INSTITUTO POLITÉCNICO NACIONAL

CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN

ANÁLISIS DE LAS MICROIMPRESIONES DE LA CREDENCIAL PARA VOTAR CON FOTOGRAFÍA

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRO EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A

LIC. JOSÉ DE JESUS DELOYA CRUZ

DIRECTORES DE TESIS

DR. EDGARDO MANUEL FELIPE RIVERÓN
DR. SALVADOR GODOY CALDERÓN

MÉXICO, D.F., JUNIO DE 2009

SIP-14

INSTITUTO POLITECNICO NACIONAL

SECRETARIA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D.F. siendo las 10:10 horas del día 17 del mes de Junio de 2009 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación del:

Centro de Investigación en Computación

para examinar la tesis de grado titulada:

"ANÁLISIS DE LAS MICROIMPRESIONES DE LA CREDENCIAL PARA VOTAR CON FOTOGRAFÍA"

DELOYA	CRUZ	JOSÉ DE JESÚS
Apellido paterno	materno	nombre(s)

Con registro: A 0 7 0 2 3 5

aspirante al grado de: **MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN**

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Presidente

Dr. Sergio Suárez Guerra

Secretario

Dr. Oleksiy Pogrebnyak Boleslavovich

Primer vocal
(Director de tesis)

Dr. Edgardo Manuel Felipe Riverón

Segundo vocal
(Director de tesis)

Dr. Salvador Godoy Calderón

Tercer vocal

Dr. Ricardo Barrón Fernández

EL PRESIDENTE DEL COLEGIO

Dr. Jaime Álvarez Gallegos

INSTITUTO POLITECNICO NACIONAL
CENTRO DE INVESTIGACION EN COMPUTACION
DIRECCION

INSTITUTO POLITECNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESION DE DERECHOS

En la Ciudad de México, D.F., el día 18 del mes de Junio del año 2009, el (la) que suscribe José de Jesús Deloya Cruz alumno (a) del Programa de Maestría en Ciencias de la Computación con número de registro A070235, adscrito al Centro de Investigación en Computación, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección de Doctor Edgardo Manuel Felipe Riverón y Doctor Salvador Godoy Calderón y cede los derechos del trabajo intitulado Análisis de las microimpresiones de la Credencial para Votar con Fotografía, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección edgardo@cic.ipn.mx, o jedeloya@gmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

José de Jesús Deloya Cruz

Nombre y firma

Resumen

La presente tesis presenta una metodología para el análisis y validación del microtexto en la Credencial para Votar con fotografía expedida por el Instituto Federal Electoral (IFE) de México, para poder votar en las elecciones federales y locales. A pesar de que la ley define como identificación oficial a las identificaciones expedidas por una dependencia gubernamental, en México este documento ha sido adoptado como identificación oficial para cualquier tipo de trámite administrativo. El IFE es un organismo independiente por lo que según la definición legal, la Credencial para Votar con fotografía no es una identificación oficial.

Esta credencial del IFE, al usarse como método de identificación, representa un blanco de los falsificadores, principalmente para los menores que quieren comprar cigarros y alcohol; sin embargo, existen personas que la tratan de falsificar para realizar fraudes mayores a instituciones bancarias y a aquellas que se dedican a préstamos bancarios.

Esta credencial posee varios candados de seguridad, los que a pesar de ser efectivos, son muy poco difundidos entre la población; el desconocimiento de estos candados la hacen un blanco fácil de los falsificadores. En esta tesis nos enfocamos en uno de los candados de seguridad de la Credencial, el microtexto, el cual en el anverso se encuentra alrededor de la fotografía y en el reverso alrededor del área destinada para la firma.

Para detectar las posibles falsificaciones de la Credencial para Votar con fotografía, se usaron distintas técnicas para el análisis de imágenes digitales, como son, los detectores de bordes, las técnicas de umbralado y algunas técnicas morfológicas.

Palabras clave: Análisis de imágenes; Credencial para Votar con fotografía; Instituto Federal Electoral; Morfología matemática; Correlación; Microtexto; Microimpresión; Reconocimiento Óptico de Caracteres.

Abstract

This work presents a methodology for the analysis and validation of microtexts printed in the Mexican identification cards (ID) issued by Federal Electoral Institute (IFE) in Mexico to vote in local and federal elections. Although law defines an official ID as an ID issued by a non-governmental dependency, in Mexico the Mexican IFE-ID was adopted as an official identification to do any transaction. The IFE is a non-governmental dependency and that defines this ID as a non official identification.

The IFE Id-card in Mexico is one of the most used method to identify Mexican citizens, that is why the Id-card is one of biggest target of counterfeiters and principally people who are under 18 and are under the influence either of alcoholic drinks or cigarettes. But the bigger threat that this ID is engaged in is falsification of banking accounts and others.

The Mexican Identification card holds many security locks, but they are not spread into the population; the citizens ignore the use and knowledge of this Id-card, this makes the ID an easy target for counterfeiters. This work focus in one of the security locks of this Id-card, the microtext, which is located around the photography on the Id-card's obverse, and around the signing area on the reverse side.

To carry out the work goals, we used digital image analysis techniques like: edge detectors, threshold techniques, and some morphological techniques.

Key words: Image analysis, Mexican Identification card, Federal Electoral Institute, Mathematical morphology, Correlation, Micro-text, Optical Character Recognition.

Agradecimientos

Es mi más profundo deseo el agradecer a todas las personas e instituciones que hicieron posible la elaboración de la presente tesis, en primer lugar, quiero agradecer al Instituto Politécnico Nacional (IPN) que, en conjunto con la Secretaría de Investigación y Posgrado (SIP) y el Centro de Investigación en Computación (CIC), me brindaron el apoyo con las instalaciones y equipo necesarios para realizar la presente investigación, además de haberme apoyado económicamente con las becas ofrecidas por la SIP.

Quiero además agradecer al Consejo Nacional de Ciencia y Tecnología (CONACyT) por haberme apoyado también económicamente con la beca que ofrece.

Además, también debo hacer mención de mis dos directores de tesis, el Doctor Edgardo Manuel Felipe Riverón y el Doctor Salvador Godoy Calderón, ya que me brindaron sus conocimientos y su tiempo para resolver las dudas que se me fueron presentando. Así mismo quiero mencionar que no solo fueron los directores de mi tesis, sino además se comportaron como amigos al sufrir y celebrar junto a mí todas mis fallas y logros dentro del CIC, además entre nosotros siempre estuvo presente un espíritu de convivencia y con todos los amigos que conocí dentro del CIC.

Es mi deseo agradecer también a los amigos, quienes con sus juegos y apoyos siempre me hicieron sentir bien dentro del Centro, entre ellos particularmente menciono a Cynthia, Jeanine, Samuel, Bryan, Benja, Víctor y todos aquellos que sin querer pudiera llegar a olvidar.

También quiero agradecer a mis padres, que sin su ayuda, consejos, regaños y palabras de aliento nunca hubiera llegado tan lejos y no escribiría estas palabras además de reconocer el hecho de que mis hermanos siempre me han apoyado en las diversas situaciones que ha presentado la vida.

En esta ocasión, quiero expresar mi más sincero y profundo agradecimiento a Cynthia, esa persona que sin querer se atravesó en mi vida, esa persona especial que conocí en el CIC, esa persona que me apoyó y me ayudó con sus palabras de aliento a terminar lo que ya había empezado, que incluso me ayudó en la redacción del presente documento, además de ser compañera mía en esta etapa de mi vida. Con ella viví muchas cosas durante la estancia en el CIC, pero lo más importante es que está conmigo en las buenas y en las malas. Gracias amor por tu apoyo y comprensión.

Por último, es mi deseo agradecer a todas las personas que cooperaron dejando que se utilizaran sus credenciales para votar con fotografía requeridas para el desarrollo y experimentación del presente trabajo, ya que sin ellos esta tesis no hubiera podido ser posible.

Contenido

Lista de Figuras

Lista de Tablas

Lista de siglas y acrónimos

Vamos a describir las siglas y acrónimos usados en la presente tesis.

IPN: Instituto Politécnico Nacional.

CIC: Centro de Investigación en Computación.

SIP: Secretaría de Investigación y Posgrado.

IFE: Instituto Federal Electoral.

OCR: Siglas en inglés de *Optical Character Recognition* (Reconocimiento Óptico de Caracteres en español).

SE: Siglas en inglés de *Structure Element* (Elemento de Estructura en español).

PGR: Procuraduría General de la República.

Glosario

Brindamos algunas definiciones, en general no académicas, de algunos términos que se usan en esta área y en otras afines.

Documento: Un documento es todo portador de la información que se puede entender, interpretar y quedar escrita en el tiempo.

Grafoscopía: De las palabras griegas $\gamma\rho\alpha\varphi\omega$ (grafo), "escribir" y skopéo "observo". Es la disciplina que se encarga del estudio de la escritura y las firmas para determinar la autoría de las mismas, así como la identificación de los sujetos a partir de las características de su escritura y de su firma.

Documentoscopía: De las palabras "documento" y la griega skopéo "observo". Es la disciplina que se encarga del análisis de un documento con la finalidad de determinar su autenticidad, falsedad o alteración. Esta disciplina no indica quién fue el autor o el momento en que fue alterado, para lo cual existen otras ciencias que se dedican a estos estudios.

La Documentoscopía utiliza dos premisas:

- "Origen" (naturaleza del documento) y
- "Autenticidad" (si es falso o no).

Grafología: De las palabras griegas $\gamma\rho\alpha\varphi\omega$ (grafo) "escribir" y $\lambda o\gamma\iota\alpha$ (logía) "tratado, estudio". Es la disciplina que estudia el perfil psicológico de las personas a partir del estudio de su escritura manuscrita.

Identificación Oficial: Es aquel documento expedido a través de una dependencia gubernamental. La Credencial para Votar con fotografía no se considera como tal, ya que la expide el Instituto Federal Electoral (IFE). Erróneamente ha adquirido tal categoría, por ser el único documento que es aceptado por bancos, empresas crediticias, trámites administrativos y por la misma sociedad.

Carácter: Dígito simple, letra, marca de puntuación u otro símbolo que el ordenador puede leer o escribir. En los microordenadores y los procesadores de textos, un carácter se almacena o se expresa con un byte.

Clave de elector: La clave de elector consta de 18 caracteres, en los cuales se representa en seis caracteres el nombre del ciudadano tomando la letra inicial y la siguiente consonante del apellido paterno, del materno y del nombre; su fecha de nacimiento en los siguientes seis caracteres; dos más para la clave de la entidad federativa donde nació; uno para el sexo; uno más para el digito verificador y dos para la clave de homonimia la cual permite diferenciar a dos electores cuyos datos produzcan la misma clave en los primeros 16 caracteres.

Microtextos o microimpresiones: Son impresiones tipográficas de un texto con caracteres de tamaño menores que un punto. Algunas personas pueden ver a simple vista el texto impreso con caracteres de 0,8mm de altura, mientras que los caracteres de 0,2 mm aparecen a simple vista como una línea fina, aunque pueden leerse con una lupa. Sin embargo, las microimpresiones ofrecen protección contra los sistemas de fotocopiado.

Pixel o píxel: Elemento básico que conforma a una imagen; la palabra proviene de la contracción de *picture element* (elemento de imagen) en el idioma inglés.

Tinta fotocromática: Tinta que cambia de color al ser expuesta a la luz ultravioleta y que al regresar bajo la luz blanca regresa a su color original.

CAPÍTULO I. INTRODUCCIÓN

1.1 Introducción

El Consejo General del Instituto Federal Electoral, en sesión de fecha 30 de abril de 1992, aprobó el informe de la Comisión Nacional de Vigilancia del Registro Federal de Electores adoptado el 29 del mismo mes y año, por el que se recomienda la expedición de una nueva Credencial para Votar que contuviera la fotografía del ciudadano.

El Consejo General denominó en esa misma sesión la realización del programa de la nueva credencial para votar con fotografía, y como consecuencia, el entonces Comité de Adquisiciones, Arrendamientos y Servicios relacionados con bienes muebles del Instituto Federal Electoral, convocó a proveedores nacionales y del extranjero a un concurso internacional en dos etapas, con el objeto de obtener propuestas de solución que satisficieran la problemática planteada por el instituto.

En sesión del 30 de junio de 1992, la Comisión Nacional de Vigilancia del Registro Federal de Electores acordó recomendar al Consejo General del Instituto Federal Electoral, la adopción de un proyecto de modelo de la Credencial para Votar con fotografía.

En sesiones del 24 de julio y 31 de agosto de 1992, la Comisión Nacional de Vigilancia del Registro Federal de Electores aprobó por razones de orden técnico, tecnológico y de control, las variantes mínimas al modelo de la nueva Credencial para Votar con fotografía, así como el diseño del holograma y otros elementos de seguridad, en los términos del acuerdo del Consejo General del Instituto Federal Electoral del 3 de julio de 1992 [1].

1.2 El problema a resolver

La presente tesis se enfoca en la resolución de un problema de clasificación en el área de la documentoscopía. El problema consiste en la autentificación de los dos microtextos que como medida de seguridad están presentes en la Credencial para Votar con fotografía vigente, como parte de un proyecto mayor que ha de autentificar la credencial completa.

1.3 Justificación

En la República Mexicana, cientos de falsificadores crean credenciales apócrifas. Para ello utilizan cámaras digitales, escáneres, impresoras de buena calidad, programas de diseño gráfico y métodos de enmicado, que no logran emular las medidas o candados de seguridad de las identificaciones legales; sin embargo, producen credenciales que logran burlar el control de los “antros” y licorerías.

La Procuraduría General de la República (PGR), ha descubierto bandas de delincuentes que clonan credenciales para votar, pero para fines más perversos, como son los fraudes bancarios. Muchos estados podrían estar a merced de grupos similares [1].

Sin embargo, a pesar de que existen todos estos problemas con la falsificación, en México hay muy poca difusión de los candados de seguridad entre la ciudadanía, es por ello que los fraudes cometidos por estos bandidos son detectados ya muy tarde y sin forma de remediarlos. Es por eso que en el caso de la presente tesis, se pretende dar una forma rápida y segura para poder verificar el candado de seguridad del microtexto en la Credencial para Votar con fotografía por medio de la visión por computadora.

1.4 Hipótesis

Mediante el análisis de los microtextos de las credenciales para votar con fotografía y sus características, se plantea que es posible determinar con un cierto grado de certeza, cuáles constituyen microtextos válidos y cuáles son producto de algún tipo de falsificación.

1.5 Objetivos

Los objetivos general y específicos de este trabajo son los siguientes:

1.5.1 Objetivo general

Crear un subsistema de software capaz de validar la autenticidad de las líneas de microimpresión, que se encuentran alrededor de la fotografía en el anverso y alrededor del área destinada para la firma en el reverso de la credencial para votar con fotografía.

1.5.2 Objetivos específicos

- Crear las condiciones para extraer la información de la microimpresión de ambas caras de la Credencial para Votar con fotografía mediante el escaneo con alta resolución.
- Crear una base de datos a partir de un número suficiente de credenciales para probar la funcionalidad del sistema.
- Crear una metodología para extraer los datos de validación del microtexto del anverso de la credencial (nombre del titular y año aproximado).
- Crear una metodología para ubicar automáticamente las áreas en las cuales están las microimpresiones en el anverso y el reverso, y extraerlas.
- Analizar dichas áreas, validar en cada una de ellas si existe o no la microimpresión y comprobar en cada caso si éstas cumplen o no con las correspondientes exigencias de autenticidad.

1.6 Medios utilizados

Para la realización de este trabajo y la creación de su interfaz gráfica, se utilizaron los siguientes medios de hardware y software:

- Escáner de color modelo HP Scanjet 8200 de alta resolución.
- Borland C++ Builder 6, Versión 6.0 Release 10.161.

1.7 Apoyos

Los apoyos recibidos para la realización de este trabajo son:

1.7.1 Apoyos

Durante el desarrollo de la investigación se contó con el apoyo de becas del CONACyT y del Programa Institucional de Formación de Investigadores (PIFI) del Instituto Politécnico Nacional.

1.8 Estado del arte

Con el problema de la falsificación de productos y la piratería de programas informáticos en el primer plano de la agenda política internacional, cada vez hay una mayor necesidad de sistemas rápidos y sencillos que permitan distinguir los productos de imitación de los productos genuinos como medio para detectar e impedir las falsificaciones. Los productos y tecnologías de autentificación cuya utilización requiere una profunda colaboración entre los titulares de derechos de propiedad intelectual y los organismos que inspeccionan los productos, cumplen un cometido importante en este campo.

La función de las tecnologías de autentificación es ayudar a los examinadores, es decir, a funcionarios de aduanas, policía y organizaciones de protección de los consumidores, a detectar la autenticidad de un producto en formas que no resulten obvias para los falsificadores, que se han convertido en expertos en la reproducción exacta de productos y embalajes. Estas tecnologías permiten al examinador ver más allá de las características patentes del producto para determinar con un grado razonable de certidumbre si el producto es auténtico. Y a la inversa, la ausencia de las características no obvias pondrá de manifiesto la imitación, incluso si el aspecto es exactamente el mismo que el del producto genuino.

Los documentos oficiales pueden estar formados por varias capas, de modo que, por ejemplo, la primera capa sea visible para el consumidor, en tanto que la capa inferior contiene un medio de examen que no resulte evidente para el falsificador.

Los dispositivos de autentificación realizan la separación en capas de los documentos analizados y detectan los diversos dispositivos con los que cuenta, estos pueden ser:

- Dispositivos manifiestos. Son visibles a simple vista bajo condiciones normales de visión, como, por ejemplo, hologramas, tintas que cambian de color, delgadas películas iridiscentes o materiales retrorreflectivos.

- Dispositivos camuflados (o semiocultos). Se hacen visibles al ojo humano mediante la aplicación de un instrumento manual de inspección, como la superposición de una transparencia, una luz ultravioleta, una lupa o un puntero láser. Esta categoría comprende tintas sensibles a la luz ultravioleta o infrarroja, microtextos, imágenes codificadas u hologramas.

- Dispositivos ocultos. Requieren un sistema o instrumento de detección más complejo. Pueden ser de tipo químico, como el etiquetado con agregados o marcadores químicos incorporados en el producto o el embalaje, o electrónicos, como un código numérico o algún tipo de identificador similar (que pueden requerir la conexión a una base central de datos). Los dispositivos ocultos engloban también el etiquetado molecular y con ADN, el etiquetado magnético y los códigos integrados.

- Dispositivos periciales. Requieren un análisis de laboratorio, que puede incluir el análisis de la composición del producto o el análisis pericial del marcador de autentificación.

Estos elementos pueden encontrarse, ya sea de forma independiente o incorporados, en un único dispositivo de autentificación.

Así, los dispositivos de autentificación, si se utilizan adecuadamente en el marco de una estrategia integral de lucha contra la falsificación, podrán contribuir efectivamente a la reducción de las falsificaciones [2].

A continuación comentaremos las características de algunos sistemas de autentificación ya implementados en el mundo, aunque aclaramos que ninguno ha sido realizado sobre las Credenciales para Votar con fotografía vigentes en la República Mexicana como instrumento de identificación.

