

**APORTES Y APLICACIONES
EN LAS CIENCIAS
COMPUTACIONALES**

Gustavo Trinidad Rubín Linares

**APORTES Y
APLICACIONES EN LAS
CIENCIAS COMPUTACIONALES**

**APORTES Y
APLICACIONES EN LAS
CIENCIAS COMPUTACIONALES**

María del Carmen Santiago Díaz
Gustavo Trinidad Rubín Linares
María de Lourdes Sandoval Solís
Yeiny Romero Hernández
(Editores)

Gustavo Trinidad Rubín Linares
(Coordinador)

María del Carmen Santiago Díaz, Gustavo Trinidad Rubín Linares, María de Lourdes Sandoval Solís, Yeiny Romero Hernández
(editores)

Gustavo Trinidad Rubín Linares
(coordinador)

María del Carmen Santiago Díaz, Gustavo Trinidad Rubín Linares, Ana Claudia Zenteno Vázquez, Judith Pérez Marcial, Yeiny Romero Hernández, Nicolás Quiroz Hernández, Alma Delia Ambrosio Vázquez, Héctor David Ramírez Hernández, Gregorio Trinidad García, María de Lourdes Sandoval Solís, Rogelio González Velázquez, Guillermina Sánchez Román, José Luis Hernández Ameca, Armando Espindola Pozos, María Blanca del Carmen Bermúdez Juárez, José Martín Estrada Analco, Luz del Carmen Reyes Garcés, Meliza Contreras González, Luis Enrique Colmenares Guillén, Elsa Chavira Martínez, Pedro García Juárez, Nelva Betzabel Espinoza Hernández, Alberto Román Flores, Roberto Contreras Juárez, Graciano Cruz Almanza, Maya Carrillo Ruiz, Ernest Cortez, Bárbara Emma Sánchez Rinza, Beatriz Beltrán Martínez, José Ítalo Cortez, Hermes Moreno Álvarez.
(revisores)

Primera edición: 2019

ISBN: 978-607-7512-96-7

Montiel & Soriano Editores S.A. de C.V.

15 sur 1103-6 Col. Santiago Puebla, Pue.

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

Rector:

Dr. José Alfonso Esparza Ortiz

Secretario General:

Dr. José Jaime Vázquez López

Vicerrector de Investigación y Estudios de Posgrado

Dr. Ygnacio Martínez Laguna

Directora de la Facultad de Ciencias de la Computación

M.I. María del Consuelo Molina García

Contenido

Prefacio	7
Estudio y Análisis de Seguridad en un Sistema de Información Web <i>Luz María Hernández Cruz</i> <i>Diana Concepción Mex Álvarez</i> <i>Margarita Castillo Téllez</i> <i>Oscar Ezequiel De la Cruz Ek</i>	8
Análisis de Fraudes en Transacciones Bancarias Aplicando Minería de Datos <i>Victor Giovanni Morales Murillo</i> <i>María Josefa Somodevilla García</i> <i>Magali Fong Juárez</i> <i>Ivo Humberto Pineda Torres</i>	12
Determinación del Tamaño de una Mano en Imágenes Radiográficas Utilizando Landmarks. <i>Jamid Israel Saenz Girón</i> <i>Jonathan Gabriel Salazar Roldán</i> <i>Salvador Eugenio Ayala Raggi</i> <i>Aldrin Barreto Flores</i>	20
Detección de Desbalance Financiero Utilizando Modelos Ocultos de Márkov <i>María de Lourdes Sandoval Solís</i> <i>Marcela Rivera Martínez</i> <i>Luis René Marcial Castillo</i> <i>Gladys Linares Fleites</i>	28
Intercomunicador con Cámara y Conectividad WiFi <i>Joel Fernando Acevedo Ruíz</i> <i>Aldrin Barreto Flores</i> <i>Salvador Eugenio Ayala Raggi</i> <i>Verónica Edith Bautista López</i>	40
Solución al Problema de la Programación de Producción - Inventario Usando Código LINGO <i>Rogelio González Velázquez</i> <i>María Beatriz Bernabé Loranca</i> <i>Adriana Méndez Montero</i> <i>Abraham Sánchez López</i>	56
Sistema Multi Sensor para Medición, Procesamiento y Envío de Parámetros Ambientales en Tiempo Real <i>María del Carmen Santiago Díaz</i> <i>Gustavo Trinidad Rubín Linares</i> <i>Hermes Moreno Álvarez</i> <i>Antonio Eduardo Álvarez Nuñez</i>	63
Desarrollo de un Robot Interactivo Como Asistente en Terapias para Niños con Autismo. <i>José Luis Hernández Ameca</i> <i>Gregorio Trinidad García</i> <i>José Ítalo Cortez</i> <i>Juan Chávez Bravo</i>	68
Diseño de un Shield con Microcontrolador ARM-Cortex-M0	

**para la Implementación de Redes Automotrices (CAN-BUS),
para Apoyar el Proceso de Enseñanza-Aprendizaje.**

Saúl Luna Minor

Nicolás Quiroz Hernández

Juan Carlos Ramírez Morales75

Seguridad Mediante un Plan de Auditorías

Héctor Joab Ibarra Caballero

Ana Claudia Zenteno Vázquez

María del Carmen Santiago Díaz

Gustavo Trinidad Rubín Linares.....88

**Desarrollo de un Descriptor Invariante a la Rotación Basado en HOGs
para Detección de Puntos de Interés en Radiografías de Manos.**

Mauricio Longinos Garrido

Salvador Eugenio Ayala Raggi

Alba Maribel Sánchez Gálvez

José Luis Tonatiúh Banda Escobar.....94

Estudio de Algoritmos para la Detección de Rostros

Nayeli Pamela Perales Soto

Kenneth Mejía Pérez

Diana Margarita Córdova Esparza.....103

**Aprendizaje Supervisado para la Detección de Plagas y
Enfermedades en los Cultivos de Aguacate**

Marcos Emiliano López Pérez

Luis Fernando Columna Álvarez

Guadalupe Michelle Ojeda Pérez.....114

Bases Matemáticas y Curvas Elípticas en la Criptografía

Héctor David Ramírez Hernández

Roberto Contreras Juárez

Nelva Betzabel Espinoza Hernández

Eduardo Mendoza Sánchez.....123

Análisis de la Optimización de Prótesis Robótica

María del Carmen Santiago Díaz

Gustavo Trinidad Rubín Linares

Roberto Morales Aguilar

Ángel Peláez Ramírez.....130

Prefacio

El avance vertiginoso de la ciencia y la tecnología han generado un gran abanico de soluciones a diversos problemas, sin embargo, en nuestra sociedad nos encontramos inmersos en un sistema que ya no brinda el soporte para una población que ha crecido de forma tan acelerada. Por ello es imprescindible resolver problemas propios de una sociedad en constante crecimiento, a fin de generar mejores condiciones de vida a nuestra población. Aunque hay identificados a nivel nacional y local los problemas que requieren solución inmediata, casi en cualquier área se requiere realizar innovaciones tecnológicas, algunas muy sofisticadas y complejas y otras no tanto, pero finalmente innovaciones, es decir, aplicar ideas y conceptos para solucionar problemas utilizando las ciencias computacionales, que aunque en muchos casos no se requiere una solución que implique años de investigación, si se requiere que la solución esté plenamente enfocada a un problema en particular. Muchas de estas soluciones en general no están a la vista sin embargo, resolver problemas ambientales, de vialidad, de producción de alimenticios, etc., representan en sí aplicar la tecnología de forma innovadora ya que aunque en nuestro país tenemos un enorme retraso tecnológico, lo que no se quiere en universidades e institutos de investigación es tener este retraso en la aplicación de la tecnología que se genera, por ello se cuenta con diversos programas internacionales, nacionales y locales para apoyar la innovación tecnológica. En nuestra universidad como en muchas otras en México y en el mundo se cuentan con programas específicos de innovación tecnológica para que laboratorios de investigación generen y apliquen tecnología propia. Pero estos esfuerzos no son suficientes, se requiere de una concientización colectiva para que desde el aula se socialice la necesidad de resolver toda clase de problemas aplicando el conocimiento impartido en clases, y no se debe esperar a una asignatura o catedra de emprendedurismo o innovación, sino desde cualquier tópico que se aborde en ciencias e ingeniería, ya que además de abstraer del mundo real el problema, se deben plantear las diversas alternativas de solución, las implicaciones tecnológicas para llevarlas a cabo, la importancia de la implementación, pero sobre todo, resolver el problema quizá por etapas o versiones hasta llegar a la solución óptima.

**María del Carmen Santiago Díaz
Gustavo Trinidad Rubín Linares**

Estudio y Análisis de Seguridad en un Sistema de Información Web

Luz María Hernández Cruz, Diana Concepción Mex Alvarez, Margarita Castillo Tellez
Oscar Ezequiel de la Cruz Ek⁴

Universidad Autónoma de Campeche, Facultad de Ingeniería. Campeche, México

¹lmhernan@uacam.mx, ²diancmex@uacam.mx, ³mcastill@uacam.mx, ⁴al053938

Resumen. A continuación, se presenta el estudio del análisis de seguridad de un sistema de información web aplicando la Norma ISO 27002. En el cual se identifican las vulnerabilidades con una herramienta de software, después, con base en las vulnerabilidades detectadas se proponen mecanismos de seguridad para mitigarlas, por último, se evalúa el resultado obtenido. Aportando una visión actual de los diferentes mecanismos de seguridad destinados a conseguir un sistema de información seguro y confiable. Además, se contribuye a ostentar los beneficios de la inclusión de mecanismos de seguridad para preservar la integridad, confidencialidad y disponibilidad dentro utilizando un estándar internacional.

