu, L., Sankur, B.: A review watermarking applications in healthcare. In: 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 4691–4694 (2006)
6. Diario Oficial de la Federación: http://dof.gob.mx/nota_detalle_popup.php?codigo=5272787 (2018)
7. Arsalan, M., Quresh, A. S., Khon, A., Rajarajan, M.: Protection of medical and patient related information in healthcare: Using an intelligent and reversible watermarking technique. Applied Soft Computing 51, pp. 168–179 (2017)
8. Thankar, F. N., Srivastava, V. K.: A blind image watermarking: DWR-SVD based robust and secure approach for telemedicine applications. Mult. Tools and App. 76(3), pp. 3669–3697 (2017)
9. Sharma, A., Singh, A. K., Ghrera, S. P.: Robust and Secure Multiple Watermarking for Medical Images. Wireless Personal Communications 92(4), pp. 1611–1624 (2017)
10. Moniruzzaman, M. D., Hawlader, A. K., Hossain, M. F.: Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Image for Medical Image Authentication. In: 17th International Conference on Computer and Information Technology, pp. 374–378 (2014)
11. Badshah, G., Liew, S. C., Zain, J. M., Ali, M.: Watermark Compression in Medical Image Watermarking Using Lempel-Ziv-Welch (LZW) Lossless Compression Technique. Journal of Digital Imaging, pp. 216–225 (2016)

12. Singh, A. K., Kumar, B., Sing, S. K., Ghrera, S. P., Mohan, A.: Multiple Watermarking Technique for Securing Online Social Network Contents Using Back Propagation Neuronal Network. In: Future Generation Computer Systems 86 (2016)
13. Singh, A. K., Dave, M., Mohan, A.: Hybrid technique for robust and imperceptible multiple watermarking using medical images. Mult. Tools and Appl. 75(14), pp. 8381–8401 (2015)
14. Giakoumaki, A., Pavlopoulo, S., Koutsouris, D.: A multiple watermarking scheme applied to medical image management. In: Conf. Proc. IEEE Engineering in Medicine and Biology Society, 2, pp. 3241–3244 (2004)