Assure-ID Professional

Assure ID – Profesional es un software para identificar en forma automática identificaciones de cualquier tamaño o nacionalidad. El software exhibe toda la información e imágenes capturadas al usuario para el análisis, incluye varias ayudas para maximizar la imagen, para destacar regiones de interés y para hacer una remisión de pruebas.

De igual forma se pueden mostrar los resultados de la autentificación y realizar, de ser necesario una variedad de reportes al documento para detectar la falsificación. El sistema incluye una biblioteca con los datos que hacen a cada documento auténtico. Este software no se puede comprar por separado, viene con un dispositivo que realiza la captura de documento para su análisis.

Los dispositivos de la captura de documento se pueden clasificar según los tamaños, documentos que leen y las clases de datos pueden capturar: ID-1 (usado para las tarjetas de crédito), ID-2 (levemente más grande que el ID-1), e ID-3 (usado para los pasaportes, las visas, etc.).

Para las tarjetas que tienen tiras magnéticas el hardware cuenta con diversas condiciones de iluminación bajo las cuales diversos documentos necesitan ser examinados para diversas cualidades de seguridad del documento: visible, del infrarrojo cercano, ultravioleta, coaxial, y direccional [3].

Sistema de Verificación de Documentos

Es sistema de verificación de documentos permite el análisis de documentos de identificación y permite detectar en forma automática posibles falsificaciones.

Es un software basado en arquitectura Web que funciona on-line y off-line que realiza la extracción de los datos según los estándares definidos, incluyendo los códigos de control, cuya coherencia se comprueba inmediatamente tras el reconocimiento de los caracteres.

La verificación del documento consiste en la ejecución de las acciones predefinidas para cada modelo de documento orientadas a la detección de falsificaciones o incidencias en el mismo. Estas acciones utilizan la información capturada del documento (imágenes y datos) y la almacenada en el repositorio para ese modelo de documento (medidas de seguridad con su nivel de precisión exigido).

Una vez que el software termina el proceso de verificación existen dos interfaces de usuario disponibles que muestran los resultados:

La primera muestra una indicación autentico – falso, y en caso de posible falso se muestra la operación de verificación que ha fallado y su resultado.

La segunda interfaz muestra una indicación autentico – falso y proporciona herramientas de análisis del documento incluyendo los resultados detallados de todas las verificaciones efectuadas.

En la figura 1 se muestra una de las vistas del sistema con un ejemplo de análisis de documentos [4].

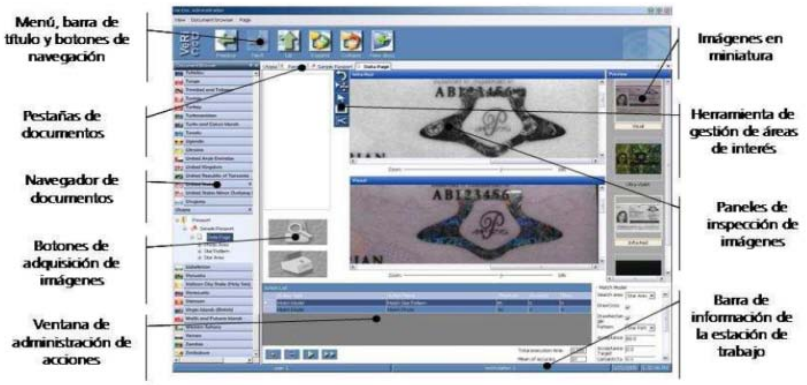


Figura 1 Ejemplo de vista del Sistema de Verificación de Documentos

Magictester

Magictester es un visor de microescritura patentado y fabricado mediante tecnología y óptica alemana, desarrollado principalmente para comprobar la autenticidad de billetes y documentos, a través de la lectura de la microimpresión.

Es un sistema simple, que descubre inmediatamente falsificaciones no detectadas incluso, por los rayos-UV. Su empleo consiste en recorrer el billete con la lente, hasta que se visualice la microimpresión que contiene y que cambian en función de su valor. También puede comprobar la existencia de marcas de agua, de concordancia, la autenticidad de la banda de plata, la veracidad del papel y el registro de transparencia.

La comprobación de todos estos elementos, se consigue gracias a un emplazamiento estratégico de elementos de luz, que iluminan el billete por la parte inferior, dejando ver en el acto la microimpresión [5].

Forgery Detection System (Sistema de detección de falsificaciones)

Este sistema cuenta con una serie de dispositivos para analizar los documentos:

Un visor de mano para verificar el laminado de seguridad; se utiliza en muchos pasaportes y cédulas de identidad para desalentar la sustitución de la fotografía del documento del portador, mientras que protege los detalles biográficos contenidos en el mismo. Con este dispositivo se puede ver fácilmente cualquier daño causado por la sustitución de una fotografía, cualquier intento de levantar el laminado, al igual que la sustitución del laminado en su totalidad.

Un microscopio portátil iluminado con 30x de magnificación que incluye una lupa de 8x, usado en la inspección de documentos para la verificación de microimpresiones y la investigación de las costuras en los pasaportes [6].

Dispositivo de autentificación móvil IDetector

El *IDetector* es una herramienta portable para el chequeo de una gran cantidad de características de seguridad mediante el uso de luces intercambiables, lentes de aumento y cámaras digitales. Cuenta con un software que se instala en el *IDetector*, haciéndolo una herramienta autónoma para realizar las autentificaciones.

El software usa el microprocesador ubicado en el *IDetector* y los resultados se observan inmediatamente en la pantalla de la cámara.

La arquitectura del programa permite añadirle varios *plug-ins* al mismo dispositivo que permiten el chequeo de varias características de seguridad, entre ellas el microtexto. Esto puede ser un obstáculo en la efectividad ya que para una autentificación fiel se necesitan varias herramientas de autentificación

El *IDetector* es un dispositivo 3 en uno al ser una cámara estándar digital, un microscopio de alto poder y un UV o fuente de luz visible. Cuenta con una alta resolución de 7 mega pixeles y lentes que dan un rango de aumento de la imagen de 10x a 150x y el software integrado para la autentificación de documentos (Figura 2) [7].

Figura 2 IDetector

1.9 Organización del documento

La estructura de este documento es la siguiente:

En el Capítulo 1 se expone el problema a resolver, su justificación y la hipótesis que consideramos válida, además del objetivo general del trabajo y los objetivos específicos que persigue. También se mencionan los medios utilizados, los apoyos obtenidos para la realización del proyecto y se desarrolla un breve estado del arte.

En el Capítulo 2 se presenta una descripción de los conceptos básicos y definiciones relacionados con el análisis de imágenes y algunas de sus principales características. En este capítulo también se detallan las características y generalidades de la Credencial para Votar con fotografía, incluyendo las relacionadas con las microimpresiones que ésta posee.

En el Capítulo 3 se describe el sistema y su interfaz gráfica, la forma en que se logró la captura de las imágenes y la metodología general para su análisis, así como la arquitectura general del sistema.

En Capítulo 4 abarca las pruebas y la evaluación de los resultados del sistema, junto con sus limitaciones.

Las conclusiones derivadas de la solución de la problemática, algunas recomendaciones, junto con el trabajo futuro se presentan en el Capítulo 5.

Por último, al final se detallan las referencias consultadas durante la realización de este trabajo de tesis.

CAPÍTULO II. CONCEPTOS BÁSICOS Y DEFINICIONES

En el presente capítulo presentamos de forma breve algunos conceptos sobre el procesamiento digital de imágenes, que consideramos necesarios para la cabal comprensión de este trabajo.

Dentro del procesamiento de imágenes se detallan los conceptos de resolución espacial y de niveles, algunos de los modelos de color más usuales, la segmentación y algunos tópicos de importancia dentro de la morfología matemática.

Finalmente se enlistarán los detalles y características de la Credencial para Votar con fotografía, sus medidas de seguridad y las microimpresiones cuya autentificación constituye la parte fundamental de este estudio.

2.1 Procesamiento digital de imágenes

Una imagen puede ser definida como una función bidimensional ($f(x, y)$) en donde x e y son las coordenadas espaciales y la magnitud de f en las coordenadas (x, y) es llamada la intensidad del nivel de gris en ese punto. Cuando los valores de x, y y f son todos finitos y discretos, podemos nombrar la imagen como imagen digital. El procesamiento digital de imágenes se encarga del procesamiento y análisis de las imágenes digitales.

Para poder realizar el análisis de una imagen y poder cuantificar automáticamente determinados objetos presentes en la misma, es preciso que el ordenador realice una clasificación. La clasificación es el proceso por el cual los pixeles pertenecientes a una imagen son divididos en clases, las que normalmente son dos: objetos de interés y fondo. Los objetos de interés pueden ser núcleos en imágenes histológicas, áreas de fibrosis en tejido hepático, vainas de mielina en axones nerviosos, etc. [8].

2.1.1 Resolución de imágenes

Una imagen analógica es continua en las coordenadas (x, y) y en la amplitud f. Para convertir la imagen a digital, se debe hacer un muestreo de la función en ambas coordenadas y en la amplitud. A la acción de digitalizar el valor de las coordenadas se le llama muestreo, mientras que a la acción de digitalizar la amplitud se le llama cuantificación de niveles.

2.1.1.1 Resolución espacial

Básicamente, la resolución espacial es la capacidad de distinguir los detalles espaciales finos. Supongamos que construimos una imagen compuesta por líneas de ancho W con un espacio entre las líneas del mismo ancho W. Un par de líneas consiste de la línea y su espacio adyacente. Esto es, el ancho de un par de líneas es 2W, y hay 1/2W pares de líneas por unidad de distancia. La definición más usada de resolución es simplemente el número más pequeño de pares de líneas distinguibles por unidad de distancia; por ejemplo, 100 pares de líneas por milímetro. La frecuencia espacial a la cual se realiza la muestra de una imagen digital (la frecuencia de muestreo), es también un buen indicador de la resolución, es decir, cuántas tomas de muestras se efectúan en una

determinada medida de longitud. Este es el motivo por el que *dots per inch* (*dpi*, o ppp, puntos por pulgada en español), o *pixels per inch* (*ppi* o ppp, pixeles por pulgada en español), son términos comunes y sinónimos utilizados para expresar la resolución de imágenes digitales. Generalmente, pero dentro de ciertos límites, el aumento de la frecuencia de muestreo también ayuda a aumentar la resolución.

El tamaño de un archivo es proporcional a la resolución de la imagen que representa. Por ejemplo (figura 3), el tamaño del archivo de una imagen con una resolución de 200 ppp es cuatro veces más grande que el tamaño del archivo de una imagen con las mismas dimensiones y una resolución de 100 ppp.

Figura 3 Resolución espacial

2.1.1.2 Resolución de niveles de gris

La resolución de niveles de gris se refiere al cambio más pequeño distinguible en el nivel de gris de una imagen, pero en realidad la medición de los cambios en los niveles de gris distinguibles es un proceso altamente subjetivo. Cuando digitalizamos una imagen se tienen valores muy discretos dependiendo del muestreo usado para realizar la digitalización, sin embargo, pero esto no sucede en la cuantificación de los niveles de gris. Debido a las consideraciones de hardware, el número de niveles de gris es usualmente un entero potencia de dos. El número de niveles más común es medido con 8 bits o sea 256 niveles de gris, aunque se usan hasta 32 bits en algunas aplicaciones en donde es necesario el realce de los rangos de niveles de gris específicos.

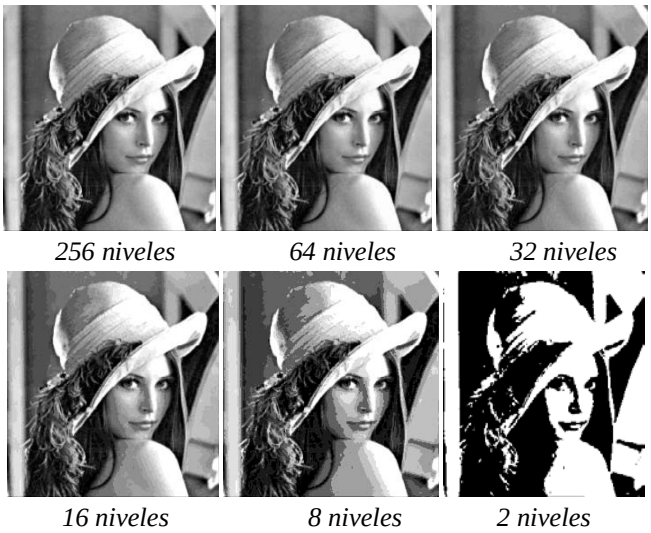


Figura 4 Imagen a diferentes resoluciones de nivel de gris

2.1.2 Digitalización de imágenes por mapa de bits

Como ya se mencionó, una imagen digital es representada por valores digitales derivados del muestreo de la imagen analógica. Los valores digitales son pulsos electrónicos discretos que han sido traducidos en una serie de ceros y unos, los únicos dígitos en un sistema de numeración binario.

Digitalizar es el proceso de traducir información como textos, imágenes o sonidos, a un formato que puedan entender los microprocesadores, ya que éstos sólo están capacitados para manejar los valores uno y cero.

Hay dos formas distintas de digitalizar las imágenes: gráficos vectoriales y gráficos rasterizados, de trama o de mapa de bits. Sólo será definida la digitalización de mapa de bits porque es el formato gráfico utilizado en el presente trabajo.

Las imágenes rasterizadas o de mapa de bits son fotos electrónicas tomadas de una escena o escaneadas de documentos como fotografías, manuscritos, textos impresos e ilustraciones de las que se confecciona un mapa en forma de un reticulado de puntos o elementos de la figura (pixeles). A cada pixel se le asigna un valor tonal (negro, blanco, tonos de gris o matices de color), el cual está representado en un código binario (ceros y unos); un ejemplo de esto se observa en la figura 5.

Los dígitos binarios (*bits*) para cada pixel son almacenados por una computadora en una secuencia, junto con la dirección numérica que ocupa, en lo que se conoce como “mapa de imagen”. Luego la computadora interpreta y lee los pixeles para producir una versión analógica para su visualización o impresión.

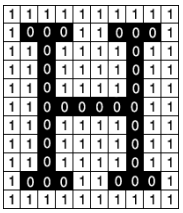


Figura 5 Imagen de una letra H digitalizada

Una imagen binaria está representada por pixeles que constan de 1 *bit* cada uno, que pueden representar dos colores, utilizando los valores 0 para el negro y 1 para el blanco. Una imagen a escala de grises está compuesta por pixeles representados por múltiples *bits* de información, que típicamente varían entre 2 a 8 *bits* o más.

Una imagen de color está representada por una profundidad de *bits* entre 8 y 24 o superior a ésta. En una imagen de 24 *bits*, los *bits* por lo general están divididos en tres grupos: 8 para el rojo, 8 para el verde, y 8 para el azul en el modelo RGB. Para representar otros colores se utilizan combinaciones de esos bits. Una imagen de 24 *bits* ofrece 16,7 millones de colores diferentes. Sin embargo, cada vez más, los escáneres de color capturan 10 *bits* o más por canal de color, llegando a digitalizar imágenes en 32 *bits* por pixel [9].

2.1.3 Modelo de color RGB

Isaac Newton (1642- 1726) fue quien primero ordenó los colores al construir un convincente círculo cromático sobre el cual se han basado muchos de los estudios posteriores.

Se han elaborado distintos modelos de color, por lo que existen diferencias en la construcción de los círculos cromáticos que responden a cada modelo. El avance que significaron los estudios de Newton brindaron la posibilidad de identificar objetiva y no subjetivamente un color nominándolo por las mezclas con las que fue creado.

Los modelos de color son fórmulas matemáticas que calculan el color. Existen diversos modelos, pero para este estudio se describirá el modelo RGB.

El modelo RGB, basado en los colores primarios de la mezcla aditiva para la luz: rojo, verde y azul, es usado para representar las imágenes en los monitores de las computadoras (Figura 6).

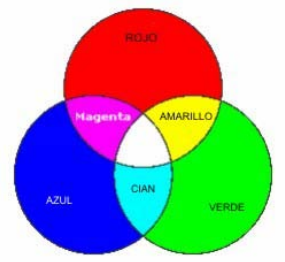


Figura 6 Modelo RGB

El modelo RGB asigna un valor de intensidad a cada pixel que oscile entre 0 (negro) y 255 (blanco) para cada uno de los componentes RGB de una imagen en color. Por ejemplo, un color rojo brillante podría tener un valor R de 246, un valor G de 20 y un valor B de 50. El rojo más brillante que se puede conseguir es el R: 255, G: 0, B: 0 (Figura 7). Cuando los valores de los tres componentes son idénticos, se obtiene un matiz de gris. Si el valor de todos los componentes es de 255, el resultado será blanco puro y será negro puro si todos los componentes tienen un valor 0. Los valores más altos de RGB corresponden a una cantidad mayor de luz blanca. Por consiguiente, mientras más altos son los valores RGB, más claros son los colores.

hexadecimal		decimal
#A52A2A		165, 42, 42
#DEB887		222,184,135
#5F9EA0		95,158,160
#7FFF00		127,255, 0
#D2691E		210,105, 30
#FF7F50		255,127, 80
#6495ED		100,149,237

Figura 7 Notaciones RGB

Un color cualquiera vendrá representado en el sistema RGB mediante la sintaxis decimal (R, G, B) o mediante la sintaxis hexadecimal #RRGGBB. El color rojo puro, por ejemplo, se especificará como (255,0,0) en notación RGB decimal y #FF0000 en notación RGB hexadecimal, mientras que el color rosa claro dado en notación decimal por (252,165,253) se corresponde con el color hexadecimal #FCA5FD [10].

2.1.4 Segmentación

La práctica ha demostrado que, en el caso general, el reconocimiento de un objeto se encuentra íntimamente relacionado con la segmentación; sin un reconocimiento al menos parcial la segmentación no puede llevarse a cabo y de la misma manera, sin una segmentación previa el reconocimiento de los objetos no es posible.

La segmentación puede también ser definida como el encontrar, por medio de un algoritmo numérico, las regiones homogéneas y sus bordes. Los métodos de segmentación usados en el presente trabajo se describen a continuación [11].

2.1.4.1 Detección de bordes

Un borde en una imagen es un cambio local significativo, normalmente asociado a una discontinuidad en los niveles de intensidad de una imagen digital. El mejoramiento de los bordes se requiere para enfatizar las posiciones en la imagen donde ocurren cambios significativos locales en los valores de intensidad. La localización de los bordes es necesaria para separar los máximos locales verdaderos (máximos debidos a bordes) de los falsos máximos (máximos debidos al ruido).

Los enfatizadores de la primera derivada basan su operación en el gradiente. El gradiente, como se sabe, es el equivalente de la primera derivada y se define como el vector:

$$G[f(x,y)] = \begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} \frac{\delta f}{\delta x} \\ \frac{\delta f}{\delta y} \end{bmatrix} \qquad (\mathbf{1})$$

Su magnitud viene dada por

$$G[f(x,y)] = \sqrt{G_x^2 + G_y^2} \qquad (\mathbf{2})$$

Que iguala la tasa máxima de crecimiento de $G[f(x,y)]$ por unidad de distancia en la dirección G [11].