Palabras Clave: 'Seguridad', 'Software', 'Sistemas'

1 Introducción

Esta investigación documenta la metodología y el análisis de vulnerabilidades del sistema de información web "BITA", así como los mecanismos de seguridad propuestos para mitigar dichas vulnerabilidades alineados a la norma estándar internacional ISO 27002; cuyo valor agregado radica en servir de guía para su adaptación dentro de otras aplicaciones web.

2 Metodología

El presente trabajo se realiza implementando una metodología experimental propuesta, que se divide en tres fases principales a seguir: Identificación, Detección y Resolución. Esta metodología, se despliega como una alternativa para la implementación de seguridad en el desarrollo de sistemas de información web.

Las dos variables principales a tratar: VI (variable independiente) representa las vulnerabilidades de seguridad encontradas en el método heurístico con la herramienta de software VEGA y VD (variable dependiente) representa el mecanismo de seguridad propuesto para mitigar las vulnerabilidades encontradas.

3 Desarrollo

Enseguida, se analiza el caso de estudio un sistema de información web desarrollado para automatizar el proceso de control y seguimiento de bitácoras y expedientes clínicos odontológicos digitales (BITA) procedentes del servicio de atención de clínicas de la Facultad de Odontología en la Universidad Autónoma de Campeche, debido a la cantidad y criticidad de la información que se maneja.

El estudio se realiza a partir de los controles de seguridad de acceso y operativa según la Norma ISO 27002 alineados a la metodología experimental propuesta. (ISO 27002, s.f.). En la fase de Identificación y Detección se encuentran las siguientes vulnerabilidades: VI₁ = Vulnerabilidad contraseña de texto limpio, VI₂ = Cookie de sesión sin bandera segura, VI₃ = Campo de contraseña de formulario con autocompletar habilitado, SA = Seguridad en la aplicación, SR = Seguridad en la red y SBD = Seguridad en la base de datos. La Tabla 1 muestra el resumen del estado (status) atendido (✓) y no

atendido (×) en el sistema de información web “BITA” de las vulnerabilidades encontradas alineadas a la Norma ISO 27002.

Tabla 1. Resumen de la Fase de Identificación

(Identificador) Controles de Seguridad	Status	Referente asociado
Seguridad de Acceso		
CA1. Restricción del acceso a la información	×	VI ₁ , VI ₃
CA2. Procedimientos seguros de inicio de sesión	×	VI ₂
CA3. Gestión de contraseñas de usuario	×	VI ₁ , VI ₃
CA4. Control de acceso al código fuente de los programas	✓	SA
Seguridad Operativa		
Protección contra código malicioso		
CO1. Controles contra el código malicioso	×	SA, SR, SBD
Copias de seguridad		
CO2. Copias de seguridad de la información	×	SBD
Gestión de la vulnerabilidad técnica		
CO3. Gestión de las vulnerabilidades técnicas	×	VI ₁ , VI ₂ , VI ₃ , SA, SR, SBD
CO4. Restricciones en la instalación de software	✓	SR

Para cada control de seguridad de la norma ISO 27002 del caso de estudio, la Tabla 2 muestra los mecanismos o medidas de seguridad asociados.

Tabla 2. Mecanismos de Seguridad

Controles de Seguridad definidos para la aplicación web BITA
<ul style="list-style-type: none"> • Cifrado (SHA-256) • Manejo de Servlet (Cookies y Sesiones) • GUI (Interfaz Gráfica de Usuario) (Configurar propiedad Autocomplete con deshabilitado) • Contrafuegos (Firewall) Filtrado de Puertos • Uso de Software Legítimo • Uso de Software periódico para el Escaneo de la Red • Usuario (Nivel de acceso y Política de seguridad en la contraseña) • Configurar Copias de Seguridad Automáticas (Backups) • Configurar el Registro Binario, Registro de Consultas y Registro de Errores en el Sistema Gestor de Base de Datos.

Resultados

Después de implantar los mecanismos de seguridad, se asigna un nivel de Efectividad (alta = 3, media=2 y baja=1) y se realiza el cálculo del Promedio de los datos de efectividad (Pe) usando las ecuaciones (1) y (2) para determinar si la implantación de los mecanismos fue exitosa.

$$Pe = \sum \frac{Efectividad}{Total\ de\ Mecanismos} \quad (1)$$

Siguiendo el análisis de resultados al implementar los mecanismos de seguridad descritos en la metodología experimental presentada, se calcula el Riesgo residual (Rr) correspondiente a cada control de seguridad mediante la siguiente ecuación:

$$Rr = \frac{Nivel\ de\ riesgo}{Promedio\ de\ Efectividad} \quad (2)$$

Al obtener un Total de riesgo residual (perfil de riesgo) de 7 y compararlo con el MaxR = 16 y el MinR = 6, podemos decir que se ha conseguido una arquitectura de seguridad sólida en el sistema de información web de estudio. La Figura 1 muestra el resumen de Efectividad resultante de los mecanismos de seguridad implantados.

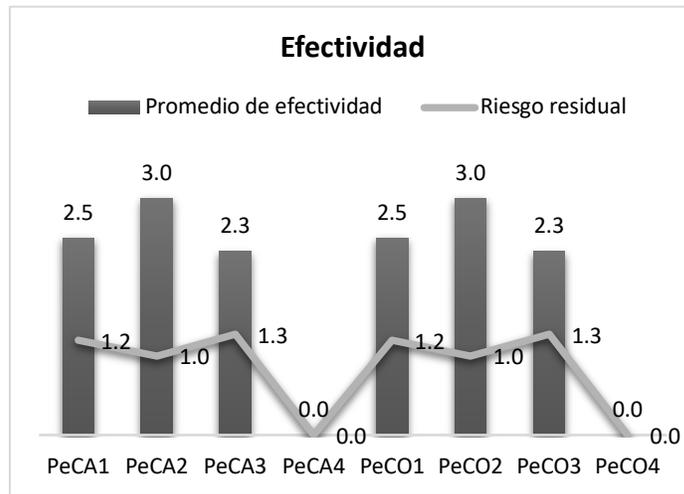


Fig. 1. Efectividad de los mecanismos de seguridad implementados.

4 Conclusiones y estudios futuros

No cabe duda que se necesita concientizar y crear cultura de la seguridad en los sistemas de información incluyendo mecanismos de seguridad para garantizar, en la medida de lo posible, la seguridad en el uso y manejo de información de los mismos. Actualmente, las fortalezas de los sistemas de información radicarán en la seguridad que ofrezcan. Las Tecnologías de Información y Comunicación son el medio, pero los Sistemas de Información son el objetivo

Referencias

1. Baca Urbina, G. (2016). *Introduccion a la Seguridad informática*. Grupo Editorial PATRIA.
2. *Blogging googling*. (11 de Abril de 2012). Obtenido de <https://cirovladimir.wordpress.com/2012/04/11/java-obtener-el-hash-sha-256-de-una-cadena/>
3. Burnett, M., & Foster, J. C. (2004). *Hacking the Code: ASP.NET Web Application Security*. Syngress Publishintg.
4. Castillo, L. (20 de Marzo de 2017). *Conociendo Github*. Obtenido de <http://conociendogithub.readthedocs.io/en/latest/data/introduccion/>
5. Didglee. (24 de Septiembre de 2016). *Mozilla Developer Network*. Obtenido de https://developer.mozilla.org/en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion
6. GUZMÁN, Á. (Agosto 2012). ITIL v3 -Gestión de Servicios de TI. *Revista ECORFAN - México CÓMPUTO*, 801-806.
7. International Organization for Standardization. (s.f.). *International Organization for Standardization*. Obtenido de <https://www.iso.org/>
8. ISO 27002. (s.f.). *ISO 27002.es*. Obtenido de <http://www.iso27000.es/iso27002.html>

Análisis de fraudes en Transacciones Bancarias Aplicando Minería de Datos

Víctor Giovanni Morales Murillo, María Josefa Somodevilla García,
Magali Fong Juárez, Ivo Humberto Pineda Torres
Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla,
Edificio CC01, 14 sur y Ave. Sn. Claudio, Fraccionamiento Jardines de Sn. Manuel
C.P. 72570 Puebla, México
vg055@hotmail.com , mariajsomodevilla@gmail.com, magali.fong@outlook.com,
ivopinedatorres@gmail.com

Resumen. El fraude es un problema para los bancos porque es difícil detectarlo y predecirlo. La solución que ofrecen los bancos es el reembolso pero lo ideal es evitarlo. Se presenta un análisis que se realizó a un conjunto de datos financieros obtenidos del simulador PaySim. Se importó el conjunto de datos a Weka, se pre-procesó el conjunto de datos, se aplicó una técnica descriptiva para identificar el atributo a clasificar y se aplicaron tres técnicas predictivas para comparar resultados.

Palabras Clave: Fraude, minería de datos, técnicas descriptivas, técnicas predictivas, métricas.

