UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido

http: revistas.udistrital.edu.co/ojs/index.php/visele/index

VISIÓN ELECTRÓNICA

VISIÓN INVESTIGADORA

Sistema para la creación y autenticación de credenciales

System for creating and authentication credentials

***Marco Antonio Abarca Rodríguez*[a], *Mariko Nakano Miyatake*[b], *Hector Manuel Pérez Meana*[c]**

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Enviado: Octubre 2014
Recibido: Noviembre 2014
Aceptado: Noviembre 2014

Palabras clave:
Tarjeta de identificación segura
Transformada Coseno Discreta (TCD)
Autenticación
Robustez
Seguridad

Keywords:
Card secure identification
Discrete Cosine Transform (DCT)
Authentication
Robustness
Security

RESUMEN

El presente artículo describe un sistema para creación y autenticación de credenciales de identificación personal (ID) seguras, utilizando como códigos de barras unidimensionales y bidimensionales, cifrado de datos con llave simétrica y una técnica de marca de agua. Para ello, se inserta una marca de agua en la fotografía del usuario, generada a partir de un código único de identificación que estará disponible en la credencial impresa, de forma que al momento de realizar la validación de la misma se lleve a cabo calculando la correlación cruzada entre la marca de agua contenida en la fotografía del usuario y la marca de agua calculada al momento de la validación usando el mismo código único de identificación. Se demuestra que una adecuada selección de los parámetros de inserción de la marca de agua: longitud, ganancia, posición, y umbral de decisión, son indispensables para asegurar el adecuado funcionamiento del esquema propuesto, con calidad suficiente en la imagen para hacer el reconocimiento visual del usuario, y suficientemente robusto para soportar el ataque de conversión de digital-analógico (D/A) y de analógico-digital (A/D).

ABSTRACT

This article present a system for creating and credential authentication personal identification (ID) safe, using one-dimensional and two-dimensional barcodes, data encryption and symmetric key technique watermark. To do this, a watermark is inserted on the photo of the user, generated from a unique identification code which will be available in printed credential so that at the time of validation of the credential is carried by calculating the cross-correlation between the watermark contained in the photograph of the user and the

[a]Ingeniero Telemático, Instituto Politécnico Nacional UPIITA, México. Maestro en Ingeniería en Seguridad y Tecnologías de la Información, Instituto Politécnico Nacional ESIME, México. Docente Universidad Politécnica de Texcoco, México. e-mail: marco.a.abarca.r@gmail.com, academiaelectronicauptex@gmail.com.

[b]Licenciatura en ingeniería, The university of Electro Communications, Tokyo, Japan. Maestría en Ingeniería, The University of Electro Communications, Tokyo, Japan. Doctorado en Ciencias, Universidad Autónoma Metropolitana, Unidad Iztapalapa, México. Docente Instituto Politécnico Nacional ESIME Unidad Culhuacán, México. e-mail: mnakano@ipn.mx

[c]Licenciatura en Ingeniería Electrónica, Universidad Autónoma Metropolitana, México. Maestría en Ingeniería , The University of Electro-Communications, Tokio Japan. Doctorado en Ingeniería, The Tokyo Institute of Technology, Tokio Japan. Docente Instituto Politécnico Nacional ESIME Unidad Culhuacán, México. e-mail: hmperezm@ipn.mx

Citar este artículo como: M. A. Abarca, M. Nakano & H. M. Pérez, "Creación y autenticación de credenciales usando marca de agua y tcd" . Visión Electrónica, algo más que un estado sólido, Vol. 8, No. 2, pinicial-pfinal, julio-diciembre 2014.

watermark calculated at the time of validation using the same unique identification code. We show that proper selection of parameters for inserting the watermark: length, gain, position of the watermark and decision threshold, are essential to ensure the proper functioning of the proposed scheme, ensuring maintain sufficient quality in visual image to the user recognition and in turn be robust enough to withstand the attack of converting digital-analog (D / A) and analog-digital (A/D).

1. Introducción

Actualmente, la seguridad en la información se ha convertido en uno de los principales retos afrontados por la comunidad informática, ya que es importante que la información que se maneje sea confidencial y que esté disponible solo para quienes están autorizados a acceder a ella, y a la vez restringida para personas ajenas a la organización dueña de los recursos. La percepción actual de un sistema de información (SI), implica que, además de brindar confidencialidad, disponibilidad e integridad a la misma, se deba tomar en cuenta la seguridad de los recursos de la empresa en general, el equipo humano que interactúa con ellos y las actividades que se realizan en la organización, para poder así garantizar la seguridad de todo el sistema. Anteriormente, este tipo de control se realizaba mediante la presencia física; sin embargo, a medida que estos sistemas han sido reemplazados por sistemas de gestión de identidad electrónicos, surge la necesidad de nuevas soluciones para garantizar la seguridad y el control de acceso en un punto importante.