2.1.4.1.1 Gradiente cruzado de Roberts

El operador cruzado de Roberts proporciona una aproximación sencilla para el cálculo de la magnitud del gradiente, dado por:

$$G[f(x,y)] = f(x,y) - f(x+1,y+1) + f(x+1,y) - f(x,y+1) \qquad (\mathbf{3})$$

Al usar máscaras de convolución, este operador se transforma en:

$$G[f(i,j)] = G_x + G_y \qquad (\mathbf{4})$$

Donde G_x y G_y son calculados usando las máscaras de la figura 8:

1	0
0	-1

0	1
-1	0

Figura 8 Izquierda Gx y derecha Gy

2.1.4.2 Umbralado

El umbralado fue una las primeras técnicas que se usaron para en el análisis de imágenes para segmentar una imagen. Consiste en convertir una imagen en nieles de gris $f(x,y)$ en una imagen binaria $b(x,y)$, buscando que los objetos de interés de la imagen queden separados del fondo.

Para que el umbralado sea efectivo se requiere que los objetos de interés presenten suficiente contraste con respecto al fondo y que se conozca el rango de intensidad ya sea de los objetos o del fondo. Si el objeto a segmentar es más claro que el fondo, entonces, de acuerdo con:

$$b(x,y) = \begin{cases} L-1 \\ 0 \end{cases} \text{ si } f(x,y) \geq u \qquad (\mathbf{5})$$

Si se sabe que el nivel de gris de la superficie del objeto se encuentra en el rango $[u_1, u_2]$, entonces:

$$b(x,y) = \begin{cases} L-1 \\ 0 \end{cases} \text{ si } u_1 \leq f(x,y) \leq u_2 \qquad (\mathbf{6})$$

2.1.4.2.1 Umbralado automático

El umbralado automático es útil en el caso de la navegación automática, donde las condiciones de iluminación e interacción entre objetos cambian a cada instante.

Para los umbralados automáticos se debe suponer que los objetos de interés son claros contra un fondo oscuro. Esto permite determinar que los niveles de intensidad con valor por encima de un umbral u pertenecen al objeto de interés, mientras que los niveles de intensidad por debajo de dicho umbral pertenecen al fondo.

2.1.4.2.1.1 Método Otsu para el umbralado

El método Otsu de umbralado, para su correcto funcionamiento, supone que los pixeles de la imagen $f(x, y)$ a binarizar pueden ser separados a través de un umbral u (a determinar) en dos clases: C_1, la clase del objeto u objetos de interés, y C_2, la clase de los pixeles de fondo.

El método de Otsu se fundamenta en la técnica del análisis discriminante al maximizar alguna medida que permita separar clases: C_1y C_2. Una de estas medidas, de acuerdo con el trabajo de Otsu, y que es la usada en el presente trabajo es la siguiente:

$$J_1(u) = \frac{P_1(u)P_2(u)[\mu_1(u) - \mu_2(u)]^2}{P_1(u)\sigma_1^2(u) + P_2(u)\sigma_2^2(u)} \quad (\mathbf{7})$$

Donde

$$P_1(u) = P_r(C_1) = \sum_{r=0}^{u} p(r) \quad (\mathbf{8})$$

Donde $P_r(C_1)$ es la probabilidad de que el valor r caiga en la clase C_1

$$P_2(u) = P_r(C_2) = \sum_{r=u+1}^{L-1} p(r) = 1 - P_1(u) \quad (\mathbf{9})$$

De igual manera, ocurre con el valor de $P_r(C_2)$, si tomamos los dos clases para los puntos, la suma de P_1 y P_2 evidentemente da 1.

$$\mu_1(u) = \sum_{r=0}^{u} rP_r(r|C_1) = \frac{1}{P_1(u)} \sum_{r=0}^{u} rp(r) \quad (\mathbf{10})$$

$$\mu_2(u) = \sum_{r=u+1}^{L-1} rP_r(r|C_2) = \frac{1}{P_2(u)} \sum_{r=u+1}^{L-1} rp(r) \quad (\mathbf{11})$$

Donde μ_1 y μ_2 son las medias de cada clase calculadas usando el previo conocimiento de los valores de probabilidad antes mencionados.

$$\sigma_1^2(u) = \sum_{r=0}^{u} (r - \mu_1(u))^2 P_r(r|C_1)$$

$$= \frac{1}{P_1(u)} \sum_{r=0}^{u} (r - \mu_1(u))^2 p(r) \quad (\mathbf{12})$$

$$\sigma_2^2(u) = \sum_{r=u+1}^{L-1} (r - \mu_2(u))^2 P_r(r|C_2)$$

$$= \frac{1}{P_2(u)} \sum_{r=u+1}^{L-1} (r - \mu_2(u))^2 p(r) \quad (\mathbf{13})$$

Donde σ_1^2 y σ_2^2 son las varianzas de cada clase calculadas por medio de las medias y las probabilidades ya mencionadas.

Para poder maximizar el criterio dado por la *ecuación (7)* las medidas de las dos clases deberían estar bastante bien separadas y las varianzas deberían ser lo más pequeñas posibles. Si esto no sucede, el valor del umbral obtenido simplemente no producirá el resultado deseado. Una imagen con un fondo muy grande comparado con el objeto u objetos en la imagen puede también dar lugar a valores de umbral que produzcan resultados indeseados.

El valor óptimo u^* puede encontrarse al buscar en el rango $[0, L-1]$ el valor de u que maximice la *ecuación (7)*. Esto es:

$$u^* = \arg \max_{0 \le u \le L-1} J_1(u) \quad \mathbf{(14)}$$

La ventaja principal del método Otsu es que no hace ninguna suposición acerca de las densidades $P_1(u)$ y $P_2(u)$, asume que pueden ser descritas sólo en términos de sus medidas y varianzas, lo que no necesariamente es cierto en el caso general.

Una de las principales desventajas de este método es la suposición de que el histograma de la imagen es bimodal, esto es, que los pixeles de la imagen pueden ser clasificados en sólo dos clases. Para más de dos clases de pixeles en la imagen, el método debe ser modificado de manera que varios umbrales puedan ser definidos de tal forma que permitan maximizar la varianza dentro de la clase y minimizar la varianza entre clases [11].

2.1.4.3 Etiquetado de componentes conexas

El etiquetado de componentes conexas, consiste en agrupar pixeles de una misma región dentro de la imagen, para lo cual les asigna la misma etiqueta a cada uno de ellos.

El concepto de componentes conexas es el siguiente: todos los pixeles que tienen un mismo valor binario "1" y están conectados entre sí (usando 4-conectividad u 8-conectividad) por un camino o conjunto de pixeles todos con ese mismo valor binario se les asigna una misma etiqueta identificativa, que debe ser única de la región a la cual pertenecen los pixeles y constituye su identificador.

Una de las operaciones más comunes en tratamiento de imágenes digitales consiste en encontrar las componentes conexas en una imagen. Por ejemplo, en tareas de segmentación, los puntos (pixeles) de una componente conexa forman una región candidata para representar un objeto (o parte de él) en una imagen.

Un algoritmo de etiquetado de componentes conexas encuentra todas las componentes de una imagen y asigna una única etiqueta a todos los puntos que están en la misma componente conexa [11].

2.1.4.3.1 Algoritmo iterativo

El algoritmo iterativo no usa almacenamiento auxiliar para producir una imagen etiquetada a partir de una imagen binaria. Consta de tres pasos básicos:

1. De etiquetado inicial

Dada una imagen binaria *b(x, y)*. Barrer *b(x, y)* hasta encontrar un pixel de tipo objeto (con valor 1 o L-1) aun no etiquetado y asignarle una nueva etiqueta E. Esto da como resultado la imagen $e_1(x, y)$.

2. De propagación de las etiquetas de arriba hacia abajo

Barrer $e_1(x, y)$ de arriba hacia abajo hasta encontrar un pixel etiquetado y propagar su etiqueta a sus vecinos, según la métrica elegida. Esto da como resultado la imagen $e_2(x, y)$.

3. De propagación de las etiquetas de abajo hacia arriba

Barrer $e_2(x, y)$ de abajo hacia arriba hasta encontrar un pixel etiquetado y propagar su etiqueta a sus vecinos, según la métrica elegida. Esto da como resultado la imagen $e_f(x, y)$.

En la figura 9 (a) se muestra una imagen binaria. En las figuras 9 (b-d) se muestra la secuencia de etiquetados hasta obtener la imagen etiquetada final [11].

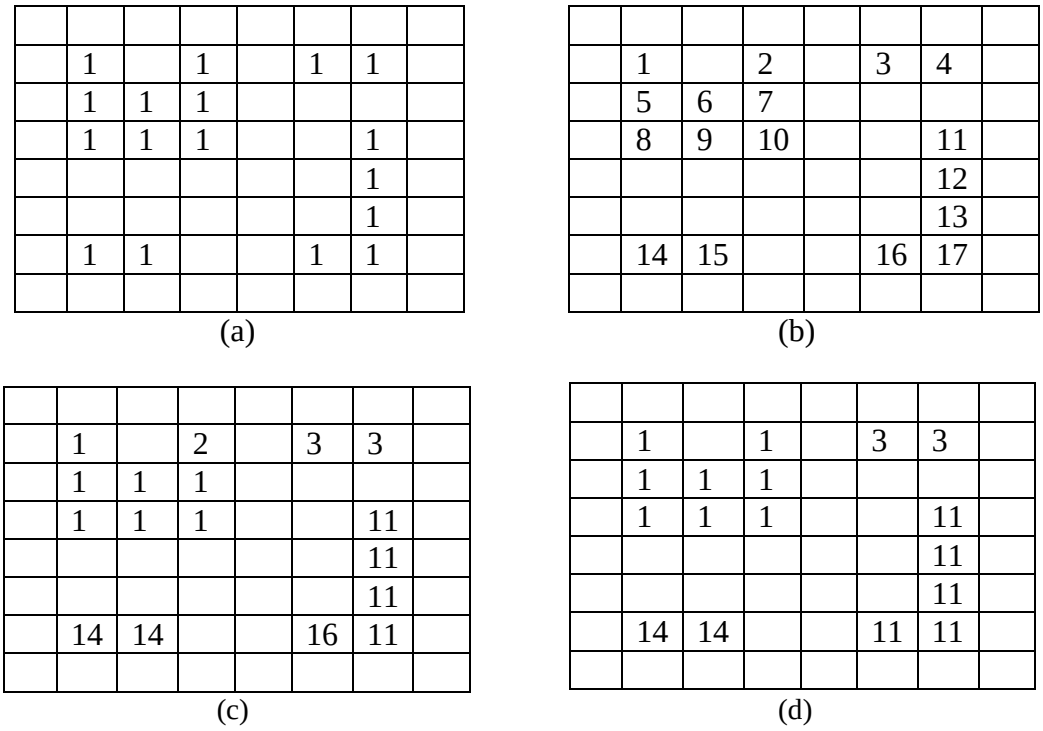


Figura 9 Una imagen binaria, (b,d) secuencia de etiquetados

2.1.5 Morfología Matemática

La descripción básica de la Morfología Matemática descansa en la 'teoría de conjuntos' cuyos primeros trabajos se deben a Minkowski y Hadwiger. La continuación de estos trabajos de investigación, bajo la impulsión y reformulación de Matheron y Serra, se darían posteriormente a conocer bajo la denominación de Morfología Matemática, como una técnica no lineal de tratamiento de señales.

La mayor parte de esta teoría ha sido desarrollada en el *Centre de Morphologie Mathématique (CMM) de l'Ecole des Mines de Paris*.

Actualmente, el ámbito y alcance de los procesamientos morfológicos es tan amplio como el propio procesamiento de imágenes. Se pueden encontrar aplicaciones tales como la segmentación, restauración, detección de bordes, aumento de contraste, análisis de texturas, compresión, etc.

La palabra morfología significa forma y estructura de un objeto. Para imágenes binarias se definen operaciones morfológicas con las que se constituye una poderosa herramienta de extracción de componentes de imagen útiles en la representación y descripción de la forma de las regiones.

Toda operación morfológica es el resultado de una o más operaciones de conjuntos (unión, intersección, complementación, etc.) haciendo intervenir dos conjuntos X, Y, ambos subconjuntos de un conjunto en el espacio Z^2. De los dos subconjuntos, Y recibe el nombre de elemento de estructura que, para operar con X, se desplazará a través del espacio Z^2 [12].

A continuación se presentan las definiciones de los operadores morfológicos fundamentales para las imágenes binarias.

2.1.5.1 Dilatación

Un operador $\delta: X \to X$ se denomina dilatación en el caso que conmute con el supremo de una colección de valores:

$$\delta\left(\bigvee_{i \in I} x_i\right) = \bigvee_{i \in I} \delta(x_i) \qquad (\mathbf{15})$$

Donde I es cualquier conjunto de índices y $\{x_i\}$ es una colección arbitraria de valores $x_i \in X$.

El resultado de la dilatación es el conjunto de puntos origen del elemento de estructura Y, tales que el elemento de estructura contiene algún elemento del conjunto X, cuando el elemento se desplaza por el espacio que contiene a ambos conjuntos:

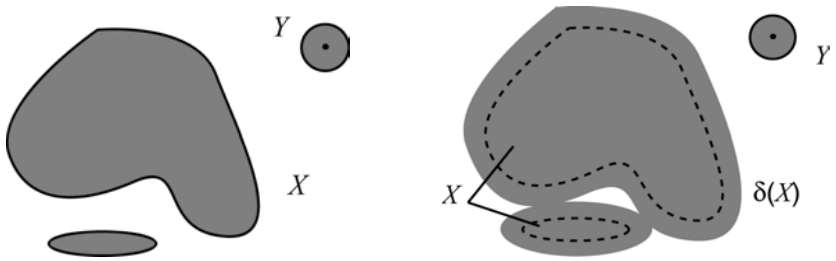
$$\delta_Y(X) = \{x | Y_x \cap X \neq 0\} \qquad \mathbf{(16)}$$

Esta última ecuación puede rescribirse como una unión de conjuntos trasladados. Las traslaciones vienen definidas por el dominio del elemento de estructura:

$$\delta_Y(X) = \bigcup_{s \in Y} X_s \qquad (\mathbf{17})$$

El efecto de una operación de dilatación puede observarse en la figura 10, en donde un elemento de estructura Y de forma de disco circular aumenta la definición del objeto X.

El resultado de la dilatación en señales bidimensionales de escala de grises (imágenes) es, generalmente, una señal de mayor valor, es decir, una imagen más clara, puesto que la dilatación maximiza el valor de la señal.



(a) (b)

Figura 10 Dilatación de X por el elemento de estructura Y. El conjunto X aumenta su definición

2.1.5.2 Erosión

Una erosión es una operación que conmuta con el ínfimo. Dado un retículo completo *X*, una erosión es una función ε: $X \rightarrow X$ en la que:

$$\varepsilon\left(\bigwedge_{i \in I} x_i\right) = \bigwedge_{i \in I} \varepsilon(x_i) \qquad (\mathbf{18})$$

Donde *I* es cualquier conjunto de índices y $\{x_i\}$ es una colección arbitraria de valores $x_i \in X$.

La transformación de erosión es el resultado de comprobar si el elemento de estructura *Y* cabe totalmente dentro del conjunto *X*. Cuando esto no ocurre, el resultado de la erosión es el conjunto vacío.

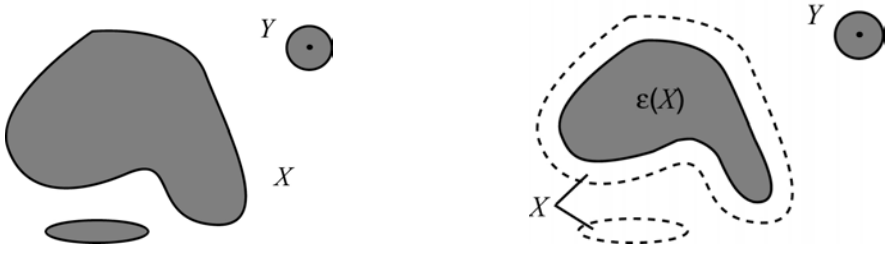
La erosión de un conjunto *X* por un elemento de estructura *Y* se define como el conjunto de puntos o elementos *x*, pertenecientes a *X*, de forma que cuando el elemento de estructura *Y* se traslada a ese punto, el elemento queda incluido en *X*:

$$\varepsilon_Y(X) = \{x | Y_x \subseteq X\} \qquad (\mathbf{19})$$

La operación anterior puede reformularse en términos de una intersección de conjuntos trasladados. Las traslaciones vienen determinadas por el elemento de estructura Y:

$$\varepsilon_Y(X) = \bigcap_{s \epsilon Y} X_s \qquad (\mathbf{20})$$

El efecto de una operación de erosión puede observarse en la figura 11, en la que un elemento de estructura *Y*, en forma de disco circular, hace desaparecer las estructuras de menor tamaño al elemento.



(a) (b)

Figura 11 Erosión de X por el elemento de estructura Y. Los elementos conectados del conjunto X más pequeños que Y son eliminados

2.1.5.3 Apertura y Cierre

Generalmente, en un retículo completo X, la dilatación $\rightarrow X$ $\delta(X)$ y la erosión $X\rightarrow$ $\varepsilon(X)$ son operaciones que no admiten inversa, por lo que, no hay manera de determinar el origen X desde las imágenes $\delta(X)$ o $\varepsilon(X)$. Sin embargo, es posible, mediante una adjunción de operadores básicos aproximarse a la forma original con base a la dualidad que poseen.

2.1.5.3.1 Apertura

La apertura de una señal *f* por un elemento de estructura *Y* se denota por $\gamma_Y(f)$ y se define como la erosión de f por *Y*, seguida de la dilatación con el mismo elemento de estructura:

$$\gamma_Y(f) = \delta_Y\big(\varepsilon_Y(f)\big) \qquad (\mathbf{21})$$

La apertura de una imagen es independiente del origen del elemento de estructura, puesto que si la erosión se corresponde con una intersección de traslaciones, la dilatación que sigue es una unión de traslaciones en dirección opuesta.

El efecto de una operación de apertura puede observarse en la figura 12, en la que un elemento de estructura *Y*, en forma de disco circular, provoca en la erosión la desaparición de una estructura que, en la operación de dilatación, no se puede recuperar.

(a) (b)

Figura 12 Apertura morfológica del conjunto X por el elemento de estructura Y. Eliminación de objetos menores en tamaño al del elemento de estructura. La apertura redondea las convexidades importantes

2.1.5.3.2 Cierre

El cierre de una señal f por un elemento de estructura *Y* se denota por $\varphi_Y(f)$ y se define como la dilatación de f por *Y*, seguida de la erosión con el mismo elemento de estructura:

$$\varphi_Y(f) = \varepsilon_Y\big(\delta_Y(f)\big) \qquad (\mathbf{22})$$

Al igual que la apertura, el cierre de una imagen es independiente del origen del elemento de estructura. El cierre de un conjunto X por un elemento de estructura con forma de disco se ilustra en la figura 13. El cierre es el espacio descrito por el elemento de estructura cuando es forzado a estar fuera de los conjuntos [12].