1 Introducción

Los delitos informáticos están aumentando porque la mayoría de las personas tienen acceso al Internet, estos delitos no solo son la piratería y el desciframiento, sino también incluyen la extorsión, la pornografía infantil, el lavado de dinero, la piratería de software, el espionaje corporativo y delitos de fraudes financieros, por nombrar algunos. Los reclamos asociados a transacciones fraudulentas en el sistema bancario es un grave problema financiero y social porque representa una alta pérdida de dinero para los bancos y sus clientes. Por tal motivo, existe un gran interés para poder predecir transacciones fraudulentas y así poder evitarlas.

Obtener acceso a conjuntos de datos de transacciones móviles para investigación es una tarea muy difícil debido a la naturaleza privada intrínseca de tales transacciones. Los investigadores solicitan permisos y acceso a conjuntos de datos financieros. En el presente trabajo se realiza un análisis para la detección de fraudes con un conjunto de datos financieros sintéticos obtenido por el simulador PaySim que se recopiló del trabajo de [13], en la sección de *Conjunto de datos* se presenta la estructura del conjunto de datos y su pre-procesamiento. Sin embargo, existe el cuestionamiento si es suficiente trabajar con datos sintéticos en lugar de datos reales. Esto es una preocupación primordial para cualquier investigador que desee realizar pruebas científicas, pero no tiene o tiene acceso limitado a un conjunto de datos financieros reales [13].

El análisis que se presenta en el artículo se centra en el tipo de transacción que representa un fraude en el conjunto de datos, estos tipos de transacción son cinco: CASH-IN, CASH-OUT, DEBIT, PAYMENT y TRANSFER [13]. CASH-IN es el proceso de aumentar el saldo de la cuenta mediante el pago en efectivo a un comerciante. CASH-OUT es el proceso opuesto de CASH-IN, significa retirar dinero de un comerciante, lo que disminuye el saldo de la cuenta. DEBIT es un proceso similar al de CASH-OUT e implica enviar el dinero del servicio de dinero móvil a una cuenta bancaria. El PAYMENT es el proceso de pago de bienes o servicios a los comerciantes que disminuye el saldo de la cuenta y aumenta el saldo del receptor. TRANSFER es el proceso de enviar dinero a otro usuario del servicio a través de la plataforma de dinero móvil. Hay otros

tipos de transacciones que decidimos excluir de la simulación debido al bajo porcentaje de datos encontrados en la muestra.

La estructura del artículo se compone de las siguientes secciones. En la sección 2, se presenta el marco teórico que contiene los antecedentes y las técnicas de minería de datos. En la sección 3, se presenta el estado del arte. En la sección 4, se presenta la metodología aplicada al conjunto de datos, la cual comprende la aplicación de técnicas descriptivas y predictivas. En la sección 5, se discuten los resultados, las métricas de evaluación y la comparación de resultados. Finalmente, en la sección 6, se presentan las conclusiones con las aportaciones de este artículo.

2 Marco teórico

2.1 Antecedentes

En 2011, los reclamos asociados a transacciones fraudulentas en el sistema bancario reportados a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros alcanzaron un monto de 476 millones de pesos. El total de operaciones asociadas a alguna actividad criminal fue de 119,000 transacciones, la mayor parte correspondía a tarjetas de crédito, que es donde hay un mayor número de resolución de conflictos a favor del cliente, pues cuatro de cada 10 incidentes implican un reembolso para el usuario. De acuerdo con la división *Business Analytics* de SAS México, muchas de las principales prácticas delictivas relacionadas con productos bancarios pueden identificarse y combatirse de manera temprana. Señala la compañía SAS México que el fraude es un problema creciente para los bancos en gran parte porque es muy difícil de detectar debido a que los estafadores emplean técnicas cada vez más sofisticadas que les permiten actuar sin mayores inconvenientes y sin ser detectados [5].

Los principales delitos que se han identificado se describen a continuación [5]. (1) Pérdida o robo de la tarjeta: sucede cuando una persona hace uso de una tarjeta que ha sido olvidada o robada, fingiendo ser el titular, (2) duplicado de tarjeta o *skimming*, donde el duplicado se realiza y se codifica sin el permiso de la compañía bancaria. La mayoría de los casos implican la copia de la información de la banda magnética de una tarjeta genuina sin el conocimiento del titular. De este fraude será inconsciente el titular hasta que los montos inexplicados aparecen en sus estados de cuenta. (3) Robo de datos: éste ocurre cuando roban la información de la tarjeta durante una transacción o por medio de un recibo y lo utilizan para hacer compras a distancia, principalmente por teléfono o a través de Internet. (4) Robo de la tarjeta antes de la entrega al titular: este fraude se produce cuando una tarjeta es sustraída antes de llegar al domicilio del titular, generalmente ocurre cuando la entidad financiera envía la tarjeta por correo y no cuenta con los elementos eficaces de acuses de recibo. (5) Cambio de identidad en tarjetas, existen dos tipos: (5.1) fraude de uso: cuando un criminal roba documentos, como estados de cuenta, y los utiliza para abrir una cuenta nueva a nombre de la víctima y (5.2) toma de posesión de la cuenta: el estafador utilizará datos personales del titular para solicitar al banco que dirija pagos a otra parte.

La minería de datos es el proceso de descubrir patrones y conocimientos interesantes a partir de grandes cantidades de datos [9]. Las técnicas de minería de datos intentan obtener patrones o modelos a partir de datos recopilados, además las técnicas son implementadas por varios algoritmos. Estas técnicas se clasifican en dos categorías: descriptivas y predictivas [8]. Las técnicas descriptivas presentan un aprendizaje no supervisado que agrupan instancias con características o atributos similares formando grupos o clusters, estas técnicas sirven para identificar el atributo que se puede utilizar para las técnicas de predicción. Las técnicas predictivas presentan un aprendizaje supervisado que con base en un conjunto de datos clasificado por expertos se entrena a sus algoritmos para poder predecir la clase de una nueva instancia. Este trabajo aplica técnicas de minería de datos [11] para realizar un análisis de fraudes en transacciones bancarias.

3 Estado del arte

Las investigaciones se han enfocado en generar y analizar conjuntos de datos financieros sintéticos porque es complejo obtener datos reales de transacciones bancarias. En el trabajo de [15] se presenta la primera implementación de un simulador para transacciones financieras de dinero móvil que utiliza el concepto de MABS (simulación basada en agentes múltiples). En el trabajo de [7] se presenta otra técnica similar para generar registros sintéticos para la detección de fraudes, en donde, la principal diferencia es que había datos reales disponibles para calibrar los resultados y comparar la calidad del resultado del simulador, el propósito de este estudio fue generar datos de prueba para que los investigadores pueden usar para evaluar diferentes enfoques. En el trabajo de [14] se presenta un simulador llamado BankSim que utiliza MABS de pagos financieros, este simulador se basa en la información financiera agregada de pagos durante los 6 meses de las dos principales ciudades de España. En el trabajo de [13] se presenta un simulador llamado PaySim que simula transacciones de dinero móvil basadas en una muestra de transacciones reales extraídas de un mes de registros financieros de un servicio de dinero móvil implementado en un país africano, los registros originales fueron proporcionados por una empresa multinacional, que es el proveedor del servicio financiero móvil que actualmente se ejecuta en más de 14 países de todo el mundo.

En el trabajo de [18] se presenta el uso de la minería de datos a través de algoritmos de árboles de clasificación J48 y reglas de asociación para la posible detección de fraudes a nivel de tarjetas de crédito (clonación de tarjetas) y se presenta una comparación de los resultados obtenidos con ambas técnicas. Además, se expone la *teoría sobre las transacciones delictivas* que plantea la existencia de patrones en el comportamiento asociados a los factores de un fraude como son la localización, la hora del día y la temperatura. En el presente trabajo se utilizara el conjunto de datos de [13] para realizar un análisis con las técnicas de minerías de datos para predecir fraudes en transacciones bancarias en dinero móvil.

4 Metodología

La metodología utilizada en este análisis de datos financieros está basada en la metodología KDD (*Knowledge Discovery in large Databases*). En particular consta de la descripción y pre-procesamiento del conjunto de datos, seguido de la aplicación de técnicas descriptivas y predictivas de minería de datos. Y finalmente de la evaluación, difusión y uso.

4.1 Conjunto de datos

Los conjuntos de datos financieros son importantes para las investigaciones en el dominio de la detección de fraudes que es el objetivo de este trabajo. El conjunto de datos se obtuvo del trabajo de [13] que se encuentra en www.kaggle.com, este sitio web se encarga de recolectar y gestionar colecciones de datos de diferentes temas a nivel internacional. Se recopiló el conjunto de datos de [13] porque existe una falta de información sobre los datos reales financieros sobre las cuentas de diferentes clientes debido a la privacidad y seguridad de los datos. El conjunto de datos que se utiliza en este artículo está formado por datos sintéticos generados por el simulador PaySim que simula transacciones de dinero móvil basadas en una muestra de transacciones reales extraídas de un mes de registros financieros de un servicio de dinero móvil implementado en un país africano. Los registros originales fueron proporcionados por una empresa multinacional, que es el proveedor del servicio financiero móvil que se ejecuta actualmente en más de 14 países de todo el mundo. Este conjunto de datos sintéticos se reduce 1/4 del conjunto de datos original. En la tabla 1, se muestran los atributos con su significado del conjunto de datos [13].

Tabla 1. Atributos del conjunto de datos.