Uno de los métodos de identificación utilizados comúnmente, tanto en los sistemas tradicionales como automatizados, se basa en las credenciales de identificación impresas, las cuales incluyen los datos del usuario y una fotografía para realizar el reconocimiento visual de quien porta la credencial; y, en algunos casos, elementos que buscan incrementar la seguridad o la practicidad de su uso, como son las imágenes ultravioletas o los códigos de barras.

Existen sistemas de autenticación mediante tarjetas seguras de identificación que incluyen tecnologías como: RFID, tarjetas con chip y tarjetas JAVA, utilizadas principalmente en Estados Unidos y en algunos países de la Unión Europea [1]; estos sistemas utilizan códigos de clave e información adicional, además de la información personal y la imagen del titular de la tarjeta, para aumentar la seguridad; estas tecnologías, al ser relativamente nuevas, tienen algunas ventajas ya que aún no han sido completamente exploradas o comercializadas y los equipos para la creación y validación son costosos; pero, a su vez, el equipo especial para la lectura y escritura de los módulos de RFID o chips y el mantenimiento especializado que requiere este tipo de sistemas representa también una desventaja, por los altos costos de implementación [1].

Tomando en cuenta los inconvenientes anteriormente mencionados, se propone un método de autenticación mediante tarjetas de identificación para tener acceso a lugares o información restringida y que mantenga un equilibrio entre la seguridad que brinda y el costo que representa, lo cual haría de dicho sistema una opción viable para su aplicación.

El sistema propuesto en el presente documento muestra una opción en la cual no se requiere hardware especial, únicamente una impresora de tarjetas convencional para crear la credencial y un escáner convencional para realizar la autenticación de la credencial, ya que el procesamiento de la imagen para la validación de la marca de agua se realiza mediante software que puede ser ejecutado en cualquier PC, lo cual reduce el costo de operación con respecto a las tecnologías anteriormente mencionadas, pues en ocasiones se cuenta con este equipo en los controles de acceso usados actualmente.

Las técnicas de marca de agua han sido consideradas como solución viable para la protección de derechos de autor; hasta ahora, se han propuesto varios métodos que operan, tanto en el dominio espacial [2, 3] como en el dominio de la frecuencia [4–6], para la validación de imágenes digitales.

De forma general, las técnicas de marca de agua en el dominio de la frecuencia muestran mayor robustez para algunos ataques comunes, tales como compresión, filtración, o modificaciones geométricas; es por ello que son más comúnmente utilizadas [4, 5, 6]; sin embargo, muy pocos algoritmos de marca de agua son resistentes a ataques que impliquen transformación de digital a analógico (D/A y A/D) ya que estos introducen una distorsión mayor en relación a los contenidos puramente digitales.

No obstante, en las tareas de autenticación mediante tarjetas, este último tipo de ataque debe ser considerado ya que las tarjetas de identificación son objetos análogos en los cuales se va a imprimir la información, en este caso la fotografía en la cual fue embebida la marca de agua, y dicha información era digital hasta el momento en que fue impresa (D/A); y cuando se requiere validar la autenticidad de la credencial, se deberá escanear la misma para transformar la información de analógica a digital (A/D) y así realizar el procesamiento de la información y validar tanto la autenticidad de la marca de agua como la del documento. Además, la detección de la marca de

agua debe llevarse a cabo sin datos adicionales a la tarjeta misma (Detección ciega). Por lo tanto, el cumplimiento de estos requisitos representa un reto a superar si se piensa desarrollar un esquema de identificación seguro y confiable basado en técnicas de marca de agua.

En el presente trabajo de investigación, se presenta un esquema para la aplicación de un sistema que se encarga del diseño, creación y validación de credenciales de identificación por medio de la técnica de una marca de agua que debe ser robusta a los ataques antes mencionados. Se demuestra, en la práctica, que los algoritmos de marca de agua representan una opción real para la autenticación de documentos impresos, conservando un equilibrio entre la calidad visual del documento y la robustez de la marca mediante el ajuste adecuado de los parámetros implicados: energía de inserción, longitud de la marca de agua, y la posición de la inserción. También se muestra el uso del algoritmo de marca de agua propuesto, en el diseño y creación de una identificación con fotografía segura, de forma práctica, por lo cual todas las evaluaciones realizadas de las tarjetas se llevan a cabo con credenciales de identificación reales, una impresora de credenciales de PVC y un escáner convencional.

El artículo se estructura de la siguiente manera: en la sección 1.1. Se muestran algunas técnicas utilizadas en otros países para brindar mayor seguridad en las credenciales de identificación y algunos de los sistemas comerciales utilizados para el diseño y creación de las mismas. En la sección 2 se muestra el marco teórico; en la sección 3 se muestran los materiales y métodos del desarrollo, comenzando con el algoritmo de marca de agua, seguido de las pruebas realizadas desde la inserción, detección y autenticación de la marca, y el sistema que se desarrolló para crear las credenciales, incluyendo el algoritmo de marca de agua propuesto. Por último, en la sección 4, se presentan las conclusiones.