(a) (b)

Figura 13 Apertura morfológica del conjunto X por el elemento de estructura Y. El cierre redondea las concavidades importantes

2.1.5.4 Apertura generalizada

La transformación *hit or miss* (acierta o falla) de X por un par disjunto (A, B) de elementos de estructura, está definida como el operador de conjuntos:

$$X \otimes (A, B) = \varepsilon_A(X) \cap \varepsilon_B(X^c) \qquad (\mathbf{23})$$

En donde A es el elemento de estructura *hit* y B el elemento de estructura *miss*. Por *hits* nos referimos a la intersección con los objetos de interés de X, mientras que por *miss* nos referimos a la intersección con el fondo de X, por ejemplo: el conjunto complemento X^c. Así, el operador *hit or miss* se define como la intersección de la erosión de los objetos y la erosión del fondo. Para abreviar, nos referiremos de ahora en adelante al par disjunto (A, B) de elementos de estructura como un solo elemento de estructura con ambos conjuntos. Se debe hacer notar que ambos están definidos con respecto al mismo centro.

La apertura ordinaria $\gamma_A(X) = \delta_A(\varepsilon_A(X))$ de X por el elemento de estructura A es una erosión seguida por una dilatación. Remplazando la erosión por el operador *hit or miss* definido anteriormente, nos permite construir lo que llamamos la apertura generalizada.

Específicamente, definimos la apertura generalizada del objeto de interés de X por (A, B) como la transformación de conjuntos:

$$\psi_{(A,B)}(X) = \delta_A[X \otimes (A, B)] \qquad (\mathbf{24})$$

Donde sea que (A, B) sean usados, usaremos la notación simplificada $\psi(X)$ [13].

2.1.5.5 Operador *Top-Hat*

Una apertura o un cierre con un elemento de estructura que no ajusta dentro de estructuras relevantes de la imagen, es usado para eliminar dichos elementos de la imagen. Estas estructuras se recobran a través de la diferencia aritmética entre la imagen y su apertura, o entre el cierre y la

imagen. Estas diferencias aritméticas son la base de la definición de los operadores *top-hat* (sombrero de copa) morfológicos [14].

2.1.5.5.1 Operador White Top-Hat

El *White top-hat* (*WTH*) -Sombrero de copa blanco- de una imagen *f* es la diferencia entre la imagen original *f* y la apertura γ:

$$WTH\,(f) = f - \gamma(f) \qquad (\mathbf{25})$$

Mientras que la apertura es una transformación de imagen anti extensiva, los valores de escala de grises de un *WTH* son siempre mayores o iguales que cero [14].

2.1.5.5.2 Operador Black Top-Hat

El *Black top-hat* (*BTH*) -Sombrero de copa negro- de una imagen *f* esta simplemente definido como la diferencia entre el cierre φ de la imagen original y la imagen original *f*:

$$BTH(f) = \varphi(f) - f \qquad (\mathbf{26})$$

Debido a la propiedad extensiva del operador cierre, los valores de las imágenes *BTH* son siempre mayores o iguales que cero [14].

2.1.5.5.3 Mejoramiento del contraste

Podemos definir el contraste como la diferencia de intensidad de iluminación en la gama de blancos y negros o en la de colores de una imagen. El contraste muestra las variaciones locales del brillo.

Cuando se pretende mejorar el contraste de una imagen se desea que "los pixeles claros se aclaren más" y "los pixeles oscuros se oscurezcan más", lo cual es el fundamento para dar mayor nitidez a las formas presentes en la imagen.

La mejora del contraste en la imagen se refiere a la acentuación o agudizamiento de las características de la imagen para hacer una visualización y representación gráfica más útil para el ojo humano.

Un operador de mejora de contraste morfológico puede ser obtenido computando en paralelo los *top-hat* blanco y negro de la imagen. El *top-hat* blanco de la imagen es entonces añadido a la imagen original para realzar objetos brillantes y el *top-hat* negro es restado de la imagen resultante para realzar los objetos oscuros. Este operador de contraste es denotado con K^{TH}:

$$K^{TH} = id + WTH_B - BTH_B = id + id - \gamma_B - \varphi_B + id = 3id - \varphi_B - \gamma_B \qquad (\mathbf{27})$$

Una imagen de un pedazo de lana mostrando un contraste pobre se observa en la figura 14 [14].

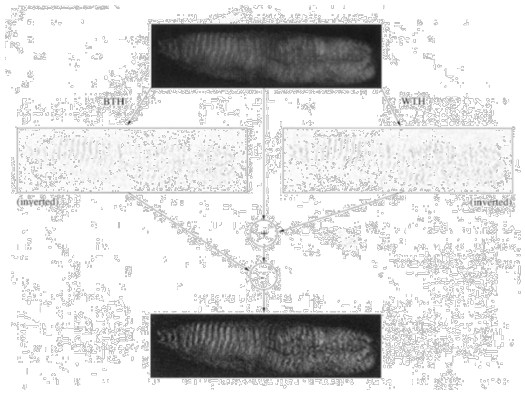


Figura 14 Mejoramiento del contraste aplicado a la imagen de un pedazo de lana

2.2 Credencial para Votar con fotografía

2.2.1 Características generales de la Credencial para Votar con fotografía

La credencial para votar deberá contener, cuando menos, los siguientes datos del elector: entidad federativa, municipio y localidad que correspondan al domicilio; distrito electoral uninominal y sección electoral en donde deberá votar; apellido paterno, apellido materno y nombre completo; domicilio, sexo; edad y año de registro; clave de registro; lugar para asentar la firma; huella digital y fotografía del elector, espacios necesarios para marcar el año en que se vote y la elección de que se trate, así como la firma impresa del Secretario Ejecutivo del Instituto Federal Electoral.

2.2.1.1 Anverso

Impreso en dos tintas (gris y negro) sobre fondo blanco. Parte superior: franja horizontal de color gris sólido a lo largo de la credencial y de 1.4cm de ancho. Sobre esta banda en la esquina superior izquierda se encuentra el Escudo Nacional y a su derecha, impreso en negro, se lee INSTITUTO FEDERAL ELECTORAL, REGISTRO FEDERAL DE ELECTORES, CREDENCIAL PARA VOTAR.

Debajo de esa franja y cargado a la izquierda ocupando el resto de la credencial, la silueta de la República Mexicana en color gris sólido sobre un fondo tramado con líneas blancas y grises.

Sobre estos elementos (siluetas y líneas) están preimpresos los datos fijos (nombre, edad, sexo, domicilio, folio, año de registro, clave de elector, estado, municipio, distrito, localidad y sección); abajo de las palabras nombre y domicilio, así como al resto de los datos fijos, están impresos los datos variables del ciudadano en color negro. A la derecha y ocupando un área de 3.2cm de altura por 2.54cm de ancho, se encuentra el espacio destinado a la fotografía. Cerca de la esquina inferior izquierda de este espacio, desfasado hacia la izquierda, se encuentra el holograma (imagen de seguridad) con el logotipo del Padrón Electoral (figura 15).

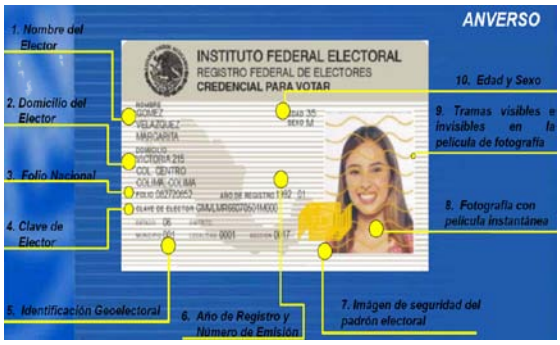


Figura 15 Anverso de la Credencial para Votar con fotografía

2.2.1.2 Reverso

Impreso en dos tintas (gris y negro) sobre fondo blanco (figura 16). Debajo de esta y a la derecha, está la superficie destinada para poner la huella digital, calada en blanco, con un área de 3.2cm de altura por 2.54cm de ancho.

Abajo, a la izquierda del espacio para la huella, se encuentra el espacio en blanco para la firma. Sus dimensiones son de 4.8cm de ancho por 1cm. de altura.

En el extremo inferior se encuentra el área destinada a los años de elección a partir de 1994, dividido en dos bloques. El primero, a la izquierda, de 4 cuadros para las elecciones federales y el segundo, a la derecha, de 15 cuadros para las elecciones locales extraordinarias.

En el extremo izquierdo de manera vertical, entre el código de barras y el bloque de recuadros para las elecciones federales, se localizan doce dígitos impresos en color negro que corresponden al código para el reconocimiento óptico de los caracteres (OCR por sus siglas en inglés) con equipo auxiliar, en un área de 3cm de altura por a.4cm de ancho.

En el extremo izquierdo de la credencial, paralelo al lado derecho del OCR, se lee la leyenda: “Este documento es intransferible. No es válido si presenta tachaduras o enmendaduras”. “El titular está obligado a notificar el cambio de su domicilio en los 30 días siguientes a que éste ocurra”.

Entre está leyenda y el espacio para la huella se encuentra el que corresponde a la firma del Director General del Instituto Federal Electoral.

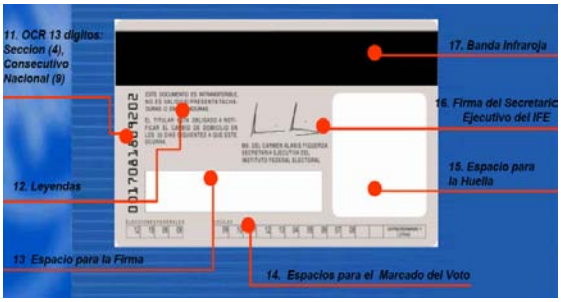


Figura 16 Reverso de la Credencial para Votar con fotografía

2.2.2 Medidas de seguridad de la Credencial para Votar con fotografía

2.2.2.1 Anverso

Veremos estas medidas de seguridad tanto en el anverso como en el reverso de la Credencial.

2.2.2.1.1 Laminado

Ambas superficies estarán cubiertas con un laminado. En el anverso de la credencial, este laminado lleva una trama con el Escudo Nacional que es solo visible bajo luz ultravioleta (figura 17).

Figura 17 Laminado con tinta invisible

2.2.2.1.2 Fotografía

La fotografía contiene una trama con las siglas “IFE” sólo visibles bajo luz ultravioleta (UV). Asimismo, tendrá una trama (senoidal) de seguridad visible cuya característica fundamental es la de no distorsionar la imagen del rostro del ciudadano y permitir su digitalización (figura 18).

2.2.2.1.3 Trama de seguridad

La trama de seguridad ultravioleta (invisible) que estará en la hoja del laminado que cubrirá el anverso de la credencial, está conformada por varios escudos nacionales. La trama de seguridad ultravioleta (invisible) del papel fotográfico la compondrán las siglas IFE ubicadas en la distinta posición. La trama de seguridad del papel fotográfico serán unas líneas onduladas (figura 18).

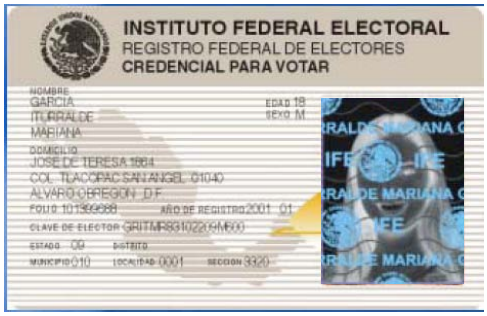


Figura 18 Fotografía impresa y sus candados de seguridad

2.2.2.1.4 Holograma

Bajo el laminado que cubrirá el anverso de la credencial está el holograma, que consiste en el logotipo del Padrón Electoral, cuya ubicación estará a la altura de la esquina inferior izquierda del espacio destinado a la fotografía y desfasado hacia este lado (figura 19).

Figura 19 Ubicación del holograma en la credencial (anterior y actual)

2.2.2.2 Reverso

En la parte superior de la credencial, se encuentra el código de barras cubierto por una franja negra (filtro infrarrojo) de 1.3cm de ancho, que se extiende hasta los bordes de la credencial. Este código de barras bidimensional es utilizado para autentificar al ciudadano mediante equipo especial al momento de la entrega de la credencial (figura 20) [1].

Figura 20 Código de barras de la Credencial para Votar con fotografía

2.2.3 Microimpresiones

La definición de lo que es el microtexto en el ambiente jurídico en México ha cambiado, ya que antes se definía como “todo texto que es tan pequeño que no se puede leer a simple vista”, pero como esa definición dependía más bien de cuán buena tenía su agudeza visual la persona que lo estaba revisando; por ello la nueva definición pasó a ser: “Todo texto impreso que mida menos de un punto en el documento es considerado microtexto”.

Ahora bien, teniendo en cuenta estas dos definiciones de microtexto o microimpresión (ya que en realidad no se han terminado de poner de acuerdo en cuál es la definición más aceptada aquí en México), se pueden dar los siguientes ejemplos de microimpresión usado como candado de seguridad en diferentes documentos, ya sea de identificación o valorados.

En nuestro país hay muchos tipos de documentos de identificación, aunque algunos de ellos sólo son válidos para las dependencias que los expiden, tales como las credenciales de las dependencias de educación, los gafetes de identificación de empresas para sus trabajadores y otros más. Otros documentos son considerados de identificación oficial; algunos ejemplos de estos son la Credencial para Votar con Fotografía (del Instituto Federal Electoral - IFE), el pasaporte, la visa, la cartilla militar, etc., aunque en realidad, de acuerdo a la definición vigente de documento de identificación oficial, se necesita que el documento sea expedido por una dependencia gubernamental; actualmente muchos de los documentos de identificación son expedidos por organizaciones independientes [15].

2.2.3.1 Características

En el año 2001 se aprobó el modelo de la Credencial para Votar con Fotografía a la cual se le hicieron algunas modificaciones como son, la tinta invisible personalizada que ya no solo tiene el escudo nacional, sino que ahora también tiene el nombre del ciudadano, la fotografía es digital de 800 puntos por pulgada, y lo más importante y que es lo que nos ocupa: en el anverso y en el reverso se le agregó una microimpresión cuyas características son las siguientes [15]:

- Tamaño de 0.5 punto
- Fuente tipo Arial
- Color negro

2.2.3.2 Ubicación en la Credencial

La microimpresión en la Credencial para Votar se puede ubicar en:

- El anverso; que aparece como un marco de la fotografía en el cual se puede leer el nombre del ciudadano y la fecha de expedición de su credencial en el contorno de la fotografía (Figura 21).

Figura 21 Línea de microimpresión en el anverso de la Credencial para Votar con fotografía

- El reverso de la Credencial, en el contorno del recuadro para la firma; con las mismas características que la microimpresión del anverso, pero esta vez solo con el nombre del ciudadano repetido en todo el contorno (Figura 22) [15].

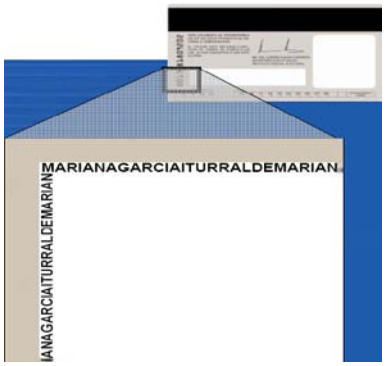


Figura 22 Línea de microimpresión en el reverso de la Credencial para Votar con fotografía

2.2.4 Algunos métodos de falsificación

Muchas credenciales para votar dejan al descubierto el proceso que los falsificadores utilizan para clonar los documentos. Hay desde los más sofisticados y casi imposibles de detectar, hasta los más burdos y rudimentarios.

El más elemental de los casos es cuando la persona utiliza una credencial original, de la que con precaución retira la película protectora de la tarjeta, remueve la fotografía, pega el “nuevo” rostro y sella todo de nuevo, quedando así, una imagen que no corresponde al dueño de la identificación.

En otros se utiliza el sistema de fotocopiado o impresión de color, en la que se pueden o no ingresar datos reales y se agrega la fotografía del interesado, una imagen completa que luego es adherida a cualquier tarjeta de plástico, como por ejemplo de telefonía, de descuentos en supermercados, de seguros de vida, etc.

En los métodos antes descritos, cambian el nombre y fotografía del individuo, pero como el microtexto no es un candado muy conocido, no le prestan atención, por lo cual es una buena manera de autentificar una credencial de elector.

En algunas identificaciones los falsificadores utilizan el método antes descrito, pero al final del proceso le colocan una película con cinta adhesiva o enmicado, consiguiendo una rigidez similar e las originales del IFE. Este método es el más utilizado.

Un grupo menor de estos documentos falsos, puede engañar hasta el más experto: se auxilian de impresiones de mejor nitidez. Sus "creadores" ponen especial cuidado en emular los candados de seguridad y son recubiertas con mica en extremo parecida al original.

En la zona fronteriza abundan las licencias de conducción falsas, que también poseen métodos de clonación similares a los descritos en las credenciales del IFE.

2.2.5 La confiabilidad de los candados de seguridad en la Credencial para Votar

Hasta el momento, no existe el convencimiento de que haya identificación falsa que emule con gran exactitud todos los candados de seguridad de la credencial para votar con fotografía; esta fidelidad impresa nos asegura que en el momento que no cumpliera con alguna de las características establecidas indica que se trata de un documento apócrifo.

Se ha detectado que en el sur de México existen grupos que utilizan clonaciones para ayudar a los sudamericanos a que logren el "sueño americano". Existen datos que indican que a muchas personas a las que se les extravía la identificación del IFE, están expuestas a que sus documentos puedan ser mal utilizados; no obstante, existe un acuerdo entre las instituciones públicas del IFE, para que las micas que son olvidadas se recojan y se resguarden en las oficinas del organismo electoral para su posterior destrucción.

Desde hace ya algún tiempo, ha ido creciendo el número de las bandas delictivas que se dedican a falsificar este documento.

En el año 2004, circuló nacionalmente la declaración de Armando Granados Carreón, Director General de Averiguaciones Previas de la Fiscalía Especializada para la Atención de Delitos Electorales (FEPADE), dependiente de la PGR, donde el funcionario daba a conocer que existen más de 15 tipos de delitos que se pueden cometer con una credencial falsa: "Una mica falsa o alterada lo mismo sirve para que un indocumentado cruce el país rumbo a Estados Unidos sin problemas, o para que alguien cobre el pago de una extorsión telefónica a través del sistema de dinero en minutos". Además, informó que con frecuencia se presentan casos en los que los delincuentes sustraen recibos de teléfono y de luz, acuden con credenciales falsas a tiendas de autoservicio para conseguir electrodomésticos y visitan las agencias automotrices para comprar un coche. Incluso se advertía en la información, que se ha detectado un "mercado negro" en el cual los asaltantes venden las credenciales originales que encuentran en las carteras que roban. "Y ¡cuidado!, si alguien extravía o le roban su credencial y no la reporta a las autoridades, puede verse involucrado en serios problemas legales" advertía Granados Carreón [1].