Número	Atributo	Definición
1	Paso	Mapea una unidad de tiempo en el mundo real. En este caso 1 paso es 1 hora de tiempo, total de pasos 744 (simulación de 30 días).
2	Tipo	CASH-IN, CASH-OUT, DEBIT, PAYMENT y TRANSFER.
3	Monto	Monto de la transacción en moneda local.
4	NombreOrigen	Cliente que inició la transacción.
5	ViejoBalanceOrigen	Saldo inicial antes de la transacción.
6	NuevoBalanceOrigen	Nuevo saldo después de la transacción.
7	NombreDestino	Cliente que es el destinatario de la transacción.
8	ViejoBalanceDestino	Destinatario del saldo inicial antes de la transacción. Tenga en cuenta que no hay información para los clientes que comienzan con M (Comerciantes).
9	NuevoBalanceDestino	Nuevo receptor de saldo después de la transacción. Tenga en cuenta que no hay información para los clientes que comienzan con M (Comerciantes).
10	EsFraude	Nuevo receptor de saldo después de la transacción. Tenga en cuenta que no hay información para los clientes que comienzan con M (Comerciantes).
11	EsBanderaDeFraude	El modelo de negocio apunta a controlar las transferencias masivas de una cuenta a otra y marca los intentos ilegales. Un intento ilegal en este conjunto de datos es un intento de transferir más de 200.000 en una sola transacción.

El conjunto de datos se presenta en el archivo paysim1.csv y contienen un total de 1,048,576 de instancias, en la figura 1 se muestra el archivo paysim1.csv.

	A	B	C	D	E	F	G	H	I	J	K
1	step	type	amount	nameOrig	oldbalanceO	newbalanceF	nameDest	oldbalanceD	newbalanceI	isFraud	isFlaggedFraud
2	1	PAYMENT	9839.64	C123100681	170136	160296.36	M19797871	0	0	0	0
3	1	PAYMENT	1864.28	C166654429	21249	19384.72	M20442822	0	0	0	0
4	1	TRANSFER	181	C130548614	181	0	C553264065	0	0	1	0
5	1	CASH_OUT	181	C840083671	181	0	C38997010	21182	0	1	0
6	1	PAYMENT	11668.14	C204853772	41554	29885.86	M12307017	0	0	0	0
7	1	PAYMENT	7817.71	C90045638	53860	46042.29	M57348727	0	0	0	0
8	1	PAYMENT	7107.77	C154988899	183195	176087.23	M40806911	0	0	0	0
9	1	PAYMENT	7861.64	C191285043	176087.23	168225.59	M63332633	0	0	0	0
10	1	PAYMENT	4024.36	C126501292	2671	0	M11769321	0	0	0	0
11	1	DEBIT	5337.77	C712410124	41720	36382.23	C195600860	41898	40348.79	0	0
12	1	DEBIT	9644.94	C190036674	4465	0	C997608398	10845	157982.12	0	0
13	1	PAYMENT	3099.97	C249177573	20771	17671.03	M20965391	0	0	0	0
14	1	PAYMENT	2560.74	C164823259	5070	2509.26	M97286527	0	0	0	0
15	1	PAYMENT	11633.76	C171693289	10127	0	M80156915	0	0	0	0
16	1	PAYMENT	4098.78	C102648383	503264	499165.22	M16353782	0	0	0	0

Fig. 1. Muestra del conjunto de datos en el archivo paysim1.csv

4.1.1 Pre-procesamiento

En primera instancia, los datos del archivo paysim1.csv se presentan sin formato específico en el software Excel, esto quiere decir, que los valores numéricos se representan como cadenas de texto y no como valores numéricos, entonces a estos valores se les cambia su formato a numérico. En segunda instancia se importó el conjunto de datos a MySQL, para esto se creó una base de datos llamada delitos con una tabla llamada fraude, donde se importó el archivo paysim1.csv. En tercera instancia se utilizó el software de Weka, que es una colección de algoritmos de aprendizaje automático para tareas de minería de datos que contiene herramientas para la preparación de datos, clasificación, regresión, agrupación, extracción de reglas de asociación y visualización [17]. Utilizando Weka se conectó la base de datos de delitos con su tabla fraude para exportar los datos al archivo Fraude.arff con un 1,048,575 instancias.

El primer filtro que se utiliza es *Discretize* que discretiza en 2 bins los atributos *EsFraude*, con la discretización del atributo *EsFraude* observamos que existen 1,047,433 instancias que no son fraude y 1142 instancias que si son fraude. El segundo filtro que se aplicó al conjunto de datos es *RemoveWithValues* que elimina las instancias de acuerdo a condiciones definidas sobre uno de los atributos [8]. *RemoveWithValues* se utiliza para remover las instancias que no son fraude que se encuentran en el atributo *esFraude* con la finalidad de conservar solo las instancias que si son fraude para predecir el tipo de fraude de una transacción. El resultado del filtro *RemoveWithValues* reduce el número de instancias de 1,048,575 a 1142, se observa que el tipo de transacción TRANSFER tiene 564 instancias y CASH_OUT tiene 578 instancias, sin embargo, los tipos de transacción CASH-IN, DEBIT y PAYMENT tienen 0 instancias. Esto quiere decir que los fraudes únicamente se presentan en el tipo de transacción TRANSFER y CASH_OUT. En la figura 2, se muestra el resultado de aplicar el filtro *RemoveWithValues*.

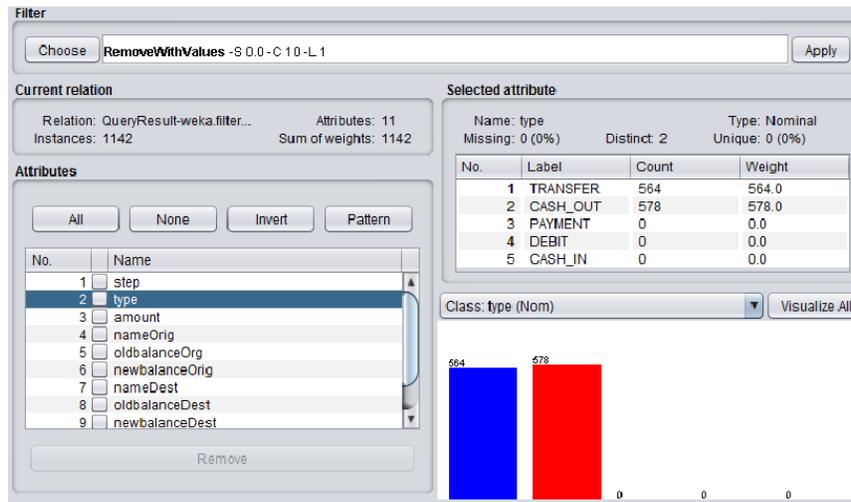


Fig. 2. Resultado de la aplicación del filtro *RemoveWithValues*.

4.2 Aplicación de técnicas descriptivas

En este trabajo utilizo el agrupamiento numérico con la técnica de *simpleKMeans* que forma k grupos con respecto a los patrones o características que presenta cada instancia para ser asignada a un grupo. Se aplicó esta técnica con 2 números de grupos (clusters) considerando los tipos de transacciones TRANSFER y CASH_OUT porque los tipos PAYMENT, DEBIT y CASH_IN no se presentan en ninguna instancia de fraude. Además, se ignoran los atributos que presentan una menor importancia que son *Paso* que es el tiempo en el que se comete el fraude pero es común que se cometan a cualquier hora, *NombreOrigen* y *NombreDestino* porque es común que solo se cometa una vez un fraude para una cuenta de origen y una cuenta de destino, *EsFraude* y *EsBanderaDeFraude* porque solo se tienen en el conjunto de datos instancias que son fraude.

```

kMeans
-----
Number of iterations: 6
Within cluster sum of squared errors: 360.202132600871
Initial starting points (random):
Cluster 0: 999999.999999,999999,999999,0,463083.63,999999.999
Cluster 1: 999999.999999,999999,999999,0,0,0
Missing values globally replaced with mean/mode
Final cluster centroids:
Attribute      Full Data      Cluster#      0      1
(1142.0)      (333.0)      (809.0)
-----
amount:      477101.1603    730079.1337    372970.5482
oldbalanceOrig  470693.2431    716609.7994    369455.1319
newbalanceOrig  33944.3212     1330.0531     47366.9705
oldbalanceDest  426946.6849    1370852.1364    38416.9997
newbalanceDest  341547.5241    966888.0583    84149.3043
Time taken to build model (full training data) : 0.13 seconds

--- Model and evaluation on training set ---
Clustered Instances
0 333 ( 29%)
1 809 ( 71%)
Class attribute: type
Classes to Clusters:
0 1 <-- assigned to cluster
0 0 | PAYMENT
9 555 | TRANSFER
324 254 | CASH_OUT
0 0 | DEBIT
0 0 | CASH_IN
Cluster 0 <-- CASH_OUT
Cluster 1 <-- TRANSFER
Incorrectly clustered instances : 263.0 23.0298 %
    
```

Fig. 3. Los dos clusters formados por *simpleKMeans*.

En la figura 3, se observa que se formaron dos cluster, el cluster 0 corresponde al tipo CASH_OUT y el cluster 1 que corresponde para el tipo TRANSFER. El cluster 0 presenta en el atributo Monto un promedio de 730,079.13, mientras que en el cluster 1 el atributo Monto se muestra con un promedio de 372,970.54. Estos valores describen que un fraude cuando es por el tipo CASH_OUT se realiza por altos montos de dinero y cuando es por TRANSFER se realiza por bajos montos de dinero para no ser detectado por los bancos. El error de instancias agrupadas es de 23.02%, esto quiere decir, que el número de instancias agrupadas correctamente es del 76.97%. Teniendo en cuenta los dos cluster obtenidos para los tipos de transacciones CASH_OUT y TRANSFER, consideramos el atributo *Tipo* de transacción como la clase a predecir. En la sección 4.3 se aplican técnicas predictivas para dicha clase.