2. Marco teórico

2.1. Tecnología para seguridad en credenciales

2.1.1. Tarjetas inteligentes

Se conocen como tarjetas inteligentes aquellas cuyos microprocesadores cumplen algunas propiedades específicas: seguridad del procesador criptográfico, seguridad del sistema de archivos, y provisión de confidencialidad a la información guardada en la memoria [1].

2.1.2. Tarjetas JAVA

Una tarjeta java es una tarjeta inteligente con un circuito integrado que permite la ejecución de pequeñas aplicaciones o applets, que son programadas en el microprocesador de la tarjeta; estas se programan conforme a la tecnología java.

2.1.3. Tarjetas de identificación por radiofrecuencia (RFID)

Las tarjetas de identificación por RFID, son dispositivos que almacenan y recuperan datos de forma remota, su propósito fundamental es transmitir la identidad del objeto mediante ondas de radio. Contienen antenas que les permiten recibir y responder a peticiones por radiofrecuencia, desde un emisor y receptor de RFID; algunas de ellas son pasivas pues no requieren alimentación eléctrica interna, y las que si lo requieren se denominan activas [7].

2.2. Mecanismos actuales de seguridad empleados en tarjetas

2.2.1. Códigos de barra

El código de barras es un sistema de codificación utilizado para cifrar información en una serie de barras de diferentes grosores y entre sus espacios.

Existen varias codificaciones que son compatibles y aceptadas internacionalmente: CODABAR, CODE 39, UCC/EAN-128, CÓDIGO PDF 417 y códigos QR.

2.2.2. Imágenes impresas con tinta ultravioleta

Son empleadas como medida para verificar la autenticidad de los documentos, este tipo de imágenes se imprimen con una tinta especial que es invisible, a menos que dicho documento sea expuesto a luz ultravioleta. En general, se puede imprimir cualquier imagen o información adicional con esta tinta; la seguridad que esto representa, dependerá de que la persona que desee falsificar algún documento no cuente: con impresoras que soporten este tipo de impresión, y con la información necesaria[1].

2.2.3. Holograma

Estos son marcas de agua visibles que se imprimen de manera tenue en alguna sección específica de los documentos o credenciales, y que se pueden detectar a simple vista si la persona pone atención en el lugar específico donde se realizó la impresión; la seguridad que esto representa se deberá a la complejidad de generar una imagen exactamente igual a la original, sin saber cómo esta se generó.

[1]La información presentada se obtuvo de la página oficial del Instituto Federal Electoral (IFE) http://www.ife.org.mx/documentos /DERFE/RFE2/cred/CredencialVotar_anverso.swf

2.2.4. *Micro texto*

Son textos que se imprimen de forma muy pequeña dentro de imágenes u hologramas y que resultan imposibles de ser detectados a simple vista; sirven para verificar la autenticidad de los documentos y se requieren, para poder imprimirlos, dispositivos especiales de alta resolución.

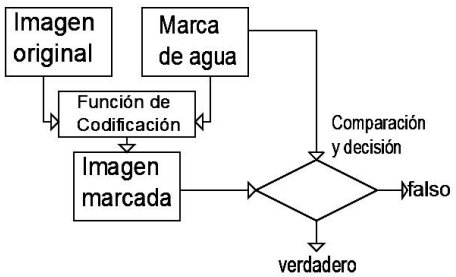
2.2.5. *Bandas magnéticas*

Son tarjetas de policarbonato o PVC, similares tarjetas convencionales y de RFID, que contienen una banda magnética en la cual se graba algún código de identificación. Este tipo de tarjetas poseen la ventaja de que la información puede ser obtenida de forma rápida; sin embargo, la seguridad que representa depende de los métodos que se hayan utilizado para cifrar dicha información y del entorno en que esta se utilice [8].

2.3. *Marca de agua*

Una marca de agua es una derivación de la estenografía - arte de comunicar de manera secreta un mensaje que está oculto en alguna otra información-, han sido utilizadas ampliamente para verificar la autenticidad de documentos o de la información que estos contienen.

Figura 1. Proceso de inserción y validación de la marca de agua.



Fuente: elaboración propia.

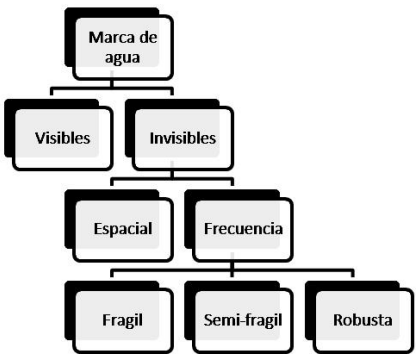
Dependiendo de las aplicaciones, las marcas de agua se pueden generar de diferentes maneras, buscando siempre que tengan las características necesarias para cada aplicación en particular; la inserción de la marca de agua, una vez que esta fue generada en la información, se hace mediante de la función de codificación; y, una vez que se requiere validar la autenticidad de la marca, se tiene que aplicar la función de codificación y comparación con algún parámetro preestablecido para tomar la decisión de si el documento es original o ha sido alterado, el diagrama bloques de dicho proceso se muestra en la figura 1 [9, 10].