CAPÍTULO III. SOLUCIÓN DEL PROBLEMA

3.1 Descripción general del sistema

La metodología que se propone en este trabajo es una herramienta de software diseñada para la autentificación del microtexto presente alrededor de la fotografía en el anverso y alrededor del área destinada para la firma en el reverso de las credenciales para votar con fotografía. Para poder realizar la validación, se tuvo la necesidad de usar diferentes herramientas de morfología y análisis de imágenes, dado que la microimpresión que existe en la credencial, no fue usada la mejor tecnología y por lo tanto el microtexto es muy ruidoso. Este sistema ha sido diseñado y construido de tal manera que, de forma automatizada, se muestren los resultados de una manera sencilla y entendible para el usuario. Los resultados obtenidos no determinan si la credencial en su totalidad es falsa o verdadera, sino nos detecta la precensia o no del microtexto en la Credencial y de estar presente nos valida su legitimidad. La pantalla principal de la interfaz gráfica desarrollada para el sistema se muestra en la figura 23.

Figura 23 Pantalla principal del sistema

3.2 Interfaz gráfica

La figura 24 muestra la pantalla principal del sistema teniendo abierta la imagen de una de las credenciales capturadas previamente.

Figura 24 Interfaz gráfica del sistema

La figura 25 muestra la pantalla principal del sistema en la que se muestran los resultados del recorte de las áreas de interés presentes en el anverso.

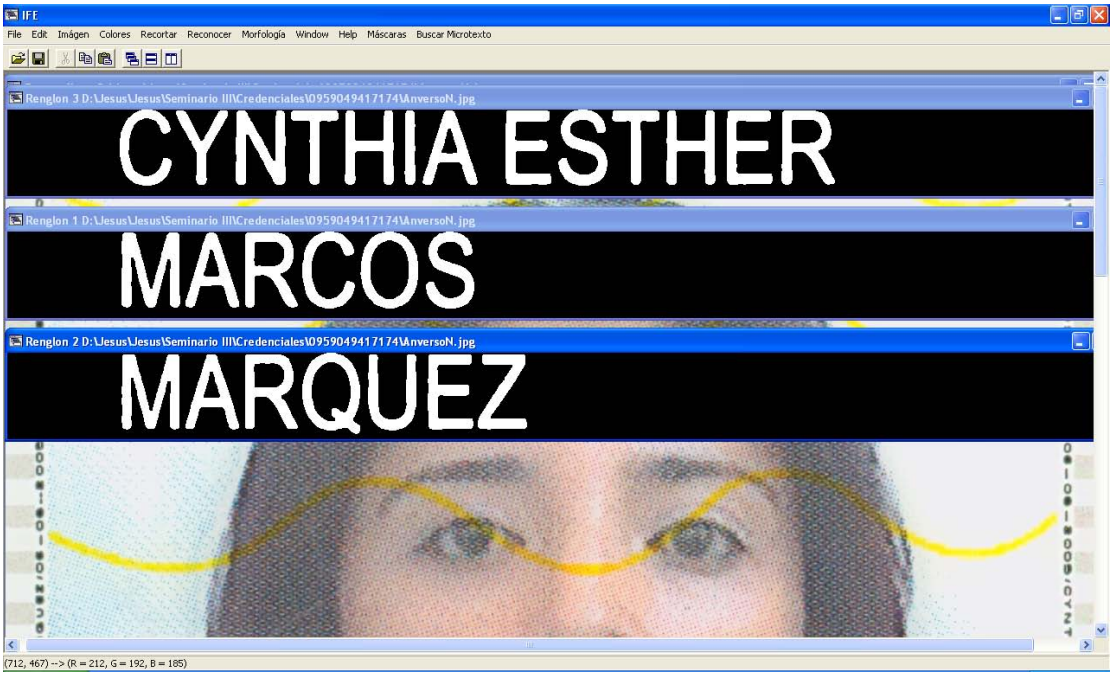


Figura 25 Interfaz gráfica conteniendo las áreas de interés del anverso recortadas

La figura 26 muestra la interfaz gráfica del sistema conteniendo el microtexto del anverso recortado.

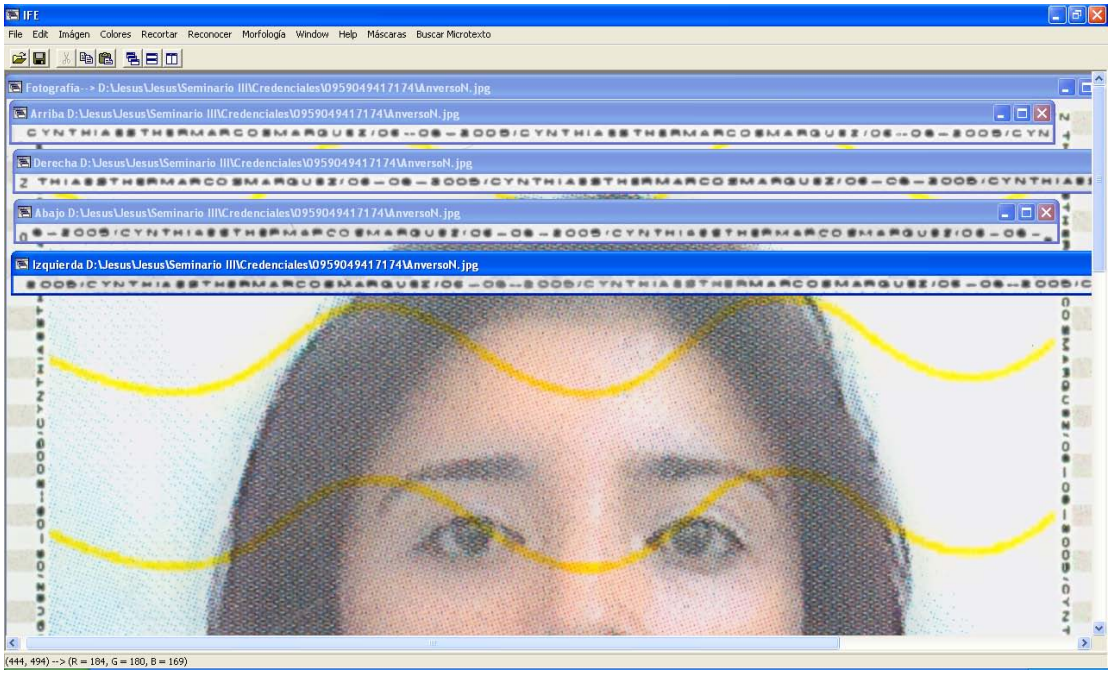


Figura 26 Interfaz gráfica y microtexto del anverso recortado

La figura 27 muestra la interfaz gráfica con el área de la firma recortada.

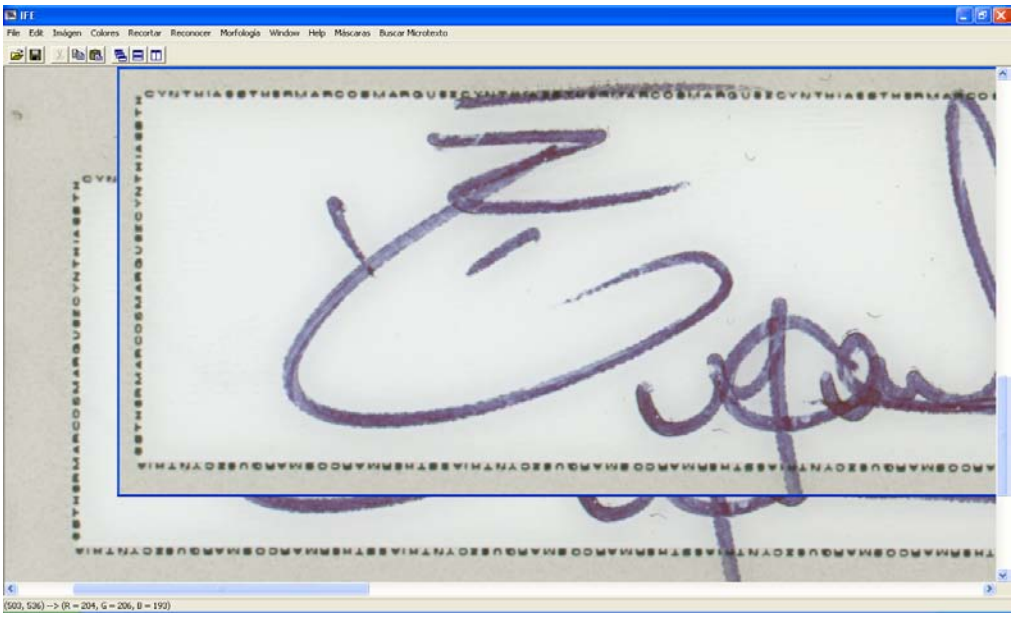


Figura 27 Interfaz con el recorte del área de la firma

En la figura 28 se muestra el recorte del microtexto en el área de la firma.

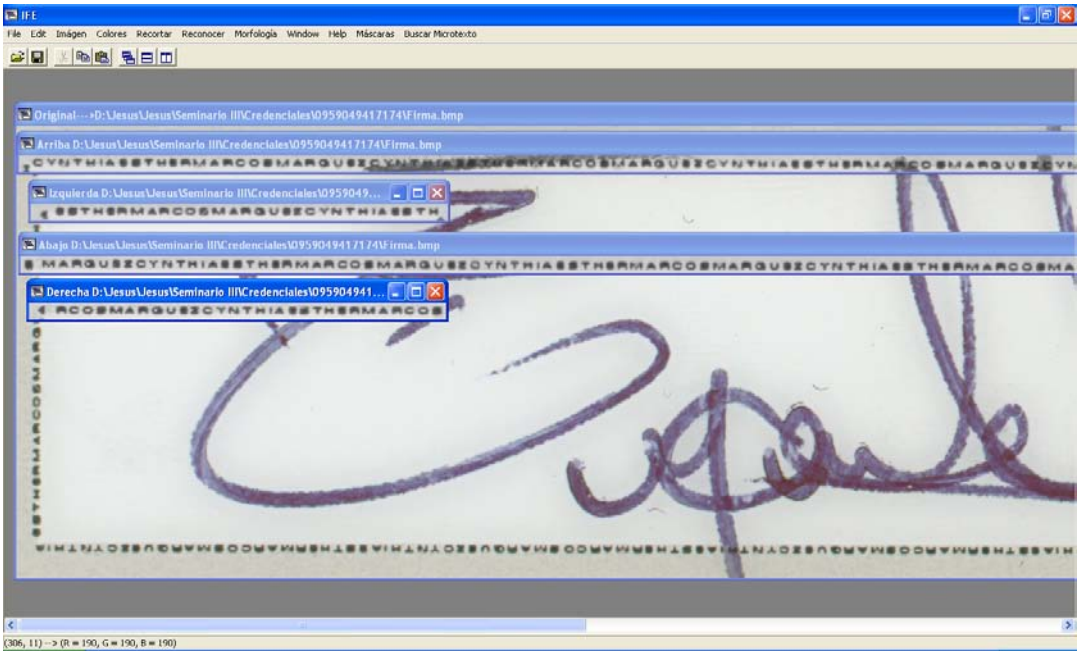


Figura 28 Interfaz gráfica con el recorte del microtexto en el reverso

3.3 Captura de las imágenes

Las imágenes de las credenciales fueron capturadas a 1200 ppp por ambos lados, gracias a un escáner modelo HP Scanjet 8200, sin más tratamiento de la imagen que las opciones por defecto (*default*) que brinda el escáner. Estas imágenes fueron guardadas en un disco duro externo Simple Tech de 500 GB de 7200 rpm.

Se escanearon 46 credenciales, de las cuales 14 son del modelo anterior al 2001, 27 son posteriores al 2001 y 5 son del modelo posterior al 2008. Estas imágenes fueron guardadas en un subdirectorio que lleva por nombre el código OCR que se encuentra en el reverso de la credencial como se describió en el capítulo anterior. Dentro de cada subdirectorio se encuentran 3 imágenes de las credenciales llamadas anverso, reverso y holograma, con un sufijo N o A dependiendo si son posteriores a 2001 (N) o anteriores a 2001 (A), lo que fue como un estándar para poder realizar las capturas de las credenciales.

Para capturar dichas imágenes, se usó un procedimiento normal de escaneo, el cual consiste únicamente en poner la credencial contra el vidrio y mantenerla pegada al borde del escáner como se muestra en la figura 29, para así evitar inclinaciones en la imagen digitalizada; además, se debe de dar la opción de que la credencial sea recortada del resto de la imagen lo más pegada a los límites de la credencial, dejando un pequeño espacio arriba, a la derecha y abajo, para poder realizar adecuadamente los recortes necesarios de la imagen durante las corridas de la aplicación.

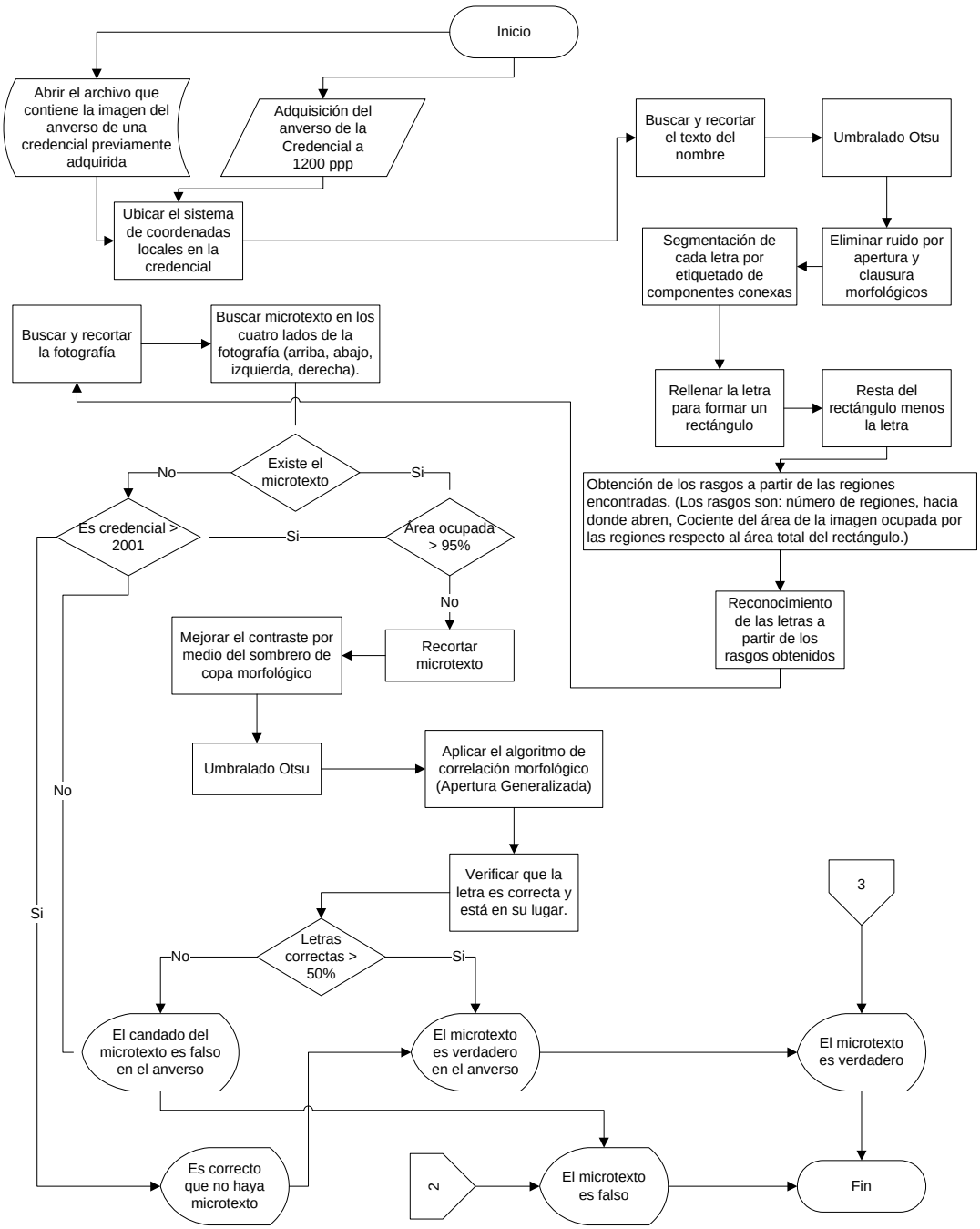
a) b)

Figura 29 Método de escaneo usado a) en el anverso b) en el reverso

3.4 Diagrama de bloques general

Para poder realizar la verificación automática del microtexto en el anverso y reverso de la Credencial para Votar con fotografía se implementó el sistema según el diagrama mostrado en la figura 30.

A)



B)

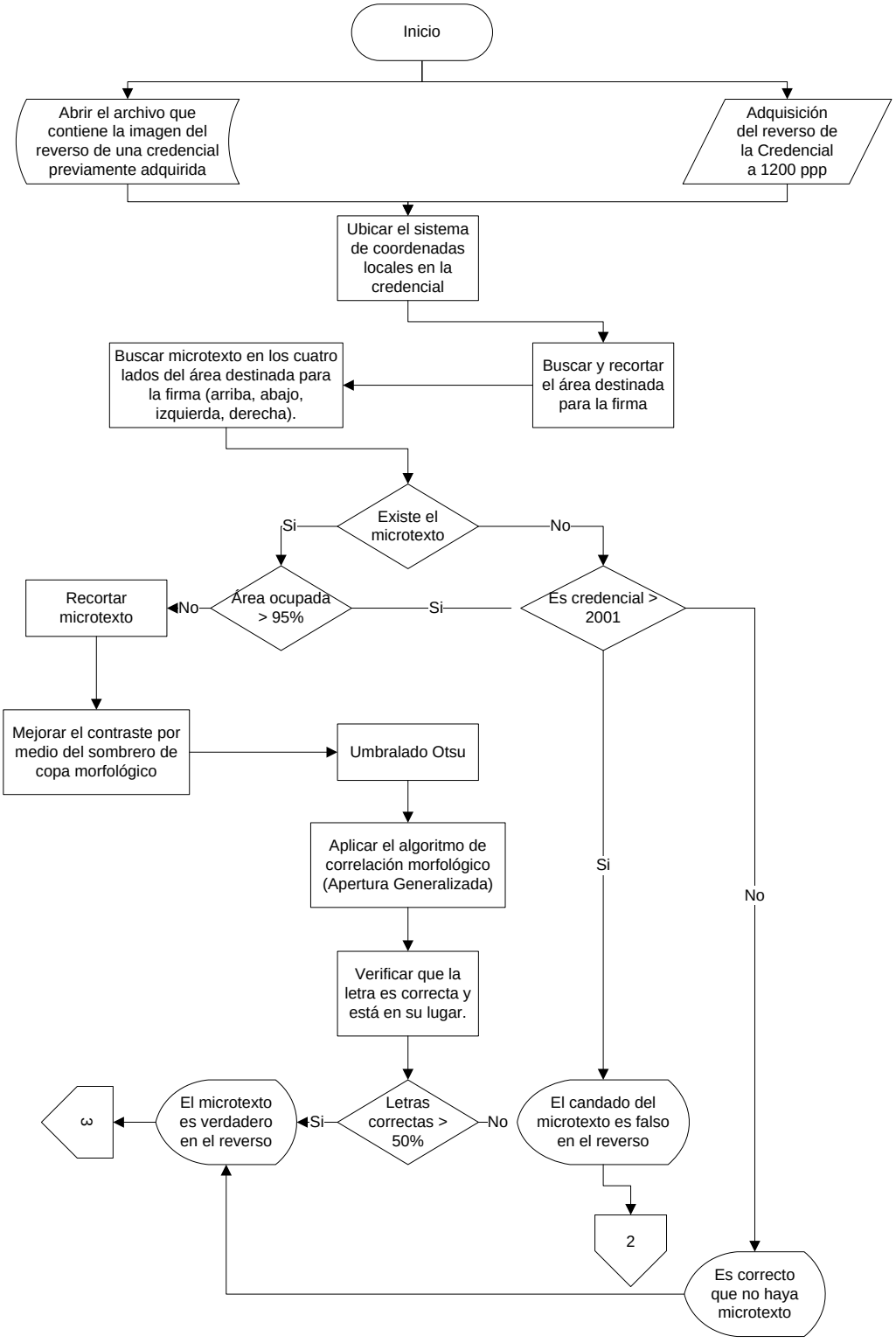


Figura 30 A) Descripción general del sistema para el anverso, B) Descripción general del sistema para el reverso

A continuación se describen en detalle cada uno de los pasos mencionados en el diagrama general del sistema.