4.3 Aplicación de técnicas predictivas

En este trabajo aplicando las técnicas descriptivas se seleccionó como clase a predecir el atributo *Tipo*. Para aplicar las técnicas predictivas se remueven los atributos que se ignoraron en la aplicación de técnicas descriptivas *Paso*, *NombreOrigen*, *NombreDestino*, *EsFraude* y *EsBanderaDeFraude*. Las técnicas predictivas que se utilizan son los algoritmos *J48*, *Naïve Bayes* y *Random Forest* [1].

El algoritmo *J48* es una versión del clásico algoritmo de árboles decisión C4.5 propuesto por Quilan, amplía las funcionalidades del C.4.5 al permitir el proceso de post-poda del árbol mediante un método de reducción de error *reducedErrorPruning* o que las divisiones sobre las variables discretas sean siempre binarias *binarySplits* [10]. El algoritmo *Naïve Bayes* se fundamenta en el teorema de Bayes que consiste en la probabilidad condicional, sin embargo, *Naïve Bayes* asume ingenuamente que las características no son condicionales pero si son independientes obteniendo la fórmula de *Naïve Bayes*, esta fórmula contabiliza la frecuencia de ocurrencias de las características seleccionadas y no se realizan búsquedas de hipótesis [2]. El algoritmo *Random Forest* conocido como bosques aleatorios, es un algoritmo compuesto por numerosos árboles de clasificación, en este algoritmo se definen una cantidad de árboles a desarrollar y una cantidad de m atributos tal que sea menor al total de atributos. Entre los árboles se reparten k patrones con reemplazo y se desarrollan los árboles, el resto de los patrones son usados para las pruebas [16]. En este trabajo se utilizaron las opciones *Cross-validation* y *Percentage Split*. Las métricas de evaluación y los resultados que se obtuvieron con estas pruebas aplicando los algoritmos *J48*, *Naïve Bayes* y *Random Forest* se presentan en la sección de resultados.

Es importante analizar las métricas de clasificación que existen en los sistemas de aprendizaje automático para evaluar y comprender el rendimiento de las técnicas predictivas [12]. En este trabajo se evaluaron las métricas de precisión, recall, f-measure [3], ROC Area y PRC Area [4], los resultados de estas evaluaciones se presentan en la siguiente sección.

5 Resultados

El primer resultado que se obtuvo es en la aplicación de las técnicas descriptivas utilizando *simpleKMeans* agrupando dos clusters por el atributo *Tipo* para encontrar los patrones que presentan los fraudes por el tipo de transacción CASH-IN, CASH-OUT, DEBIT, PAYMENT o TRANSFER. El resultado es del 76.97% como el número de instancias agrupadas correctamente, con este resultado se seleccionó el atributo *Tipo* como la clase a predecir con la aplicación de las técnicas predictivas.

El segundo resultado se obtuvo en la aplicación de las técnicas predictivas con los algoritmos J48, Naïve Bayes y Random Forest utilizando la opción *Percentage Split* con un 66% de instancias para el conjunto de entrenamiento y un 44% de instancias para el conjunto de pruebas. En la tabla 2, se muestran estos resultados.

Tabla 2. Resultados de la aplicación de las técnicas predictivas utilizando *Percentage Split* a 66%.

Técnica	Instancias correctas clasificadas	Precision	Recall	F-Measure	ROC Area	PRC Area
J48	98.19%	.982	.982	.982	.982	.973
Naïve Bayes	82.98%	.877	.830	.835	.973	.976
RandomForest	99.22%	.992	.992	.992	.997	.996
PROMEDIO	93.46%	.950	.934	.936	.984	.981

El tercer resultado se obtuvo en la aplicación de las técnicas predictivas con los algoritmos J48, Naïve Bayes y Random Forest utilizando la opción de *Cross-validation* [19] con un $k=10$ [6]. En la tabla 3, se muestran estos resultados.

Tabla 3. Resultados de la aplicación de las técnicas predictivas con la opción de *Cross-validation*.

Técnica	Instancias correctas clasificadas	Precision	Recall	F-Measure	ROC Area	PRC Area
J48	97.54%	.976	.975	.975	.973	.960
Naïve Bayes	84.58%	.882	.846	.851	.950	.947
RandomForest	98.33%	.984	.983	.983	.997	.996
PROMEDIO	93.48%	.947	.934	.936	.973	.967

Los resultados de las técnicas predictivas con *Percentage Split* a 66% y *Cross-validation* con un $k=10$ son similares con 0.02% de diferencias de instancias correctas clasificadas. Analizando los resultados de los algoritmos, se observa que los algoritmos de árboles de decisión: RandomForest y J48, presentan mejores resultados que Naïve Bayes porque en el conjunto de datos existen más atributos numéricos que nominales. Además, se observa que el algoritmo RandomForest presenta mejores resultados que del algoritmo J48 porque es una combinación de árboles aleatorios, sin embargo la diferencia es mínima.

6 Conclusiones

En este artículo se utilizó un conjunto de datos sintéticos generados por el simulador PaySim que simula transacciones de dinero móvil basadas en una muestra de transacciones reales extraídas de un mes de registros financieros de un servicio de dinero móvil implementado en un país africano. Se realizó un pre-procesamiento al conjunto de datos de fraude, se aplicaron técnicas descriptivas para identificar el atributo *Tipo* como variable de clase para las técnicas predictivas. Se aplicaron las técnicas predictivas con dos formas de evaluación *Percentage Split* a 66% y *Cross-validation* con un $k=10$, se utilizaron los algoritmos J48, Naïve Bayes y RandomForest. Se evaluaron las métricas de precisión, recall, f-measure, ROC área y PRC área. Finalmente, se analizaron los resultados en donde los algoritmos de árboles de decisión presentan mejores resultados que el algoritmo Naïve Baye porque existen un mayor número de atributos numéricos y destaca RandomForest de J48 por sus árboles aleatorios que utiliza.

El número de reclamos por transacciones fraudulentas en el sistema bancario reportados a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros es alto, por tal motivo, es importante aportar herramientas de seguridad y prevención para los posibles fraudes que se puedan cometer. Este trabajo es una aportación para la identificación de patrones de los tipos de fraude que se pueden

cometer. Además, el análisis de este trabajo sirve como base para futuras investigaciones que generen herramientas tecnológicas para la prevención de fraudes financieros.

Referencias

1. Berzal, F. (1 de Mayo de 2019). *Clasificación y predicción*. Obtenido de <http://elvex.ugr.es/idbis/dm/slides/3%20Classification.pdf>
2. Colmenares, L., Morales, V., Carrillo, M., & López, G. (2019). Validación de un algoritmo de clasificación para la identificación de interacciones. *Revista Ingeniería Investigación y Tecnología*, 1-8.
3. Computer Science Department of Cornell University. (2003). *Performance Measures for Machine Learning*. Estados Unidos de América: Cornell University.
4. Ekelund, S. (1 de Marzo de 2017). *Precision-recall curves – what are they and how are they used?* Obtenido de <https://acutecaretesting.org/en/articles/precision-recall-curves-what-are-they-and-how-are-they-used>
5. Expansión. (21 de Junio de 2012). *Expansión*. Obtenido de <https://expansion.mx/mi-dinero/2012/06/20/los-5-fraudes-mas-temidos-por-los-bancos>
6. Future Learn. (1 de Mayo de 2019). *Data Mining with Weka*. Obtenido de <https://www.futurelearn.com/courses/data-mining-with-weka/0/steps/25384>
7. Gaber, C., Hemery, B., Achemlal, M., Pasquet, M., & Urien, P. (2013). Synthetic logs generator for fraud detection in mobile transfer services. 3 International Conference on Collaboration Technologies and Systems (CTS), 174-179.
8. García, J., & Molina, J. (1 de Enero de 2012). *TÉCNICAS DE ANÁLISIS DE DATOS APLICACIONES PRÁCTICAS UTILIZANDO MICROSOFT*. Madrid: Universidad III de Madrid. Obtenido de http://matema.ujaen.es/jnavas/web_recurros/archivos/weka%20master%20recursos%20naturales/apuntesAD.pdf
9. Han, J., Kamber, M., & Pei, J. (2012). *DATA MINING Concepts and Techniques*. Waltham: Morgan Kaufmann.
10. Hernán, C., Gelvez, N., & Palacios, J. (2016). Análisis de datos mediante el algoritmo J48, sobre un cluster en la nube de AWS. *REDES DE INGENIERÍA*, 145.
11. Hernandez, O., Ramirez, Q., & Ferri, R. (2004). *Introducción a la minería de datos*. Madrid: Pearson educación.
12. Lever, J., Krzywinski, M., & Altman, N. (2016). Points of significance: Classification evaluation. *Nature Methods*, 541-542.
13. López, E., Elmir, A., & Axelsson, S. (1 de Enero de 2016). *Synthetic Financial Datasets For Fraud Detection, Synthetic datasets generated by the PaySim mobile money simulator*. Obtenido de kaggle: https://www.kaggle.com/ntnustestimon/paysim1#PS_20174392719_1491204439457_log.csv
14. Lopez-Rojas, E. A., & Axelsson, S. (2014). Social Simulation of Commercial and Financial Behaviour for Fraud Detection Research. In *Advances in Computational Social Science and Social Simulation*.
15. Lopez-Rojas, E., & Axelsson, S. (2012a). Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml). *Nordic Conference on Secure IT Systems*, 25-32.
16. Orozco, E., Iruretagoyena, G., Vazquez, S., Delgado, J., Castro, J., & Gutierrez, F. (2010). Métodos de clasificación para identificar lesiones en piel a partir de espectros de reflexión difusa. *Revista Ingeniería Biomédica*, 34-40.
17. The University of Waikato. (10 de Mayo de 2019). *waikato*. Obtenido de [waikato: https://www.cs.waikato.ac.nz/ml/weka/](https://www.cs.waikato.ac.nz/ml/weka/)
18. Wanumen, L. F. (2010). MINERÍA DE DATOS PARA LA PREDICCIÓN DE FRAUDES EN TARJETAS DE CRÉDITO. *Vinculos*, 44-57.
19. WIKIPEDIA. (15 de Mayo de 2019). *WIKIPEDIA K-medias*. Obtenido de <https://es.wikipedia.org/wiki/K-medias>