2.3.1. *Generación, función de codificación, decodificación y tipos de marca de agua*

Las marcas de agua digitales son secuencias pseudo aleatorias de menor energía que la imagen a la cual se aplicará con el fin de que esta sea menos notoria. La función de codificación se representa como $E(I, W) = I'$, donde I es la imagen, W es la marca de agua e I' se denomina imagen marcada. Dicha función modifica la información de la imagen original en términos de cada bit de la secuencia de la marca de agua, para generar la imagen marcada; el tamaño máximo de la secuencia de marca de agua será igual al número de bits que se tienen en la imagen.

Para verificar si una imagen es auténtica, se tiene una función de decodificación D; teniendo una imagen que puede contener o no una marca de agua, de la cual se necesita saber si es auténtica, dicha función realiza la comparación de la imagen J con algún parámetro preestablecido que puede ser la versión original de la imagen I o con la marca de agua en caso de que dicha imagen la tenga. Los tipos de marcas de agua se presentan en la Figura 2.

Figura 2. Tipos de marca de agua.



Fuente: elaboración propia.

2.3.2. *Requisitos, aplicaciones y ataques de marca de agua*

Los requisitos de un sistema basado en marca de agua son: seguridad, imperceptibilidad, robustez, facilidad de detección y detección no ambigua. Algunos de los propósitos de las marcas de agua pueden ser: la autenticación de contenido, la protección de propiedad intelectual, e incluso la recuperación de algún material que fue modificado.

Dependiendo de la función práctica que tenga la marca de agua, esta puede ser sometida a diversos ataques inherentes al proceso de inserción, detección, o al manejo que se le de a la información marcada; algunos

de los ataques más comunes son: compresión, contaminación por ruido, distorsiones geométricas (rotación, escalamiento y recorte), filtrado y compensación gamma, y alteraciones digitales.

3. Materiales y Métodos

3.1. Marca de agua

La marca de agua que se utiliza en el algoritmo propuesto es binaria, es decir: sus únicos valores posibles son -1 y 1; para que cumpla con las condiciones mencionadas en la sección 2, la mitad de los elementos de la marca de agua deben ser -1 y la otra mitad 1; cabe mencionar que no es la única forma de cumplir con esos requisitos, por ejemplo: una función gaussiana normalizada también los cumple; sin embargo, se obtienen mejores resultados usando marcas de agua binarias, [12].

Dado que se trabajará con contenidos digitales, puede considerarse la marca de agua como un vector de longitud N de la forma $X = \{x_1, x_2, x_3, \ldots, x_N\}$; dicha secuencia es necesario que sea única para cada usuario, por ello se usará como semilla para generar la secuencia pseudoaleatoria una función hash (SHA-1) [13] del identificador único del portador de la credencial (número de empleado, clave de registro, número de alumno, etc), el cual debe estar disponible impreso en la misma credencial para su validación cuando sea requerido y que, por motivos de seguridad, se propone que sea cifrado con la llave secreta de la empresa emisora de las credenciales, previo a la impresión de la tarjeta. Posterior a la función hash, se aplica una operación XOR a la secuencia binaria del identificador único de la tarjeta para generar una clave secreta que es única para cada identificación. Las operaciones están dadas por (1) y (2).

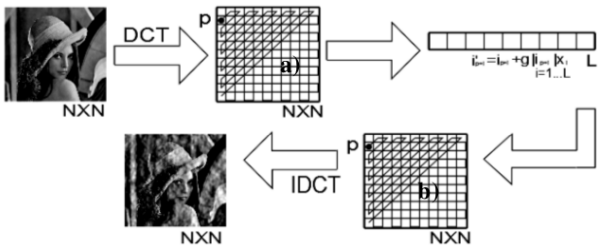
$$K = f_{HASH}(C_B) \tag{1}$$

$$\tilde{K} = k_1 \oplus k_2 \oplus \ldots k_{10} \tag{2}$$

Donde la función hash (SHA-1), es la representación binaria del identificador único. En (1) se obtiene la secuencia K de longitud fija de 160 bits, la cual se divide en 10 secuencias binarias de 16 bits de longitud cada una. Aplicando la operación XOR a las 10 secuencias binarias se obtiene $\tilde{K}$ cuyo valor esta entre [0, 216]. Usando K como llave única de usuario, se genera la marca de agua binaria.

El proceso de inserción de la marca de agua consiste en obtener una imagen digital y generar una marca de agua única para el usuario, para luego insertarla en la imagen en el dominio de la Transformada Coseno Discreta (DCT por sus siglas en inglés) en orden de zig-zag, como se puede visualizar en la Figura 3.

Figura 3. Proceso de inserción de la marca de agua. a) Bits originales que serán modificados, b) bits modificados insertados en la DCT.



Fuente: elaboración propia.