3.4.1 Captura de la imagen del anverso o del reverso de la credencial

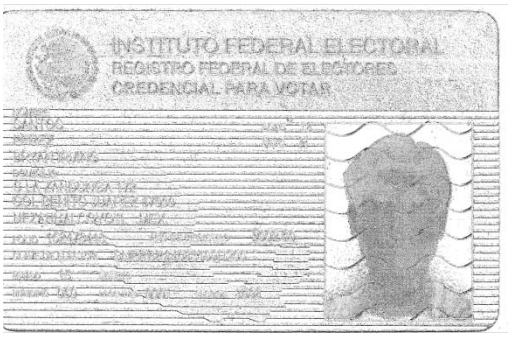
Primero que todo, para poder reconocer una credencial, se debe contar con las imágenes digitalizadas del anverso y del reverso de la Credencial para Votar con fotografía; en este caso ya contamos con una base de datos de 53 credenciales como se describe en el apartado 3.3, junto con el procedimiento para la captura de las mismas.

3.4.2 Ubicar el sistema de coordenadas locales en la credencial y recorte de la fotografía y los textos en el anverso de la credencial

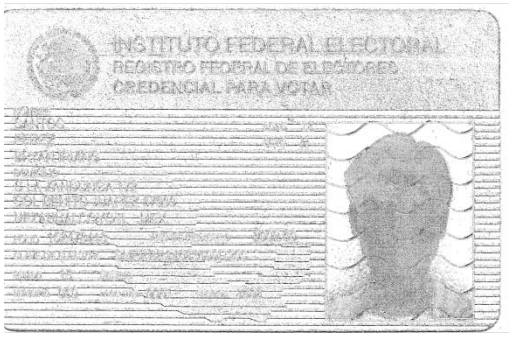
Para poder recortar el área de interés, primero se debe ubicar el sistema de coordenadas dónde comienza la credencial; para esto se aprovecha el hecho de que el escáner usa una superficie blanca para contrastar la imagen capturada con el fondo (aunque en realidad el fondo escaneado es en realidad un nivel de gris mayor que 200 y no el nivel blanco que es 255), ya que esto nos permite saber en primera instancia si la credencial fue escaneada pegada a su borde superior o la credencial tiene un poco del fondo blanco situado en su parte superior.

En caso de que la credencial tenga algo arriba de la superficie blanca del escáner, se usa la sombra creada por la credencial sobre la superficie blanca para detectar un nivel de gris menor que 200 y así saber en dónde comienza la credencial.

Para recortar la fotografía y los textos localizados en el anverso de las credenciales, fue necesario el uso de un detector de bordes. Fueron probados los detectores de Sobel, Prewitt, Frei-Chen y Roberts, cada uno con un umbral doble para segmentar la línea que marca el final del área de título de la credencial; el umbral seleccionado para el detector de Sobel es 20<u<60, para el de Prewitt se usó 15<u<40 y para el de Frei-Chen se usó 15<u<40; para Roberts, el umbral usado se detalla más adelante. Se decidió usar el gradiente cruzado de Roberts por ser el más sencillo computacionalmente, además de que para fines prácticos todos los detectores arrojaban resultados similares como se muestra en la figura 31, en la cual los bordes están presentados en color negro por ser imágenes invertidas.



A)



B)

C) *D)*

Figura 31 Resultados de la aplicación de los detectores de bordes(imagen invertida): A) Sobel. B) Prewitt, C) Frei-Chen, D) Roberts

El gradiente cruzado de Roberts nos permitió detectar el borde donde terminaba el área de título de la Credencial para Votar con fotografía en un tiempo razonablemente corto; para esto fue necesario usar, además, un umbral doble (7<u<15) con el fin de eliminar el exceso de ruido. Además, para determinar concretamente el final del área de titulo, se buscó una línea de más de 215 pixeles dentro del área sombreada en rojo en la figura 33.

Figura 32 Credencial original

Figura 33 Detector de bordes

Figura 34 Texto del nombre y texto del nombre umbralado

Una vez obtenida la posición en la que termina el área del título de la credencial, sabemos por consiguiente en dónde empieza el texto que dice “NOMBRE”. Para encontrar el texto del nombre, se umbraló la credencial usando el método Otsu y se buscó el siguiente renglón después del texto “NOMBRE” para así obtener el área mostrada en la figura 33, la cual contiene la información necesaria para verificar el microtexto en la credencial. Así mismo, con estas medidas, se pudo recortar la fotografía de la Credencial, pues sabíamos que el inicio de la fotografía está 80 pixeles más abajo que el final del área de título, que la fotografía mide como máximo 1580 pixeles de alto, y que usando el método de escaneo antes definido, que por el lado izquierdo la credencial siempre está escaneada en su borde exacto, entonces la fotografía estría limitada en su lado izquierdo a los 2560 pixeles y por la derecha, podemos tan solo quitar 152 pixeles al ancho máximo de la imagen.

Teniendo estos datos se obtiene el recorte de la fotografía (como se muestra en la figura 35) para su posterior uso.

Figura 35 Resultado del recorte de la fotografía

Una vez obtenida el área de la parte inferior izquierda de la figura 34, se usó el método de umbralado Otsu para binarizar la imagen y se eliminó el ruido aplicando una apertura y un cierre morfológicos. El resultado se muestra en la parte inferior derecha de la figura 34.

3.4.3 Segmentación de las letras a reconocer

Para poder reconocer las letras y saber el nombre del titular de la credencial, primero el texto fue separado en tres renglones como se muestra en la figura 36, teniendo así en el primer renglón el apellido paterno, en el segundo el apellido materno, y en el tercero el nombre o nombres del titular de la credencial.

Figura 36 Separación del texto del nombre en renglones

Posteriormente cada renglón fue analizado por separado, lo que se logró mediante el etiquetado de componentes conexas, etiquetando a cada una de las letras en el orden de izquierda a derecha, es decir, en una lista fueron guardadas las etiquetas y las posiciones de las letras, además de los máximos y mínimos en las coordenadas “x” y “y” para posteriormente ordenarlas de izquierda a derecha de acuerdo a su posición. Después de algunas pruebas, nos dimos cuenta de que algunas credenciales tienen el problema de que al umbralar y eliminar el ruido, se unen algunas letras (RA, LA y KA), por lo que creamos un algoritmo con el cual se detectan regiones de no más de 90 pixeles para separarlas por la mitad y así realizar el reconocimiento correcto.

3.4.4 Relleno de la letra, obtención de las áreas que describen la letra y extracción de las características

A partir del etiquetado se pudo conocer el alto y el ancho de cada letra y así poder trazar sobre la misma un rectángulo como se muestra en la figura 37.

Figura 37 Rectángulo relleno

Para obtener las áreas descriptoras de la letra, se necesita extraer el área ocupada por la letra del rectángulo descrito anteriormente. Como las imágenes son binarias, se aplicó la operación lógica *And* entre el rectángulo y la imagen de la letra negada para obtener las áreas que describen la letra; el resultado se muestra en la figura 38.

Figura 38 Extracción de regiones

Para obtener las características de cada región que componen cada letra, se usa nuevamente un algoritmo de etiquetado de componentes conexas haciendo un ordenamiento de arriba hacia abajo y de izquierda a derecha de las regiones, por medio de una lista de las mismas características que la usada para segmentar las letras. Con este algoritmo fue posible obtener las coordenadas límite de cada región y el número de pixeles que la componen. A partir de estos datos se obtuvieron los siguientes rasgos:

- Número de áreas: este rasgo fue obtenido con la longitud de la lista de áreas etiquetadas.

- Cociente del área de la imagen ocupada por las regiones respecto al área total del rectángulo: los algoritmos de etiquetado usados para obtener las regiones y segmentar las letras, nos dieron sus áreas totales, por lo que fue muy fácil realizar esta operación.

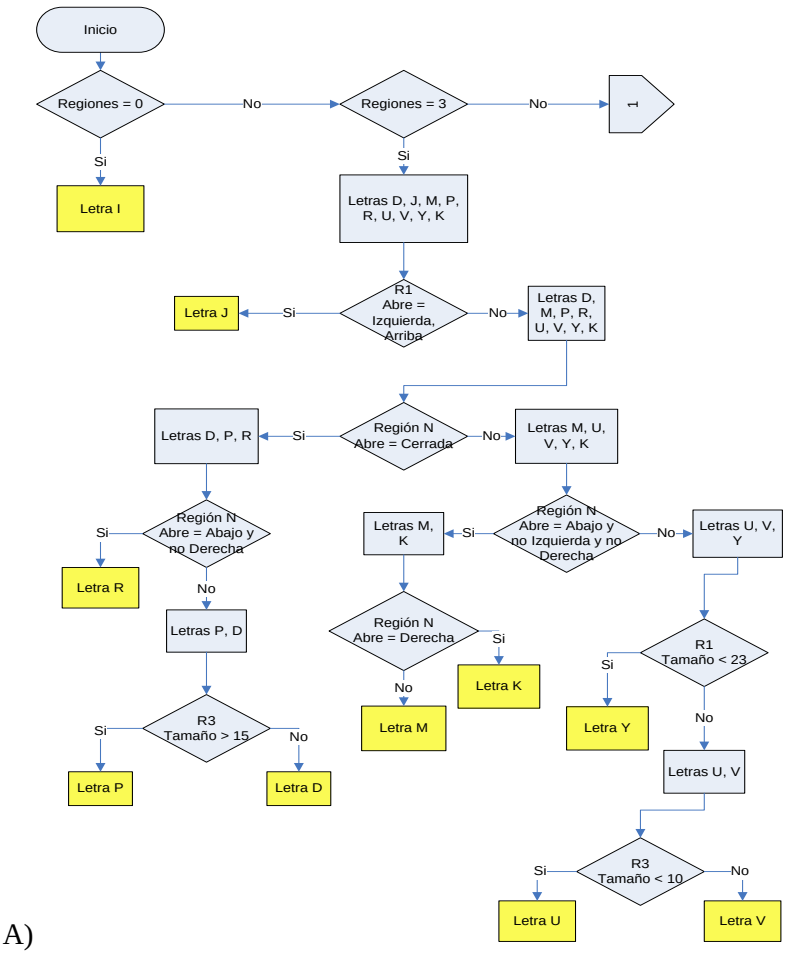
- Apertura del área: cada una de las áreas tiene máximos y mínimos en las coordenadas “x” y “y”; si una de estas coordenadas máximas es igual a una de las coordenadas máximas de la letra, o si alguna de las mínimas es igual a las mínimas de la letra, entonces el área es abierta, de lo contrario, el área es cerrada.

3.4.5 Árbol de decisión para la identificación

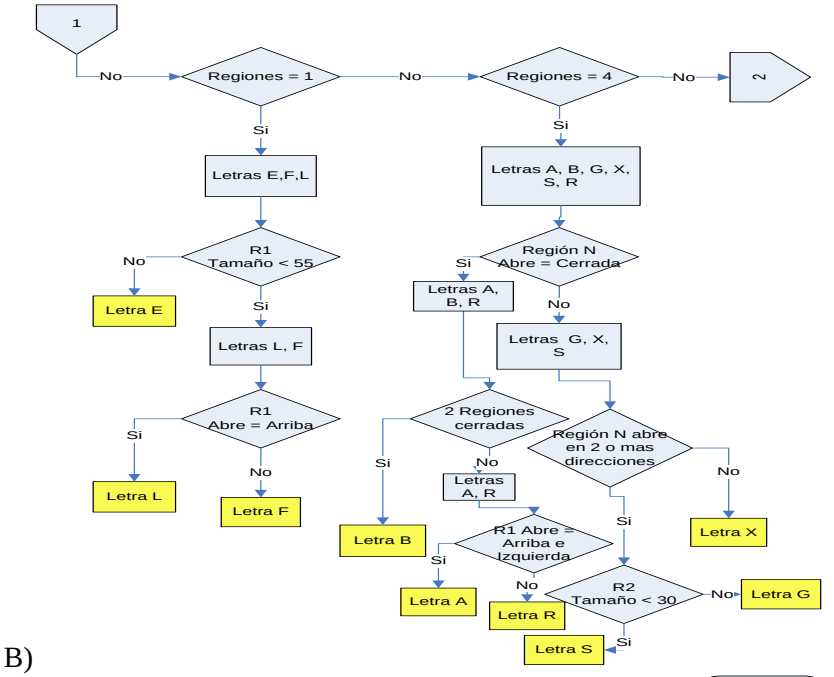
Para la clasificación de cada una de las letras, se creó un árbol de decisión que nos facilita y nos ahorra tiempo de cómputo en el proceso de identificación de las letras. Este árbol ha dado muy buenos resultados usándolo en las letras del nombre que se encuentra en el anverso de la Credencial para Votar con fotografía, ya que tiene flexibilidad con al tamaño de la letra y usa rasgos característicos de las letras que se usan en los tipos de fuente usados en las credenciales, por lo que también tiene flexibilidad en la clasificación de las letras de los tipos de fuente usados para las credenciales.

Entre las debilidades detectadas, se observa poca flexibilidad si la letra es rotada, pero en el caso del presente trabajo esto no representa problemas graves, ya que las letras no están rotadas en la imagen. El árbol de decisión, además, puede no funcionar con otros tipos de fuente, ya que, como ejemplo, el caso de la A en fuente tipo Arial-Cursiva, presenta por lo menos, un cambio en el rasgo del número de regiones, es decir, la A en ese caso tiene una región menos que la A Arial.

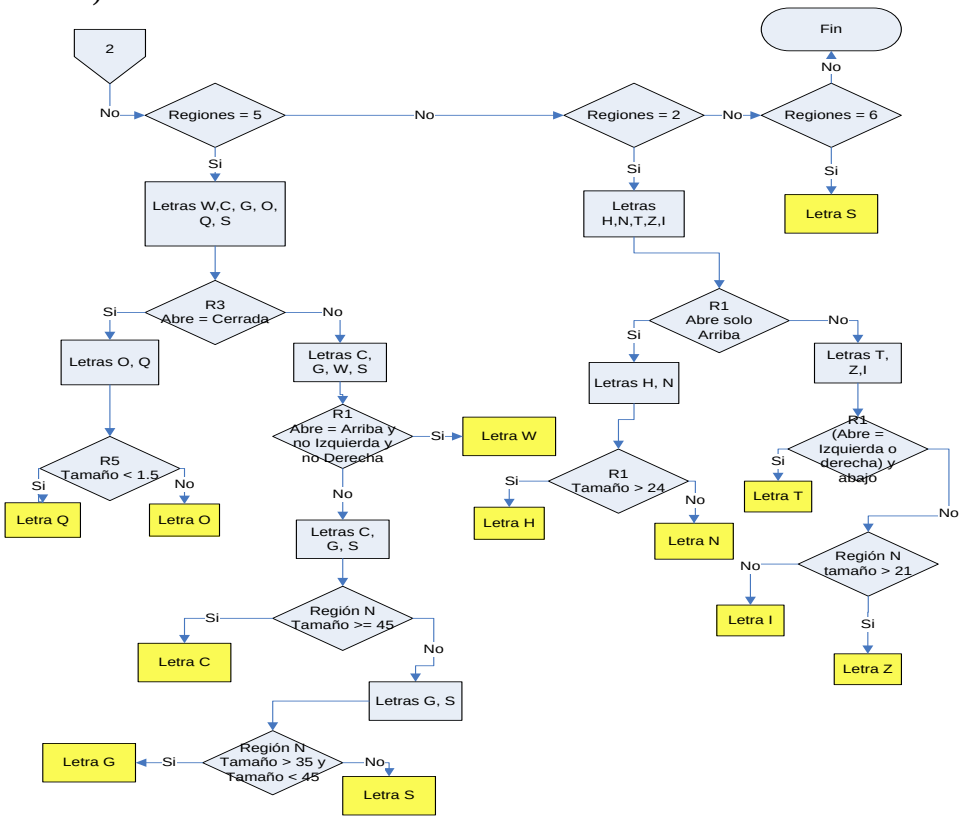
Como comentario final acerca del árbol presentado, éste no está concebido para reconocer las letras minúsculas de ningún tipo de fuente. Las decisiones de este árbol son tomadas por medio de sentencias if - then - else. El diagrama de éste árbol se muestra en la figura 39.



A)



B)



C)

Figura 39 Árbol de desición para el algoritmo OCR para las letras: A) I, D, J, M, P, R, U, V, Y, K; B) E, F, L, A, B, G, X, S, R; C) S, W, C, G, O, Q, H, N, T, Z, I con base y tope, es decir, de fuente Times New Roman

3.4.6 Recorte del microtexto alrededor de la fotografía y alrededor del área destinada para la firma y verificación del mismo

Una vez obtenidos los valores que deben ser analizados en el microtexto, debemos entonces, recortar el microtexto del anverso y con esto iniciar su análisis.

Para empezar, convertimos la fotografía a niveles de gris usando solo el promedio de los canales rojo y verde, ya que en el canal azul, la trama crea ruido en el microtexto. Una vez hecho esto, umbralamos la fotografía para buscar el inicio del microtexto en cada uno de los 4 lados de la Credencial. Para esto, ante todo buscamos una línea recta de por lo menos 35 y a lo más 70 pixeles de un total de 100 pixeles verificados que estén en blanco, primero para ver que exista el microtexto y segundo para cerciorarnos que no sea una línea recta.

Si este inicio es encontrado, entonces podemos verificar el resto de la línea. Empezamos a verificarla determinando que a lo más deben de ser 95% de los pixeles, para cerciorarnos de que no sea una línea recta en vez de un microtexto.

Teniendo esto, podemos comprobar entonces que si la credencial es de años anteriores al 2001 y por lo tanto no contiene un microtexto, entonces puede considerarse legítima; igualmente si la Credencial es de años posteriores al 2001 y es detectado un microtexto, entonces se continúa con el proceso de validación y se recorta el microtexto. Cualquier otro caso se considera como microtexto apócrifo.

Este sistema guarda en memoria los datos encontrados en los pasos mencionados anteriormente, por lo que se pueden cerrar todas las ventanas abiertas y cargar la imagen del reverso de la Credencial para hacer el análisis correspondiente. Para obtener el área destinada para la firma, a la imagen del reverso de la credencial se le aplica un algoritmo similar al usado para el recorte de la fotografía en el anverso. Una vez obtenida el área destinada para la firma, se aplica el algoritmo descrito en el apartado anterior para recortar y obtener el microtexto. El siguiente apartado, nos muestra el algoritmo desarrollado para la verificación de ambos microtextos.