Determinación del Tamaño de una Mano en Imágenes Radiográficas Utilizando Landmarks

Jamid Israel Saenz Giron, Jonathan Gabriel Salazar Roldán,
Salvador Eugenio Ayala Raggi, Aldrin Barreto Flores
Facultad de Ciencias de la Electrónica,
Benemérita Universidad Autónoma de Puebla, Av. San Claudio y 18 sur,
Col. Jardines de San Manuel, C.P. 72570 Puebla, Puebla, México
israel.93.ig@outlook.com,
{jonasala117, saraggi, abfver}@gmail.com

Resumen. Al estudiar y analizar imágenes radiográficas de la mano, se encuentra que no suelen estar alineadas ni comparten una buena ecualización. Debido a que las manos tienen relaciones de aspecto y ángulos diversos, encontrar de manera automática características, nos permitiría alinearlas y mejorar la relación de contraste, de este modo se facilitará el posterior trabajo con las radiografías. Para lograr este objetivo se propone un método basado en puntos de interés o *landmarks*.

Palabras Clave: Procesamiento de Imágenes, Landmarks, Set de Datos, Radiografías, Análisis por Componentes Principales, Pre-procesamiento, Eigenfaces.

1 Introducción

La localización de *landmarks* o puntos de interés en imágenes radiográficas y en este caso en particular radiografías de manos, es un paso importante para localizar regiones de interés que proporcionen información determinada, donde la más común es determinar la edad ósea [1],[2], útil para médicos radiólogos, para diagnosticar enfermedades. Desafortunadamente las zonas colindantes de los huesos de las manos resultan ser similares, por lo que se vuelve un problema desafiante, pero además se encuentran otros obstáculos como son: el contraste de las imágenes y así como diversas anomalías que pueden surgir al tomar y digitalizar la radiografía. Dichos inconvenientes ocasionan que se busquen diversos métodos para localizar *landmarks*, aplicando procesamiento de imágenes como se propone en [3]. Los autores aplican un filtro gaussiano, para extraer bordes de los huesos de la mano con la detección de bordes de Canny, a continuación, segmentan los huesos con el algoritmo Watershed y pasan la imagen a formato binario. Enseguida extraen ejes de los dedos, formando ramas que corresponden a ejes longitudinales aproximados. Se refinan con el fin de posicionarlos en el centro de cada dedo analizando secciones transversales sucesivas. En el trabajo [4], se creó un sistema automático con el propósito de estimar la edad ósea, aplicando un método de procesamiento de imágenes y visión por computadora. El método para la detección de *landmarks*, consiste en tres pasos: entrenamiento, detección inicial y refinamiento; para el primero se generaron conjuntos de parches, los cuales, se utilizarán para determinar la ubicación de los puntos en la etapa de evaluación, conjuntamente se crearon formas para considerar la zona de los puntos de acuerdo con su posición relativa y todo el conjunto de *landmarks*. En el área de machine learning también se han realizado métodos como en [5], donde la idea básica es usar un bosque aleatorio para determinar el vector de desplazamiento de un parche de imagen para obtener *landmarks* y buscar una zona específica del hueso de

la mano como es la epífisis, la cual va determinando el crecimiento de la persona. También se han aplicado lo que son redes neuronales convolucionales como en [6], a partir de regresión de heatmap y configuración espacial, la red aprende a estimar la ubicación de los puntos y a eliminar información que ubicara de forma errónea las landmarks. Los autores además de usar radiografías de manos utilizan resonancias magnéticas de manos, encefalogramas laterales y tomografías de la medula espinal. Finalmente, en [7], se aplican métodos como es el de esquemas de registro híbrido, para modelar la deformación de la imagen como un proceso de regresión gaussiano y consideran landmarks como información adicional sobre deformaciones admisibles.

En las radiografías utilizadas, hay demasiada información, y parte de ésta no es útil, si se considera un banco grande de radiografías, es necesario obtener las zonas que aportan la información necesaria. El detectar los puntos de interés permitirá extraer solo la información que lo rodea, minimizando el poder computacional requerido. Debido a las características mencionadas se basó en el método de [8],[9], el cual es mayormente utilizado para el reconocimiento de caras, llamado Eigenfaces, compuesto por el análisis por componentes principales. Este documento se muestra como localizar landmarks de acuerdo con la obtención de información previa que es el entrenamiento y a partir de esta, localizar de manera automática puntos en las zonas del entrenamiento con radiografías nuevas. Para la primera, se extrajeron de un conjunto de imágenes sus valores característicos para crear dos eigenespacios de la parte superior e inferior del hueso medio del metacarpo y continuar con la segunda etapa llamada evaluación, donde se buscará encontrar dos landmarks en cada radiografía reduciendo la resolución y ubicar los puntos en dicha escala, y finalmente regresar a una resolución estándar la cual ubica los puntos de acuerdo con la primera localización.

2 Entrenamiento

De [10] se tomó un grupo de radiografías, para que sirvan de entrenamiento, en el grupo de entrenamiento se marcaron manualmente las *landmarks* mostrados en la Fig. 1, los puntos que nos interesa calcular automáticamente, estas marcas nos permitirán, recortar estas regiones más adelante (Fig. 3).



Fig. 1. Colocación Manual de Landmarks

Al analizar el banco de radiografías con el que se va a trabajar, es notorio una variación en el contraste de las radiografías, Fig. 2 por lo cual es necesario que se le aplique un pre-procesamiento a las imágenes, siendo un ajuste de contraste basado en los valores del histograma. Este ajuste se realiza calculando de acuerdo con las intensidades de los píxeles la media μ y desviación estándar σ . Para la media máxima y mínima se tiene que $Medmax = \mu + 1.5\sigma$ y $Medmin = \mu - 1.5\sigma$, este factor se determinó de forma empírica, de manera, por lo cual todas las imágenes ahora tienen un contraste más similar.

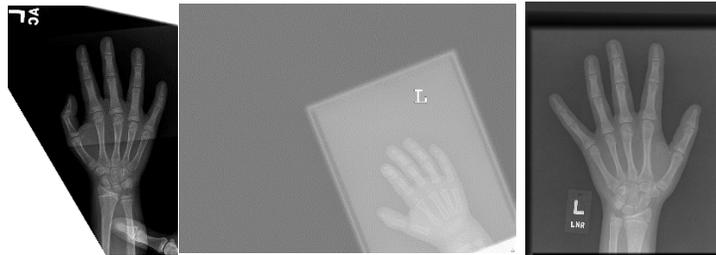


Fig. 2. Distintas radiografías del banco de imágenes, donde se aprecian los distintos contrastes de ellas.

Ahora se puede realizar un mapeo lineal de cada valor de gris en la imagen a un nuevo rango de 0 a 255. Lo siguiente fue realizar recortes de tamaño 13x13 pixeles de los puntos marcados para generar los dos espacios, Fig. 3.



Fig. 3. Recortes del hueso del metacarpo de baja resolución, para generar los dos eigenespacios, del lado izquierdo la parte superior del metacarpo, del lado derecho la inferior.

Puesto que la posición de la mano en cada radiografía es diferente, se debe de rotar cada recorte realizado de acuerdo con su ángulo dominante θ para posicionarlo hasta que el nuevo ángulo θ sea cero. Lo siguiente es aplicar una máscara circular de forma que en pasos posteriores solo se procese lo que se encuentre en el círculo sin que ésta afecte con valores o ruido. En la Fig. 4 se muestra cómo se rotó y aplicó lo mencionado anteriormente, para cada espacio.

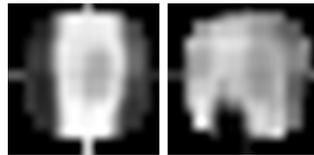


Fig. 4. Recortes del hueso del metacarpo de baja resolución para rotados con de acuerdo con su ángulo dominante θ y aplicada la máscara circular.

En este punto se tienen en total 1200 imágenes, con 600 para el primer espacio y 600 para el segundo, con lo que se procedió a llamar los espacios de Eigenmanos.