3.2. Algoritmo de detección y comparación

Para esta investigación, la detección de la marca de agua es ciega, es decir, que no requiere de la imagen original para la extracción y la comparación. Para calcular el valor de correlación cruzada entre la marca de agua detectada y la marca de agua calculada a partir de un número de identificación único se utiliza la ecuación 3.

$$C_c = \frac{1}{L} \sum_{i=1}^{L} x_i \, \tilde{i}_{p+i} \tag{3}$$

Donde C_c es el valor de la correlación cruzada, $\tilde{i}$ son los coeficientes de la DCT marcados y posiblemente distorsionados, x es la secuencia de marca de agua generada usando el identificador único, L es la longitud de la marca de agua y p es la posición inicial a partir de la cual se insertó la marca de agua.

Por último, el valor de la correlación cruzada es comparado con un umbral predefinido (Th), calculado por (5), a fin de minimizar la probabilidad de error de falso positivo y falso negativo. Si C_c es mayor al umbral se considera que la identificación es auténtica, de lo contrario, se considera falsa.

$$Th = \mu_d + K_p \sqrt{2\,\sigma_d^2} \tag{4}$$

Donde Th es igual al umbral, μ_d es la media de la gaussiana correspondiente a la señal sin marca de agua o con una marca de agua distinta; K_p es una constante calculada mediante la función de error que define el nivel de falsos positivos permisibles, de tal forma que puede adecuarse al valor requerido por algún estándar; y σ_d^2 es la varianza de la gaussiana correspondiente a la señal sin marca de agua o con marca de agua distinta, según el modelo estadístico del problema de falsas alarmas descrito en [1].

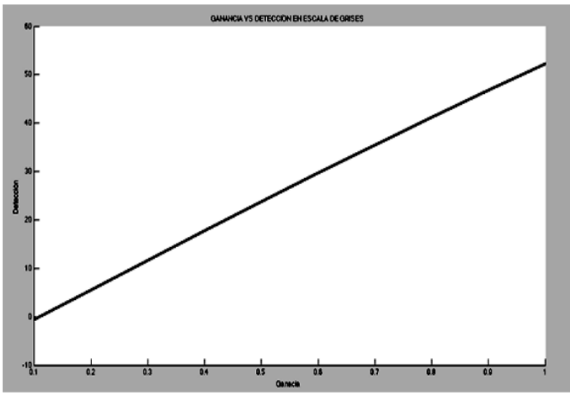
3.3. Pruebas realizadas

Para validar el funcionamiento del algoritmo de marca de agua propuesto, se crearon las credenciales con un sistema usando la plataforma JAVA y se validaron con un algoritmo creado con el entorno de MATLAB® con la intención de lograr el ajuste de los parámetros que están involucrados en el desempeño de la marca de agua (ganancia, longitud); se realizaron experimentos para analizar el efecto que tiene cada uno de los parámetros en términos de imperceptibilidad y robustez de la marca de agua, variando los parámetros.

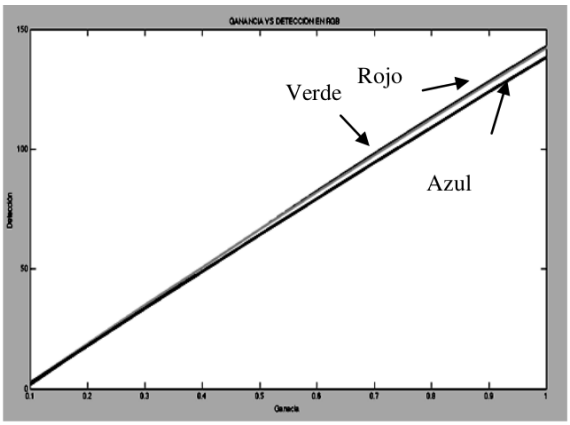
a. Ajuste de ganancia

En la Figura 4 a) se muestra la gráfica que corresponde a la diferencia entre la correlación cruzada y el valor de umbral (capacidad de detección) en función de la ganancia.

Figura 4. Ganancia vs. detección de a) escala de grises y b) sistema RGB.



a) Escala de grises



b) Sistema RGB

Fuente: elaboración propia.

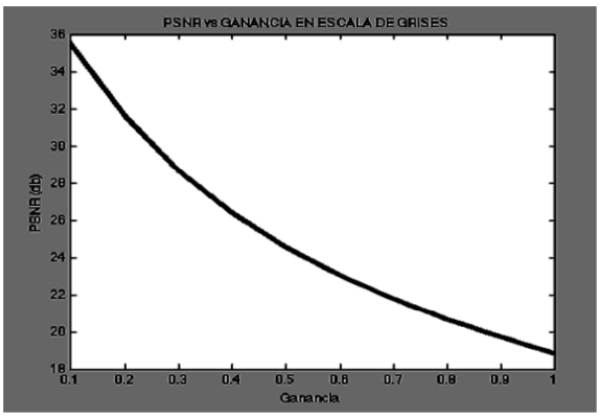
Se observa además que la relación entre la correlación cruzada y el valor de umbral es lineal, lo cual quiere decir que mientras mayor sea la ganancia mayor será la capacidad de detección de la marca.