Una vez recortado el microtexto, éste se analiza línea por línea, es decir, primero el de arriba, luego el vertical de la derecha, después el de abajo y por último el vertical de la izquierda de la fotografía. A cada una se le aplica el algoritmo de contraste por sombrero de copa morfológico descrito en el capítulo 2 de la presente tesis. Una vez aplicado este algoritmo, cada una de las líneas del microtexto es umbralada.

Una vez umbralada cada una de las líneas, se le aplica un algoritmo de correlación morfológico, consistente en usar la apertura generalizada con imágenes de cada una de las letras como elemento de estructura. Recordemos que en la apertura generalizada se usan dos elementos de estructura por letra: un elemento de estructura que marca los aciertos y uno que marca los fallos, es decir, uno nos limita el tamaño mínimo de la letra al erosionar el área de interés, mientras que el otro nos limita la letra a un tamaño máximo al erosionar el fondo. La figura 40 nos muestra el ejemplo del elemento de estructura *Miss* (o falla) para la letra A y en la figura 41 se observa el ejemplo del elemento de estructura *Hit* (o acierto) para la letra A.

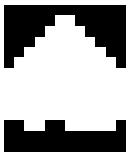


Figura 40 Elemento de estructura Miss para la letra A

Figura 41 Elemento de estructura Hit para la letra A

Estos elementos de estructura se obtuvieron después de experimentar tratando de encontrar los que nos minimicen al máximo los errores al no encontrar algunas letras, y al mismo tiempo, los que no nos encuentren más letras de las que debe haber.

A pesar de los cuidados tomados, el microtexto es muy ruidoso y tiene demasiados errores al momento de ser creada la credencial. Es por ello que tuvimos que dejar de tomar en cuenta cuatro letras. Las letras no verificadas son las siguientes: D, F, P y la B que son las más ruidosas y se confunden la F con la P, la B se confunde en algunos casos con la E, pero no siempre, por lo que no se dejó de tomar en cuenta la E pero sí la B; de igual manera sucede entre la O y la D, por lo que la O no se dejó de tomar en cuenta. Un ejemplo de esto se observa en la figura 42.

Figura 42 Ejemplo en el cual se confunden la P y la F, en este caso se debería leer FELIPE

Como se puede ver en la figura anterior, no fue posible hacer un elemento de estructura que diferenciara bien la F de la P.

Después de las experimentaciones con estos elementos de estructura, se vio la necesidad de crear un juego alterno de elementos de estructura para las credenciales del año anterior al 2004 y posterior al 2001. Este nuevo juego de elementos de estructura, tomó en cuenta la letra P y la F, además de la D, dejando fuera nuevamente a la letra B, ya que la P en el caso de estas credenciales es posible diferenciarla de la F, lo mismo la D de la O, pero la B siguió siendo muy ruidosa.

El resultado de este algoritmo son imágenes con las posiciones de las letras en la línea, como se muestra en la figura 43, en la cual se muestra el resultado de aplicar el algoritmo con las máscaras de la letra C en la línea superior del microtexto.

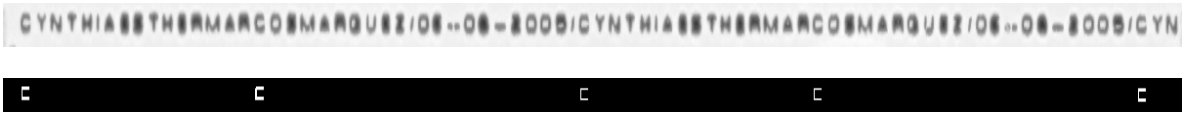


Figura 43 Resultado del algoritmo de correlación para la letra C

3.4.7 Análisis de la posición detectada

Una vez obtenidos los resultados anteriormente descritos, por medio de un algoritmo de etiquetado de componentes conexas, tomando en cuenta además que algunas veces las letras del microtexto se cortan, es decir, aparecen como dos regiones diferentes, se crea una lista, la cual es modificada de tal forma que si una región es muy angosta (comparada con el tamaño que debe tener una letra completa; para esto usamos la información obtenida del texto del nombre en el anverso para ver qué letra debe ser la que se presenta en cada posición), se une a la región contigua a la derecha. De igual manera, si la región es demasiado ancha para la letra que debe estar en esa posición, la región es partida en 2. Así obtenemos las posiciones de cada una de las letras.

Obtenidas las posiciones de las letras, se procede a realizar una comparación de las imágenes obtenidas a partir del algoritmo y la lista de posiciones para ver cuántas letras fueron detectadas positivamente (posición correcta) y cuántas no fueron detectadas; las que fueron detectadas en una posición errónea (fueron confundidas con otra letra), no son contadas. El algoritmo como parte de su salida, entrega una imagen en la cual fueron unidos los resultados por medio de la función XOR, para que los usuarios se pudieran dar una idea correcta del resultado obtenido. Un ejemplo de esto se muestra en la figura 44.

Figura 44 Reconstrucción del microtexto

Finalmente, se calcula el porcentaje de reconocimiento dividiendo el número de letras correctamente reconocidas entre el número total de letras que tiene el nombre. Teniendo esto, se dice que una credencial es legítima si dos de sus cuatro lados pasan el 50%, de dudosa legitimidad no hay dos lados que pasen el 50%, pero hay dos lados que pasan el 20% y apócrifa en cualquier otro caso.

CAPÍTULO IV. PRUEBAS Y RESULTADOS

En el presente capítulo se detallan las pruebas que se realizaron, los resultados obtenidos de ellas y la evaluación del sistema completo y así determinar si es eficiente o no para la tarea propuesta.

4.1 Pruebas

Para realizar los experimentos que prueban la validez de nuestra propuesta, se utilizó una base de datos de imágenes con 46 credenciales legítimas para votar con fotografía escaneadas a 1200 pixeles por pulgada, y comprobado los microtextos con el texto del nombre. De estas 46 credenciales hay 14 anteriores al 2001, 28 credenciales posteriores al 2001 y 4 credenciales del 2009.

La siguiente credencial está en el subdirectorio 030759888763 del directorio de credenciales. El resultado obtenido es que en el anverso no hay microtexto y en el reverso fue detectada una línea recta, pero como la credencial es anterior al 2001, la credencial es válida, al menos respecto de este candado.

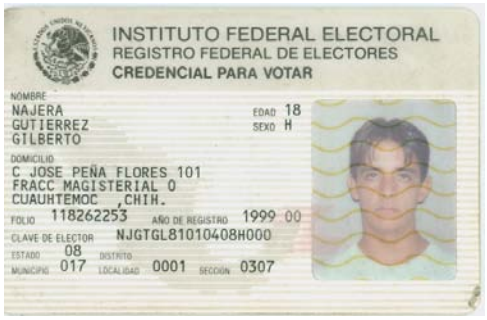


Figura 45 Credencial original

Figura 46 Texto del nombre en el anverso

Figura 47 Fotografía recortada y microtexto no encontrado

Figura 48 Área destinada para la firma en donde se observa una línea completa

La siguiente credencial se encuentra en el subdirectorio 0959049417174 del directorio de credenciales.

Figura 49 Credencial original

Figura 50 Recorte del nombre

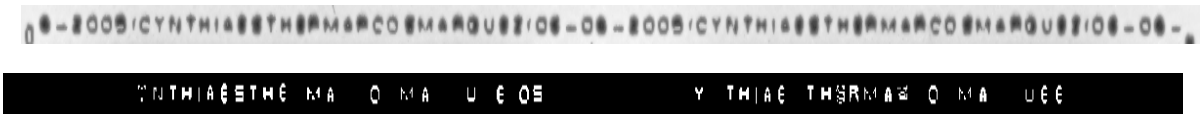
A partir del recorte obtenido en la figura 50, se pudo saber el nombre del titular de la credencial.

Figura 51 Foto recortada del anverso

La foto fue recortada para poder hacer el reconocimiento del microtexto. En la siguiente figura se muestran los resultados obtenidos como ya se explicó anteriormente.

Arriba

Abajo



Izquierda

Derecha

Figura 52 Resultado de la validación del microtexto

En la figura 52, con fondo negro, se muestra el resultado de la reconstrucción de cada lado del microtexto; encima de cada reconstrucción, se observa la respectiva imagen original. Se puede observar en estas imágenes, que en la parte de arriba se obtuvo un 83% de aciertos; en el texto de abajo se encontró el 67%; en el del lado izquierdo se obtuvo el 56% y en el del lado derecho se

obtuvo el 66%. Tomando en cuenta que en el caso de la reconstrucción se hizo una operación de XOR, se puede decir que están mal las que se ven borrosas, ya que fueron confundidas con más de una letra; por lo tanto, como por lo menos dos de los cuatro lados supera el 50% de letras reconocidas, decimos que el microtexto es correcto.

La siguiente credencial está en el subdirectorio 175487808843 del directorio de credenciales; el resultado obtenido es que en el anverso no hay microtexto y en el reverso fue detectada una línea recta, pero como la credencial es anterior al 2001, la credencial es válida, al menos respecto de este candado.

Figura 53 Credencial original

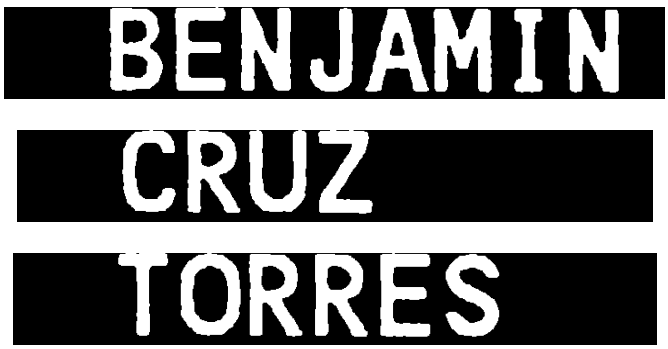


Figura 54 Texto del nombre en el anverso

Figura 55 Fotografía recortada y microtexto no encontrado

Figura 56 Área destinada para la firma en donde se observa una línea completa

La siguiente credencial se encuentra en el subdirectorio 0665048370090 del directorio de credenciales.

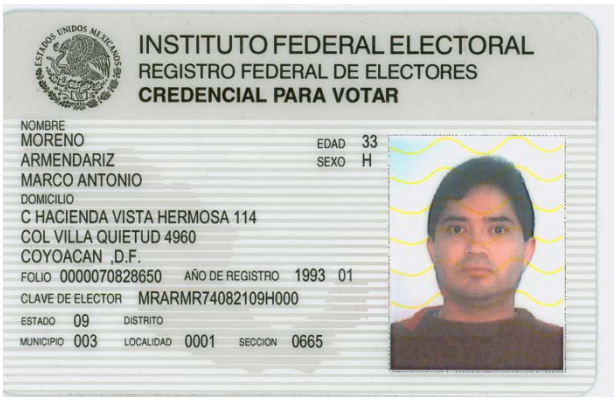


Figura 57 Credencial original

Figura 58 Recorte del nombre

A partir del recorte mostrado en la figura 58, se pudo saber el nombre del titular de la credencial.

Figura 59 Foto recortada

La foto fue recortada para poder hacer el reconocimiento del microtexto. En la siguiente figura se muestran los resultados obtenidos como ya se explicó anteriormente.

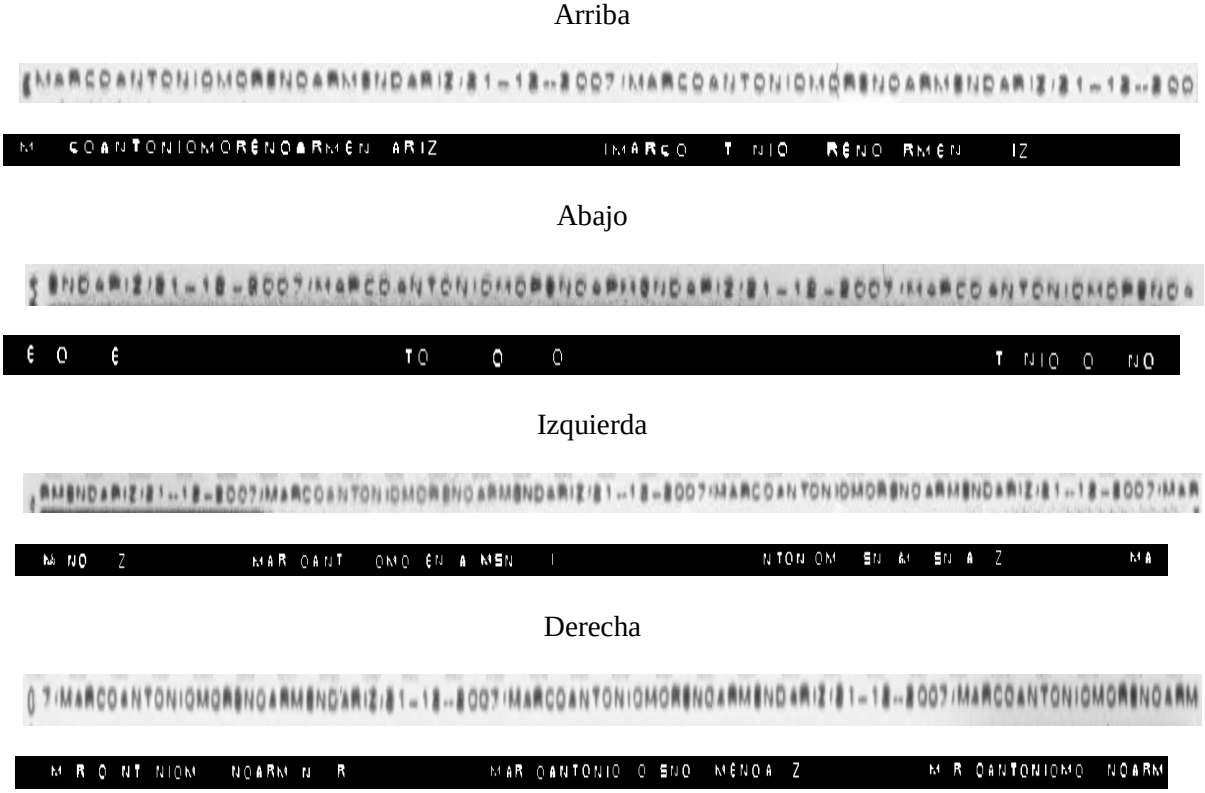


Figura 60 Resultado de la validación del microtexto

En la figura 60 se muestra el resultado de la reconstrucción de cada lado del microtexto, y arriba de cada reconstrucción, se observa la respectiva imagen original. Se puede observar en estas imágenes que en la parte de arriba se obtuvo un 88% de aciertos; en el microtexto de la parte de abajo, se encontró el 34%; en el del lado izquierdo se obtuvo el 52% y en el derecho el 73%. Tomando en

cuenta que en el caso de la reconstrucción se hizo una operación de XOR se puede decir que están mal las letras que se ven borrosas, ya que fueron confundidas con más de una letra; por lo tanto, como por lo menos dos de los cuatro lados supera el 50% de letras reconocidas, decimos que el microtexto es correcto, todo esto tomando en cuenta que la letra D en este caso fue omitida por lo explicado antes.

La siguiente credencial se encuentra en el subdirectorio 0665048370090 del directorio de credenciales.

Figura 61 Credencial original

Figura 62 Recorte del nombre

A partir del recorte obtenido en la figura 62, se pudo saber el nombre del titular de la credencial.

Figura 63 Foto recortada

La foto fue recortada para poder hacer el reconocimiento del microtexto. En la siguiente figura se muestran los resultados obtenidos como ya se explicó anteriormente.

Arriba

Abajo

Izquierda

Derecha

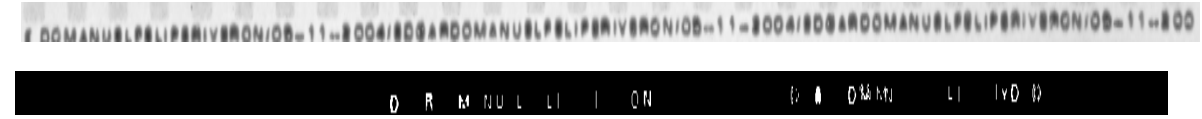


Figura 64 Resultado de la validación del microtexto

En la figura 64 se muestra el resultado de la reconstrucción de cada lado del microtexto, y arriba de cada reconstrucción, se observa la respectiva imagen original. Se puede observar en estas imágenes que en la parte de arriba se obtuvo un 86% de aciertos; en el microtexto de la parte de abajo, se encontró el 39%; en el del lado izquierdo se obtuvo el 50% y en el derecho el 34%. Tomando en cuenta que en el caso de la reconstrucción se hizo una operación de XOR se puede decir que están mal las letras que se ven borrosas, ya que fueron confundidas con más de una letra; por lo tanto, como por lo menos dos de los cuatro lados supera el 50% de letras reconocidas, decimos que el microtexto es correcto, todo esto tomando en cuenta que las letras D, F y P en este caso fueron omitidas por lo ya explicado.

A continuación, se presenta el resultado de una de las credenciales apócrifas creadas por nosotros, en este caso el microtexto fue modificado para probar el sistema:

Figura 65 Credencial Apócrifa

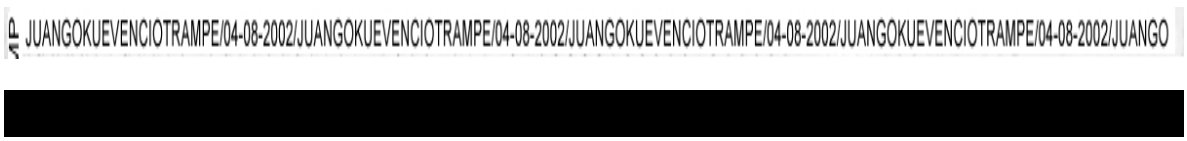
Figura 66 Recorte del nombre

A partir del recorte obtenido en la figura 66, se pudo saber el nombre del titular de la credencial.

Figura 67 Fotografía recortada

La foto fue recortada para poder hacer el reconocimiento del microtexto. En la siguiente figura se muestran los resultados obtenidos como ya se explicó anteriormente.