2.1 Método de Análisis por Componentes Principales (PCA)

Se busca representar datos de D dimensiones en un espacio de dimensión inferior, que mejor describan la variación, para reducir complejidad de operaciones, tiempo y espacio. Para esto el análisis de componentes principales cumple con estas condiciones, ya que se generan un conjunto ortonormal de vectores [11]. Para el entrenamiento se tienen los siguientes pasos:

1. Se tiene un conjunto de imágenes I_1, I_2, \dots, I_M , cada una debe convertirse a un vector $\Gamma_1, \Gamma_2, \dots, \Gamma_M$ de dimensión N^2 , concatenar cada vector formando una matriz de $N^2 \times M$.
2. Obtener el vector promedio Ψ :

$$\Psi = \frac{1}{M} \sum_{i=1}^M \Gamma_i \quad (1)$$

3. El vector promedio se debe restar a cada imagen para obtener un nuevo conjunto de vectores.

$$\Phi_i = \Gamma_i - \Psi \quad (2)$$

donde conforma la matriz $A = [\Phi_1 \ \Phi_2 \ \dots \ \Phi_M]$ de $N \times M$.

4. Calcular la matriz de covarianza C :

$$C = \frac{1}{M} \sum_{i=1}^M \Phi_i \Phi_i^T = AA^T \quad (3)$$

de $N^2 \times N^2$

5. Calcular los eigenvectores u_i de AA^T :

Debido a que AA^T es demasiado grande y eso no es práctico, se debe buscar una aproximación de estos vectores.

- a. Calcular los eigenvectores v_i de $A^T A$:

$$A^T A v_i = \mu_i v_i \quad (4)$$

Buscar una relación entre μ_i y v_i . Se obtiene que:

$$A v_i = \mu_i u_i \quad (5)$$

- b. Normalizar μ_i de manera que $||\mu_i|| = 1$
 6. Conservar solamente los K eigenvectores con más aportación.
 7. Obtener la matriz

$$\Omega^T = [w_1, w_2, \dots, w_M] \quad (6)$$

y

$$w_i = u_j^T \phi_i \quad (7)$$

donde $j = 1, 2, \dots, K$; $i = 1, 2, \dots, M$.

8. Proyección

- a. Dada una imagen desconocida Γ_D

- b. Realizar

$$\Phi = \Gamma_D - \Psi \quad (8)$$

- c. Calcular la proyección de acuerdo con:

$$w_i = u_j^T \phi_i \quad (9)$$

3 Evaluación

3.1 Localización de Landmarks

Ya que se tienen las matrices de las ecuaciones 5 y 6 para la parte superior e inferior del hueso medio del metacarpo, se pasa a la evaluación de imágenes radiográficas.

Para realizar la localización, se parte de reducir su escala a la nueva imagen, delimitar la zona y localizar los puntos para que después se aumente la escala y el proceso sea más rápido, al buscar en la imagen original. Ya que se busca en imágenes sucesivas al reducir A continuación se plantean los pasos para realizar dicha búsqueda:

1. Se carga la imagen radiográfica a evaluar $M(x)$.
2. Cambiar el tamaño de la imagen, reduciendo a 255 píxeles el valor más pequeño y el otro reduciéndolo para mantener la relación de aspecto.
3. Reducir a la mitad de su escala, la cual servirá para buscar y localizar los puntos característicos.
4. Aplicar la corrección de contraste ocupada en la sección de entrenamiento.
5. Se emplea un filtro pasa-bajas para reducir aportaciones de objetos alrededor.
6. Localizar los bordes de la imagen, mediante la detección de bordes de Canny.
7. Obtener el baricentro, que deberá ubicarse dentro de la mano.
8. A partir del baricentro realizar un recorte $R(x)$ de 60 píxeles arriba, abajo, derecha e izquierda.
9. Crear una ventana que servirá para realizar la proyección de cada eigenespacio en la imagen del paso 3.
10. De acuerdo con $R(x)$ realizar lo siguiente:
 - a. Tomar una ventana del tamaño del paso 9 en la radiografía.
 - b. Rotar la ventana de acuerdo con su ángulo dominante.
 - c. Aplicar una máscara circular.
 - d. Proyectar la ventana en su eigenespacio correspondiente.
 - e. Obtener w_p y calcular el error de reconstrucción (10) para almacenarlo en una matriz de errores

$$e = ||w_p - w_j|| \quad (10)$$

11. Localizar en la matriz de errores el valor mínimo para cada eigenespacio, para marcarlo como landmark.

4 Resultados

De la base de datos de la cual se extrajeron las imágenes de entrenamiento [9] se tomó un total de 200 imágenes para evaluar el método propuesto. A las radiografías entrantes, se reduce de escala y se les ajusta el contraste, esto es para que a continuación se pueda localizar el baricentro, el cual nos permite acotar la zona de búsqueda ya que este siempre está en dentro de la mano, Fig. 5. Y posteriormente se recorta la zona donde se buscarán las landmarks, Fig. 6.

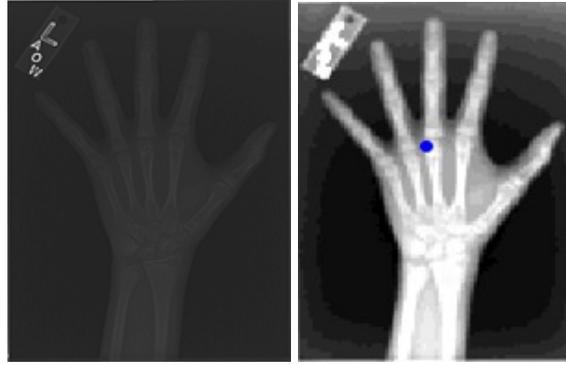


Fig. 5. Pasos iniciales para la localización de landmarks: a la izquierda, la entra original, a la derecha la imagen reducida en escala, con ajuste de constante y localización del baricentro.

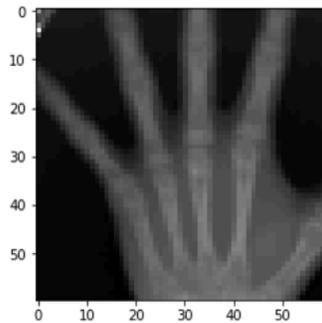


Fig. 6. Recorte de la radiografía a partir del baricentro localizado

Sobre esta sección de la radiografía de escala reducida, se fue extrayendo una ventana para ser procesada individualmente, la cual en este primer paso es de menor resolución que la imagen original, para proyectarla en los dos eigespacios, esta reconstrucción nos dará un error, este nos indicara que tan diferentes son las ventanas de nuestro espacio, el error lo podemos ver en la Fig. 7, la posición donde el error sea menor, implicara que es el punto que se busca, en este se tomara una ventana con mayor resolución y se repetirá el procedimiento hasta tener toda la resolución como se puede ver en Fig. 8. La cual nos muestra los puntos de interés encontrados.

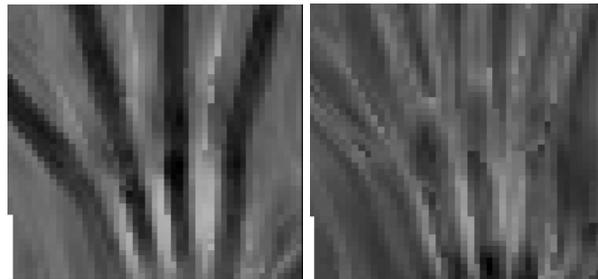


Fig. 7. Matrices de errores en los distintos eigespacios, se busca el valor mínimo del error para ubicar la landmark, del lado izquierdo la parte superior del hueso del metacarpo y del lado derecho la parte inferior del hueso del metacarpo.

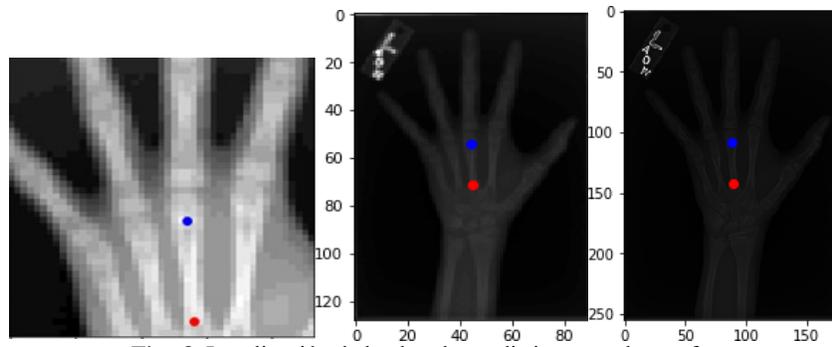


Fig. 8. Localización de landmarks en distintas escalas, se fueron localizando de izquierda a derecha.

El obtener estos puntos nos permitirá acotar de una mejor manera la mano para trabajar con ella, ya que muchas imágenes radiográficas incluyen bordes u otros objetos que no aportan información como las mostradas en Fig. 9.

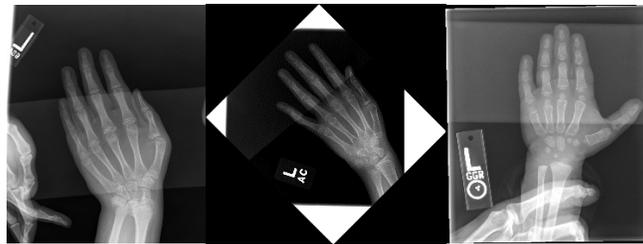


Fig. 9. Ejemplos de radiografías que contienen objetos extraños.