b. Relación entre ganancia y distorsión de la imagen

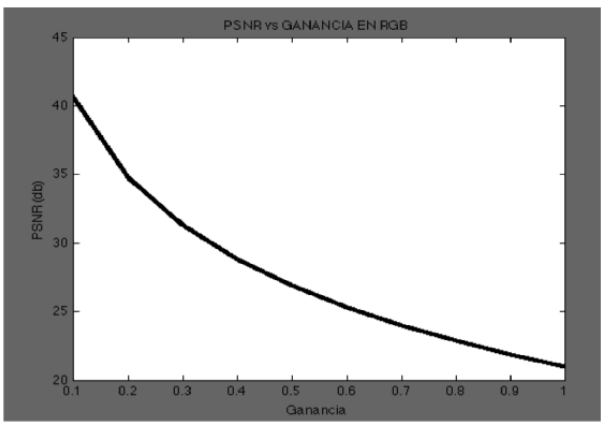
Ahora, se observa la relación entre el PSNR (dB) de las imágenes generadas, con respecto a la original, a diferentes valores de ganancia, y dejando fija la longitud en 3000 bits.

En la Figura 5 se muestra dicha función. Como se observa, la calidad de la imagen decae mientras aumenta la ganancia de inserción.

Figura 5. PSNR vs. Ganancia a) escala de grises b) Sistema RGB.



a) Ganancia en escala de grises



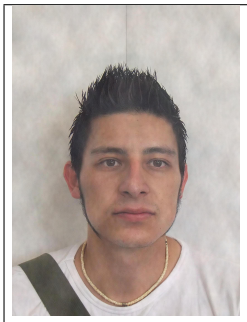
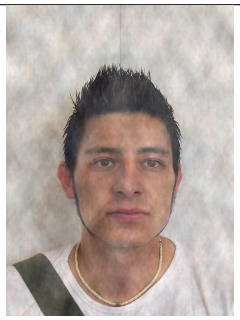
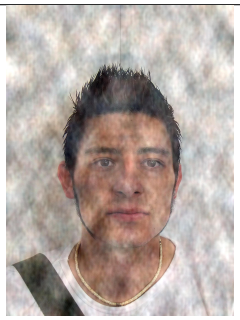
b) Ganancia en sistema RGB

Fuente: elaboración propia.

Tabla 1: Imágenes obtenidas ajustando las ganancias.

				
G= 0.1	G= 0.2	G=0.3	G=0.4	G=0.5
PSNR=35.6dB	PSNR=32 dB	PSNR=28 dB	PSNR=25.8 dB	PSNR=24 dB

a) Imágenes obtenidas insertando la marca en imágenes en escala de grises.

				
G= 0.2	G= 0.4	G=0.6	G=0.8	G=1.0
PSNR=34.73 dB	PSNR=28.80dB	PSNR=25.31 dB	PSNR=22.87 dB	PSNR=21.02 dB

b) Imágenes obtenidas insertando la marca en los tres canales de color

Fuente: elaboración propia

c. Imágenes obtenidas ajustando las ganancias

En la tabla 1 se muestran algunas de las imágenes obtenidas variando la ganancia de inserción de la marca de agua para compararlo con el PSNR , y apreciar el efecto visual sobre las imágenes marcadas, cabe mencionar que dichas imágenes fueron usadas así mismo para la obtención de las gráficas que se muestran en las figuras 4 y 5.

d. Creación y autenticación de la credencial

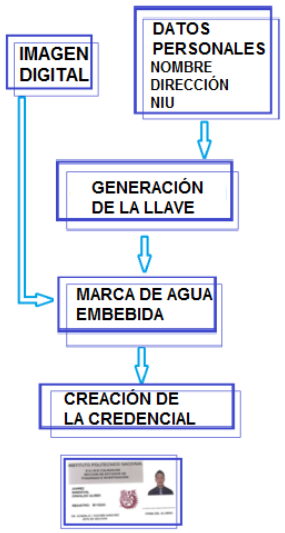
Para este apartado se describirá el proceso por el cual se realiza la creación de la credencial segura y la autenticación de la misma, por medio de técnicas en donde intervienen la generación y extracción de la marca de agua con diferentes valores de ganancia. En este artículo se propone una mejora de un sistema de autenticación de la tarjeta de identificación propuesto en [10, 11].

En la Figura 6 a) se muestra el diagrama para la creación de la credencial y en la Figura 6 b) el diagrama que describe el proceso de autenticación de la credencial.