Arriba



Abajo

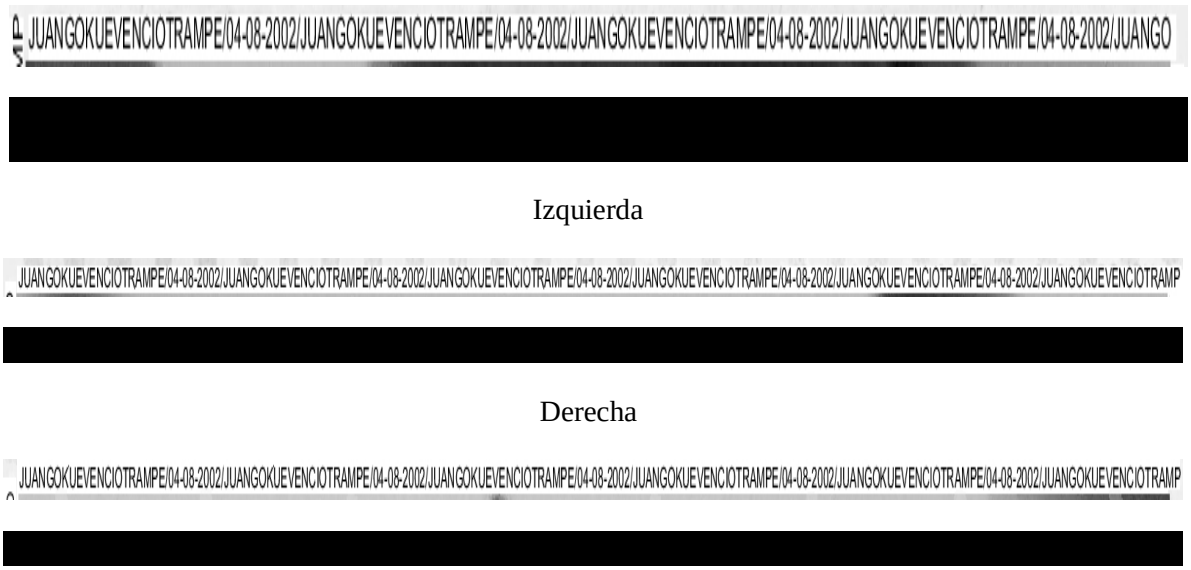


Figura 68 Resultado de la validación del microtexto

Como podemos observar, el hecho de que el microtexto tenga tantos defectos, fue un arma de dos filos, ya que no solo impide que el microtexto sea reconocido perfectamente, sino que impide que sean reconocidas letras mejor trazadas.

4.2 Resultados

Los resultados obtenidos usando el algoritmo de reconocimiento de caracteres para obtener el nombre del titular para las 46 credenciales fueron los siguientes:

El tiempo de análisis de cada letra puede variar de 0.029 a 0.066 segundos dependiendo de la profundidad que tiene la letra en el árbol de decisión; el promedio por cada letra fue de 0.04751 segundos.

El tamaño en pixeles para la letra más pequeña (I) es de 9 pixeles de ancho por 82 pixeles de alto, mientras que para la más grande (Q) es de 63 pixeles de ancho por 90 pixeles de alto, dando tamaños de área desde 738 pixeles hasta 5670 pixeles.

Por medio de la experimentación descrita anteriormente, se tomó una muestra de once credenciales para ver el porcentaje de reconocimiento de letras en el microtexto que se está generando con los elementos de estructura. De aquí se obtuvieron los resultados que se muestran en la tabla 1.

Tabla 1 Porcentaje de reconocimiento de las letras en el microtexto y promedio

	Porcentaje			
	Arriba	Izquierda	Derecha	Abajo
1	69.09	59.42	65.22	50.00
2	42.59	42.42	56.00	22.64
3	85.45	74.60	67.16	72.34
4	89.09	65.33	76.00	59.62
5	73.47	63.49	47.54	46.81
6	7.69	4.69	6.25	5.77
7	80.00	78.79	82.35	58.49
8	28.07	40.00	40.58	60.00
9	66.67	54.55	59.32	37.21
10	81.48	44.44	42.25	35.85
11	69.81	57.81	64.06	62.26
Promedio	63.04	53.23	55.16	46.45

Con los datos presentados en la tabla anterior, se obtuvo un promedio general de 54.47% de letras reconocidas. Tomando esto en cuenta y para darle flexibilidad al algoritmo, se llegó a la conclusión de que con el 50% de las letras analizadas dadas como válidas, es suficiente para poder dar como válido el microtexto en cada uno de los cuatro lados de la fotografía y del área para la firma. Además, observando el hecho de que el microtexto está mal impreso y que en ocasiones, sobre todo en los lados izquierdo y derecho, el microtexto presenta ondulaciones e inclinaciones que evitan que se pueda analizar adecuadamente, se estableció que para que el microtexto sea válido en el anverso o reverso, debe ser válido en por lo menos dos de los cuatro lados del microtexto. Este algoritmo es robusto al hecho de que por la apertura generalizada no deja pasar cuadros ni líneas continuas por lo que hay menos posibilidades de falla y detectar mal las letras.

Así mismo, tomando en cuenta los valores más bajos obtenidos en esta muestra, se observó que es inaceptable un valor menor que el 20% para los microtextos, por lo que se creó un segundo umbral para que el usuario tenga la oportunidad de verificar manualmente si el microtexto es válido. Este umbral es el umbral que nos indica que el microtexto es de dudosa legitimidad para el sistema; sus valores son menores que el 50% y mayores que el 20% en por lo menos dos de los cuatro lados. Con cualquier otro caso, para el sistema el microtexto es falso y la credencial apócrifa.

Usando estos parámetros, se obtuvieron los resultados mostrados en la tabla 2.

Tabla 2 Resultados de las credenciales analizadas

Año	Credenciales Analizadas	Apócrifas	Legítimas o dudosas
<2001	14	0	14
>=2001	32	1	31
Apócrifas	3	3	0

Por lo que 48 de las 49 credenciales fueron correctamente clasificadas, es decir, un 97% de clasificación.

CAPÍTULO V. CONCLUSIONES Y TRABAJO FUTURO

5.1 Conclusiones

- Este trabajo presenta una metodología que nos permite analizar el microtexto mediante la digitalización en alta resolución y el manejo de técnicas del análisis de imágenes y de la morfología matemática.

- El sistema logró reconocer de manera eficiente las credenciales apócrifas, dando como resultado 4 credenciales apócrifas, de las cuales 3 eran efectivamente apócrifas creadas exclusivamente para la experimentación.

- Este trabajo, presenta una metodología que nos permite analizar el microtexto mediante la digitalización en alta resolución y el manejo de tecnologías como el análisis de imágenes y la morfología matemática.

- Se presenta como una de las principales aportaciones un algoritmo por medio del cual se reconoce y se extrae exitosamente la información necesaria para la validación del microtexto (nombre del titular). Este algoritmo está presentado en los epígrafes 3.4.1 al 3.4.5, comenzando así con la digitalización de la credencial a alta resolución, y terminando en el uso del árbol de decisión para el reconocimiento del texto del nombre.

- Dentro de ésta metodología, se presenta una manera de extraer los microtextos mediante la ubicación de la posición de los mismos usando un algoritmo detector de bordes, además de estadísticas que nos permiten determinar en qué grado puede ser un microtexto y en qué grado es solo una línea recta o ruido en la imagen.

- Un resultado importante es el análisis del microtexto, logrado por medio del algoritmo de apertura generalizada con las letras del nombre como elementos de estructura.

- Es importante hacer notar que la metodología presentada en este trabajo puede ser usada para validar no solo el microtexto de la Credencial para Votar con fotografía, sino puede extenderse al análisis del microtexto presente en otros medios de identificación que lo usan, como es el caso del papel fiduciario (billetes de banco). Todo esto fue abordado en el informe técnico referido en [15].

- Hay que hacer notar además que en el presente trabajo se experimentó con una credencial que fue digitalizada con otro tipo de escáner, incluso de otra marca, presentando el algoritmo un comportamiento satisfactorio, por lo cual podemos concluir que las credenciales pueden ser digitalizadas con cualquier escáner que pueda digitalizar con resoluciones superiores a los 1200 ppp y usar el algoritmo propuesto para analizarla con resultados satisfactorios.

- Una conclusión importante, es que los defectos del microtexto funcionan como un arma de dos filos, ya que además de impedir su reconocimiento total, impiden también su falsificación con métodos de manipulación de imágenes.

5.2 Errores y limitaciones del sistema

El sistema tuvo errores principalmente con imágenes que al ser escaneadas resultaron con muy poco contraste o que estaba muy dañada cuando fue digitalizada.

El sistema tuvo ciertos errores durante el reconocimiento OCR creado para poder obtener el nombre del titular, ya que en ocasiones las letras L y A, así como la R y la A y las letras K y A, se juntaban creando una sola región, lo que provocaba un fallo en el etiquetado de componentes conexas.

Esto fue corregido completamente al dividir entre dos el ancho de la región de estas letras unidas después de que el algoritmo de etiquetado las detectara como una sola región.

Al comenzar con la experimentación, en el sistema se usaba primeramente un algoritmo de correlación basado en la apertura simple; sin embargo, la experimentación era muy mala, ya que no prevenía problemas tales como la detección de letras en cuadros que fueran puestos en lugar de las letras del microtexto; esto nos traía muchos errores. Finalmente se decidió que la mejor forma de atacarlo era con la apertura generalizada, la cual nos brindó resultados satisfactorios.

Las principales limitaciones del sistema están dadas por la resolución requerida del escáner y el método de digitalización usados para obtener las imágenes de la credencial.

Estas limitaciones pueden ser evitadas con el solo hecho de usar un escáner similar al usado en el desarrollo de la presente tesis (de 1200 ppp) y mediante el método ya descrito.

Otra de las limitaciones del sistema fue el tiempo que toma el procesamiento completo de la credencial, debido al escaneo de alta resolución.

Algo muy importante que debe mencionarse como limitación del presente trabajo, es que el sistema no tiene flexibilidad en cuanto al análisis del microtexto en una credencial rotada un pequeño ángulo, además de que en ocasiones el microtexto no está dispuesto en línea recta en algunas de las credenciales, sino que se presenta una cierta ondulación en la posición de las letras; esto hace difícil su reconocimiento y llega a afectar los resultados obtenidos por el sistema. Es por esto que para darle una mejor flexibilidad, fue ideada la clase de dudosa legitimidad para indicar al usuario que el sistema no tiene certeza de si la credencial es legítima o apócrifa, dando la posibilidad de que el usuario pueda revisar manualmente la credencial.

5.3 Recomendaciones

A pesar de la búsqueda y la investigación que se hizo para el presente trabajo, no se pudo hallar nada sobre la manera en que son impresas las letras del microtexto en las credenciales. Al analizar este candado de seguridad se llegó a la conclusión de que tiene ciertos defectos de impresión debido a que los caracteres son impresos con poco puntaje y en tamaño real, los que difícilmente pueden ser corregidos por parte de la empresa encargada de la impresión (tomando en cuenta que el IFE no es el encargado de hacer las credenciales ni sus candados, si no que contratan a una empresa "especialista" en ese campo).

Los principales problemas encontrados en este sistema se detallan a continuación:

- El problema más característico del microtexto impreso es que el tipo de letra varía en las diferentes versiones de la credencial (figura 69), lo que puede ser debido a que cada vez que el modelo va a ser modificado de alguna forma, el IFE hace una licitación entre diversas empresas de seguridad para ver cuál de ellas ofrece más ventajas para los nuevos candados de seguridad. Una recomendación para evitar esto en la mayor medida posible, es que el IFE se quede con los "moldes" usados para la impresión de los microtextos cada vez que vaya a realizar cambios en el modelo de la credencial; los principales saltos en este aspecto son en los años 2001 (que es cuando se empezó a implementar este candado), 2004 y 2008.

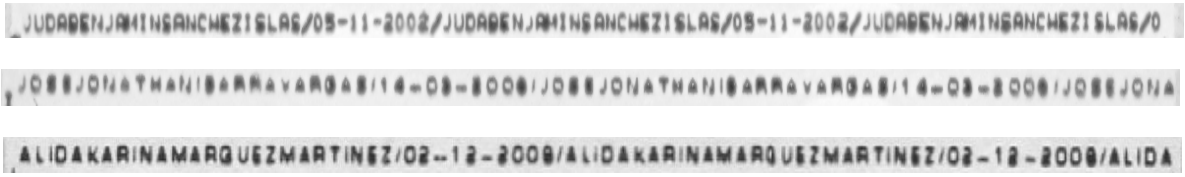


Figura 69 De arriba hacia abajo se presentan los microtextos de las credenciales de los años 2002, >2004 y 2008 respectivamente

- Otro problema también muy característico que se presentó durante el análisis del microtexto, es que al hacer la impresión de los caracteres del microtexto, no se tuvo el suficiente cuidado con la tinta y ésta presenta manchones en los caracteres, impidiendo de esta manera el correcto reconocimiento de las letras. Un ejemplo de este comportamiento se puede observar en la figura 70. Esta es una de las razones por las cual la letra B no fue tomada en cuenta para el reconocimiento. En este caso la recomendación es que se tenga más cuidado con la impresión y se consiga además un método de impresión más eficiente.

a) b)

Figura 70 Recorte de las letras E (a) y B (b) a partir del ejemplo mostrado de la credencial mayopr al 2004 en la figura 69

- El problema más grave y que no pudo ser arreglado en el presente trabajo, es que el microtexto presenta ciertas irregularidades en su alineación, ya que este debería ser presentado siempre con los caracteres dispuestos en una línea recta; sin embargo en ocasiones el microtexto se presenta con una irregularidad ondulada en cuanto a la posición de los caracteres (figura 71), lo cual hace que las letras lleguen a quedar fuera del área analizada lo cual se traduce en una disminución de la calidad del reconocimiento.

Figura 71 Ejemplo de microtexto con un problema grave de forma, se aprecia que la posición de los caracteres no es en línea recta, si no que es ondulado

Éstos son los problemas más graves detectados durante la realización del presente trabajo, pero cada uno de ellos podría ser resuelto si se adoptara una mejor forma de impresión de los microtextos. Esto no sucede con la moneda fiduciaria, toda vez que los microtextos son impresos con el tamaño adecuado en una credencial de gran tamaño, los que después ambos son reducidos por medios ópticos a su tamaño real. En este caso, la tecnología a utilizar para la creación de las credenciales de elector tendría que ser muy diferente a la actual.

5.4 Trabajo futuro

Como trabajo futuro podríamos mencionar los siguientes:

- Extender la metodología presentada en esta tesis para el análisis de los microtextos presentes en cualquier identificación o en los billetes de banco que usen los microtextos como candado de seguridad, ya que la presente metodología trabaja bajo las premisas: ¿Qué debe decir el microtexto?, y ¿En donde se encuentra ubicado?, además de los elementos de estructura que nos indiquen la forma de las letras del microtexto.

- Mejorar el diseño de los elementos de estructura de cada una de las letras del alfabeto para poder reconocerlas en el microtexto con una mayor precisión.

- Crear un algoritmo que permita “enderezar” los microtextos en los casos que sea necesario para así poder corregir los posibles problemas de la forma en que está acomodado el microtexto, que se alejen de la forma rectilínea.

- Crear un algoritmo que permita crear automáticamente los elementos de estructura idóneos para cada uno de los caracteres de los microtextos usados en cada tipo de identificación en particular, es decir, los elementos para las credenciales IFE, para los pasaportes, etc.

- Analizar los demás candados de seguridad presentes en la credencial y proponer una metodología general que permita clasificar las credenciales en apócrifas o legítimas sobre la base de los resultados obtenidos en la presente tesis junto con el análisis de los demás candados de seguridad.

5.5 Publicaciones realizadas

Durante el desarrollo de este trabajo se han hecho las siguientes publicaciones:

5.5.1 Reportes técnicos

Fueron realizados los siguientes reportes técnicos como justificación a la presente investigación:

- "La importancia del microtexto como candado de seguridad"
  José de Jesús Deloya Cruz, Samuel Sanchez Islas, Edgardo Manuel Felipe Riverón, CIC-IPN, 19 páginas, ISBN: 978-970-36-0484-5

- "Características y Candados de Seguridad en las Credenciales para Votar con Fotografía"
  Samuel Sanchez Islas, José de Jesús Deloya Cruz, Edgardo Manuel Felipe Riverón, CIC-IPN, 22 páginas, ISBN: 978-970-36-0485-2

5.5.2 Ponencias en congresos

Durante la realización de este trabajo, se presentó la ponencia siguiente:

An optimized character recognition algorithm based on convex hull feature extraction, José de Jesús Deloya Cruz, Edgardo Manuel Felipe Riverón y Salvador Godoy Calderón. XVII Congreso Internacional de Computación CIC – 2008, 3 al 5 de diciembre de 2008.

Referencias

1. *Características y Candados de Seguridad de las Crendenciales para Votar con Fotografía*. **Sánchez Samuel, Deloya Jesús, Felipe Edgardo.** México, D.F. : IPN, 2008.

2. ***Lancaster, Ian M.*** *El papel de las tecnologías de autenticación en la lucha contra la falsificación*. OMPI, Revista de la. [En línea] abril de 2006. Disponible en World Wide Web: <http://www.wipo.int/wipo_magazine/es/2006/02/article_0004.html>.

3. **AssureTec.** *Autentifica cualquier identificación automáticamente*. [En línea] mayo de 2009. Disponible en World Wide Web: <http://www.assuretec.com/index.php/products/demo/>.

4. **Telvent.** *Verificación de Documentos.* [En línea] enero de 2006. [Citado mayo de 2009]. Disponible en World Wide Web: <http://www.telvent.com/downloads/areasnegocio/administraciones/verificacion.pdf>.

5. **Elba Securidoc.** *Nuevos productos para la autentificación de documentos de Securidoc. Accesogroup.* En accesogroup. [En línea] 2002. Disponible en World Wide Web: <http://www.acceso.com/display_release.html?id=6638. *accesso.com*>.

6. **SAS R&D Systems.** *Forgery Detection System.* [En línea] 2004. [Citado mayo de 2009]. Disponible en World Wide Web: <http://www.sasrad.com/spanish/products/forgery.htm>.

7. **Graphic Security Systems Corporation.** *IDetector Mobile.* [En línea] noviembre 2008. [Citado mayo de 2009]. Disponible en World Wide Web: <http://www.graphicsecurity.com/pdfs/iDetector_Mobile_Brochure.pdf>.

8. **Wikipedia.** *Análisis de Imágenes.* Wikipedia La enciclopedia libre. [En línea] mayo 2009. [citado mayo 2009]. Disponible en World Wide Web: <http://es.wikipedia.org/wiki/An%C3%A1lisis_de_im%C3%A1genes>.

9. **Gómez Pérez, José Ramón.** *La Digitalización.* [En línea] 2005. [Citado mayo 2009]. Disponible en World Wide Web. < http://boj.pntic.mec.es/jgomez46/documentos/cav/digitalizacion.pdf>.

10. **Luciano, Moreno.** *Descripción de los tipos de color conocidos.* Desarrolloweb. [En línea] mayo 2004. [Citado mayo 2009]. Disponible en World Wide Web: <http://www.desarrolloweb.com/articulos/1483.php>.

11. **Humberto, Sossa Azuela Juan.** *Rasgos Descriptores para el Reconocimiento de Objetos.* México, D.F. : s.n., 2006.

12. **Ortiz Zamora, Francisco Gabriel.** *Procesamiento morfológico de imágenes en color. Aplicación a la reconstrucción geodésica.* Alicante : Biblioteca Virtual Miguel de Cervantes, 2002.

13. *Generalized Hit-Miss Operators with Applications to Document Image Analysis.* **Bloomberg, Dan.** 1990.

14. **Soille, Pierre.** *Morphological Image Analysis Principles and Aplications.* s.l. : Springer.

15. **Deloya Cruz, José de Jesús, Sánchez Islas, Samuel y Felipe Riverón, Edgardo Manuel.** *La Importancia del Microtexto como Candado de Seguridad.* México D.F. : I.P.N., 2008. 978-970-36-0484-5.