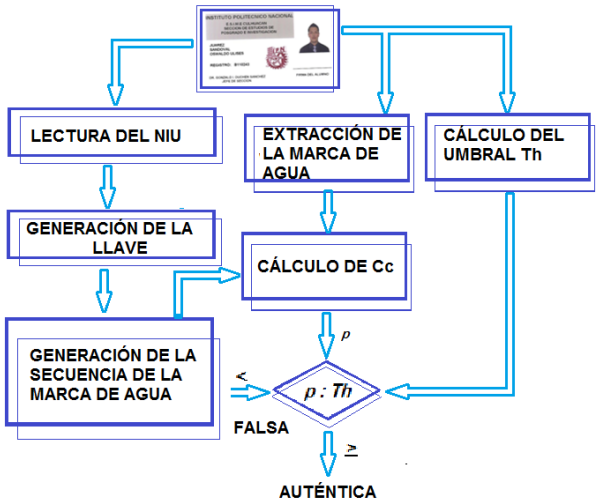
En la etapa de creación de las credenciales (Figura 6 a)) utilizadas para las pruebas realizadas, se imprimieron en credenciales de PVC: una imagen marcada con los datos personales del usuario y un código de barras con el número de identificación único cifrado con la llave secreta que fue registrada en el software al momento de instalarlo y que está disponible solo para personal autorizado de la organización dueña de los recursos.

Para realizar la autenticación de las credenciales se requiere escanear la credencial para extraer la imagen con la marca de agua embebida y el código de barras que contiene un número de identificación único, el cual es la llave con la que se genera la marca de agua utilizando el procedimiento descrito en la sección 3.2; posteriormente, se descifra el código obtenido y se genera la secuencia que se compara con la secuencia recuperada de la imagen marcada que estaba impresa en la credencial y así obtener la correlación cruzada; por último, se compara el valor numérico de la correlación con un umbral que se calcula a la par para tomar la decisión y decir si la credencial es auténtica o es falsa.

Figura 6. Creación y validación de la credencial.



a) Creación de la credencial



b) Proceso de validación de la credencial

Fuente: elaboración propia.

4. Resultados de evaluaciones realizadas a las credenciales

Al realizar pruebas para verificar el funcionamiento de la marca de agua para la aplicación propuesta, se insertó la marca de agua a imágenes de diferentes tamaños en escala de grises (120 × 120, 240 × 240 y 512 × 512) pixeles y para imágenes en espacio de color RGB; se probaron en diferentes combinaciones de potencia en cada una de las capas de color usando imágenes de 1024 × 1024 pixeles, las cuales posteriormente fueron impresas en credenciales con un tamaño fijo de 120 × 120, tanto para imágenes a color como para imágenes en escala de grises; dichas credenciales fueron escaneadas con distintas resoluciones (200pp, 400pp, 600pp) para recuperar las imágenes marcadas y realizar su validación, dichos resultados se muestran en las tablas 2 y 3.

Tabla 2. Evaluaciones realizadas a las credenciales en escala de grises.

Ganancia (G)	Longitud (L)	Umbral (Th)	Correlación (Cc)	Detección
0.3	87500	0.6641	1.12	OK
0.3	17500	2.65	4.66	OK
0.3	5700	2.2	3.78	OK
0.3	87500	O.67	1.12	OK
0.3	87500	0.67	1.15	OK
0.3	5700	2.29	3.99	OK
0.2	87500	0.66	0.75	OK
0.2	87500	0.63	0.89	OK
0.2	5700	2.17	2.90	OK
0.2	87500	0.66	0.93	OK
0.1	5700	2.13	1.98	NO
0.1	17500	2.74	2.05	NO
0.1	87500	0.65	0.58	NO

Fuente: elaboración propia

Tabla 3. Evaluaciones realizadas a las credenciales en imágenes a color.

GANANCIA			CORRELACIÓN			UMBRAL			DETECCIÓN
R	G	B	R	G	B	R	G	G	OK
0.3	0	0	12.8	0	0	0.8	0	0	OK
0.4	0	0	14.8	0	0	0.9	0	0	OK
0.5	0	0	16.3	0	0	0.9	0	0	OK
0.6	0	0	17.8	0	0	0.9	0	0	OK
0.7	0	0	20.8	0	0	0.9	0	0	OK
0.8	0	0	23.8	0	0	1.0	0	0	OK
0.9	0	0	26.8	0	0	1.0	0	0	OK
1	0	0	29.8	0	0	1.4	0	0	OK
0.2	0.2	0.2	8.59	8.56	8.4	1.0	0.9	0.8	OK
0.3	0.3	0.3	9.07	9.13	9.13	0.8	0.8	0.7	OK
0.4	0.4	0.4	12.7	12.5	12.5	0.9	0.8	0.8	OK
0.5	0.5	0.5	21.3	21.1	20.4	1.0	1.0	1.0	OK
0.6	0.6	0.6	25.4	25	24.3	1.1	1.0	1.0	OK
0.5	0.4	0.3	21.9	17.3	12.5	1.0	1.0	0.9	OK
0.3	0.4	0.5	8.86	11.8	14.7	0.7	0.7	0.7	OK
0.5	0.3	0.4	14.8	8.9	11.7	0.8	0.7	0.7	OK
0.3	0.5	0.4	12.8	20.9	16.9	1.0	2.0	0.9	OK
0.5	0.4	0	21.9	17.3	0	1.0	1.0	0	OK
0.4	0.3	0	17.5	13	0	1.0	1.0	0	OK
0.3	0.4	0	13.1	17.3	0	1.0	1.0	0	OK
0.4	0.5	0	12.2	16.6	0	0.8	1.0	0	OK
0.3	0.5	0	9.19	16.6	0	0.8	1.0	0	OK
0.5	0.3	0	15.3	10	0	0.9	0.9	0	OK

Fuente: elaboración propia

5. Conclusiones

El algoritmo de marca de agua que se propuso funciona correctamente para la aplicación de crear credencial que tengan como medida de seguridad extra una marca de agua embebida - la cual sirve para validar la autenticidad tanto de la credencial como de la identidad del usuario-; se mostró que esta técnica puede convivir con los mecanismos que se ocupan actualmente para brindar seguridad a este tipo de documentos y complementado a códigos de barras, bandas magnéticas, chips, o RFID.

Puede simplificarse su implementación en entornos automatizados ya que el algoritmo propuesto cumple con las condiciones necesarias pues mostró ser robusto a la conversión D/A y A/D, al ataque de escalamiento, soportando rotaciones de algunos grados que son producto de la distorsión de impresión y escaneo, además de que soporta recorte en los bordes. Los resultados que se presentan demuestran que bajo las condiciones descritas en el presente artículo, el algoritmo funciona de manera estable, y tiene la ventaja de que la detección es ciega, que el tiempo de procesamiento es bajo, que solo se requiere una impresora de tarjetas común, un escáner con resolución mayor a 200 dpi, y una pc; además, la imagen conserva calidad suficiente para realizar la identificación visual del usuario, por lo cual representa una opción viable para la aplicación de validar usuarios mediante credenciales de identificación.

Se elaboró un programa para la creación de dichas credenciales y se validó el funcionamiento del algoritmo. Como perspectiva, puede tenerse como base para crear un software especializado que, además de la marca de agua, sea capaz de usar códigos de barras y códigos bidimensionales y que usando la criptografía de llave simétrica brinde mayor seguridad a dichas credenciales.

Referencias

[1] Mi-Cheng-Lu, Cheng-Yuan-Ku, Lain-Chyr-Hwang, Hui-Ming-Chao. “Using smart card in RFID infraestructure to protect consumer privacy”. International Journal of innovative computing information and control. Volume 7 No. 4. April 2011.

[2] R. Schyndel, A. Tirkel and C. Osborne, “A Digital Watermark”, Proc. Of IEEE int Conf. on Image Precessing, Vol. 2, pp.86-90, 1994.

[3] O. Bruyndonckx, J.J. Quinsquater and B. Macq. “Spatial Method for Copyright Labeling of digital Image”, Proc Of IEEE Nonlinear Signal and Image Processing, 1995, pp. 456-459

[4] IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, 1998, pp 529-539

[5] D. Kundur and D. Hatznakos, “Digital Watermarking for Tamper Proofing and Authentication, Proceedinggs of de IEEE vol. 87, No. 7, 1999.

[6] J. Cox J. Killian and T. Shamoon “Secure spread sectrum watermarketing for multimedia”, IEE trans On image Proceesing Vol 6 No, 12, 1997, pp. 1687.

[7] D. I. Tapia, J. R. Cueli, O. García. J. M. Camacho. J. Bajo, A. Saavedra. “Identificación por radiofrecuencia: fundamentos y aplicaciones”. Artículo de la 1era conferencia científica sobre RFID. Ciudad Real. Noviembre de 2007.

[8] J. Zapata, M. Arango, W. Adame. “Herramientas tecnológicas al servicio de la gestión empresarial”. Revista: Avances en sistemas e informática. Vol. 7. No. 3, Diciembre 2010.

[9] M. Zedillo. “Análisis de algoritmos de marca de agua robustos ante ataques geométricos en el dominio de la transformada de Fourier”. Tesis de Maestría en Ciencias de Ingeniería en Microelectrónica. SEPI-ESIME Unidad Culhuacán. 2006.

[10] C. Máximo S. Ávila. “Autenticación y recuperación de imágenes digitales”. Tesis de Maestría en Ciencias de Ingeniería en Microelectrónica. SEPI-ESIME Unidad Culhuacán. 2011.

[11] E. Bollain-y-Goytia, M. Nakano-Miyatake and H. Perez-Meana “Authentication of Identification Card Using Watermarking” IEEE International 48th Midwest Symposium on Circuits and Systems 2005, pp.1422-1425

[12] M. González Lee. “Detección optima de marcas de agua digitales”, Ed. THP . 18. México, Primera edición 5 Septiembre 2005, pp. 4-12.

[13] N. Ferguson and B. Scheneier, “Practical Cryptography”, Wiley Publishing, Inc. USA, 2003,pp 88.