4 Conclusiones y trabajos futuros

En este trabajo se desarrolló un método para obtener de manera automática landmarks, estos puntos que se localizaron permitirán acotar un área en las radiografías la cual es la que trae la mayor aportación de la edad ósea, esta se utilizara para seguir desarrollando un trabajo para detectar la edad ósea de manera automática. En un futuro se aplicara este mismo método para marcar más áreas en la mano, con el fin de refinar las zonas de donde se extraerá la información, siendo estas la parte intermedia de los huesos tanto de las falanges proximales como de los huesos del metacarpo, el poder calcular la edad ósea de manera automática y eficiente, es importante ya que en la radiología es necesaria para detectar síntomas o enfermedades en menores de edad y atender enfermedades que en el futuro dañen la salud del menor siendo las más comunes: trastornos de crecimiento, problemas ortopédicos, enfermedades a nivel hormonal, entre otras.

Agradecimientos

Agradecer a Mauricio Longinos Garrido y a nuestro asesor Salvador Eugenio Ayala Raggi por su apoyo y asesoramiento en la realización de este proyecto.

Referencias

1. Tanner, J.; Whitehouse, R.; Cameron, N.; Marshall, W.; Healy, M.; Goldstein, H.: Skeletal maturity and prediction of adult height (tw2 method). *Archives of Disease in Childhood*, Vol.51, No. 6, pp. 488 (1976).
2. Greulich, Pyle, S., Radiographic atlas of skeletal development of hand wrist. *Quarterly Review of Biology*, Vol.26, Standford University Press. (1959).
3. Moreno, E. M.; Lopez, C.A.; Angel, M.; Andez, I.: Automatic detection of landmarks for image registration applied to bone age assessment. *5th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision*, pp. 117-122, (2005).
4. Banda, J.L.T.: Sistema automático de aprendizaje incremental supervisado para reconocimiento de la edad ósea. Benemérita Universidad Autónoma de Puebla, 2018.
5. Hanhmann, F.; Böer, G.; Gabriel, E.; Deserno, T.; Meyer, C.; Scramm, H.: Classification of Voting Patterns to Improve the Generalized Hough Transform for Epiphyses Localization. *Medical Imaging 2016: Computer-Aided Diagnosis*, Vol. 9785, No. 0, pp. 1-11, (2016).
6. Payer, C.; Štern, D.; Bischof, H.; Urschler, M.: Integrating spatial configuration into heatmap regression based CNNs for landmark localization, *Medical Image Analysis*, Vol. 54, pp. 207-219, (2019).
7. Lüthi, M.; Jud, C.; Vetter, T.: Using Landmarks as a Deformation Prior for Hybrid Image Registration. *Pattern Recognition*, pp. 196-205, (2011).
8. Turk, M.; Pentland, A.: Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*, Vol. 3, No. 1, pp. 71-86, (1991).
9. Turk, M.; Pentland, A.: Face recognition using eigenfaces. *International Conference on Pattern Recognition*, pp. 586-591, (1991).
10. Mader, K.: RSNA Bone Age Predict Age from X-Rays. Kaggle. <https://www.kaggle.com/kmader/rsna-bone-age> (2017). Accedido el 28 de Mayo de 2019.
11. Jolliffe, I.T.: Introduction: Principal Component Analysis. Springer, pp. 1-9 (2002).

Detección de Desbalance Financiero Utilizando Modelos Ocultos de Márkov

María De Lourdes Sandoval Solís, Marcela Rivera Martínez, Luis René Marcial Castillo,
Gladys Linares Fleites

Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla,
4 Sur 104, Colonia Centro Puebla, 72000

¹maria.sandoval@correo.buap.mx, ^{2,3}{cmr, lmc}@cs.buap.mx, ⁴gladyslinares1@yahoo.es

Resumen. En este trabajo se presenta la aplicación de los Modelos Ocultos de Márkov para detectar el desbalance financiero. Se Muestra la convergencia de la matriz de transición al aumentar el tamaño de la secuencia de observaciones. Se ejemplifica el método con la base de datos Berka.

Palabras Clave: Modelos Ocultos de Márkov, Detección de Desbalance Financiero.

1 Introducción

Los Modelo Oculto de Márkov HMM (Hidden Márkov Model), tradicionalmente se han utilizado en el área de computación para detectar patrones y detectar los cambios de éstos. En las cadenas de Márkov, los estados son observables, por esto también se les conoce como Modelos de Márkov Observables, sin embargo, para varios problemas de interés el estado no siempre es observable, como puede ser en el reconocimiento de voz, en este únicamente se ve la señal de la voz, pero no el conjunto de palabras ó fonemas que lo conforman, a este tipo de estados se les llama ocultos. Un Modelo Oculto de Márkov (HMM) permite modelar este tipo de problemas.

El objetivo principal de este trabajo es determinar el Modelo Oculto de Márkov HMM que se adapte al desbalance de transacciones bancarias de un usuario. Mediante este modelo determinar el desbalance bancario. Para este objetivo se aplicó la técnica a dos cuentas bancarias de la base datos conocida como Berka [1].

2 Modelos Ocultos de Márkov

Un Modelo Oculto de Márkov (HMM) es un proceso estocástico doblemente embebido con un proceso aleatorio que no es observable (está oculto), pero que puede ser visto solamente a través de otro conjunto de procesos aleatorios que produzcan la secuencia de observaciones y satisface la siguiente propiedad: Propiedad de Márkov: Esta propiedad hace referencia a la falta de memoria de una proceso estocástico, esto es, el estado actual de un proceso únicamente depende de su estado anterior y no de la secuencia de eventos que precedieron a éste último estado. Los HMM está definido por los siguientes componentes:

- Q: Número de estados en el modelo, cada estado individual se etiqueta como q_1, q_2, \dots, q_N .
- O: Secuencia de observaciones tomadas de un vocabulario $V = \{v_1, v_2, \dots, v_M\}$, denotadas como $O = (O_1, O_2, \dots, O_M)$.
- A: la matriz de transición $A = \{a_{ij}\}$, donde cada a_{ij} representa la probabilidad del estado i al estado j : $a_{ij} = P(q_{t+1}=j \mid q_t = i)$.
- B: Probabilidad de observación de cada símbolo del vocabulario, también llamada probabilidad emisión, $b_j(k) = P(O_t = v_k \mid q_t = j)$, es decir, la probabilidad de que la observación O_t sea generada por el estado j .

- π : Distribución de probabilidad sobre el estado inicial $\pi = \{\pi_i\}$, definida como: $\pi_i = P(q_{1=i})$, es decir, la probabilidad de iniciar en alguno de los estados de q .

Es evidente que una especificación completa de un HMM requiere la estimación de los parámetros del modelo, A, B y π por lo tanto un HMM se define como λ .

$$\lambda = (A, B, \pi) \quad (1)$$

Este modelo toma dos suposiciones importantes, la primera, al igual que en las cadenas de Márkov de primer orden es la suposición de Márkov, el estado actual únicamente depende de su predecesor, expresado como:

$$\text{Suposición de Márkov } P(q_t | q_1, \dots, q_{t-1}) = P(q_t | q_{t-1}) \quad (2)$$

Como segunda suposición, la probabilidad de observación O_t depende únicamente del estado que la produce q_t y no de cualquier otro estado u observación, expresado matemáticamente como:

$$\text{Independencia de salida: } P(O_t | q_1, \dots, q_t, \dots, q_T, o_1, \dots, o_t, \dots, o_T) = P(o_t | q_t) \quad (3)$$

3 Tres Problemas De Los HMM

Los HMM Introducidos por Rabiner (1989) [2], se caracterizan por tres problemas esenciales, necesarios a resolver para hacer que los HMM sean aplicables a aplicaciones reales.

- Problema 1 (Probabilidad) : El primer problema consiste en la evaluación de una secuencia de observaciones O dado el modelo $\lambda = (A, B, \pi)$. La solución a este problema nos brinda la probabilidad de que la secuencia fuera generada por ese modelo λ , es decir: $P(O|\lambda)$.
- Problema 2 (Descodificación): Dada una secuencia de observación O y el modelo $\lambda = (A, B, \pi)$, determinar cuál es la secuencia de estados Q mas probable que haya generado la observación O .
- Problema 3 (Aprendizaje): Ajustar los parámetros A y B del modelo para maximizar la probabilidad de observación $P(O|\lambda)$.

3.1 Probabilidad

Para obtener la probabilidad total de la observación, se tiene que sumar sobre todas las posibles secuencias de Q estados ocultos, en general:

$$P(O|\lambda) = \sum_Q P(O, Q) = \sum_Q P(O|Q) P(Q) \quad (4)$$

Dada esto podemos notar que si tenemos un número de estados ocultos muy grande al igual que el tamaño de la cadena de observación es muy grande tenemos un problema computacional del orden exponencial, lo cual implica que el tiempo de cómputo sería muy grande.

Para atacar el problema de tiempo computacional al que hemos llegado tendremos que hacer uso del algoritmo Forward que es del orden $O(N^2T)$, el cual evita hacer cálculos repetidos

3.1.1 Algoritmo Forward:

Considerando la siguiente variable $\alpha_t(j)$, definida de la siguiente forma:

$$\alpha_t(j) = P(O_1, O_2 \dots O_t, q_t = j | \lambda) \quad (5)$$

Esto representa la probabilidad de estar en el estado j después de t observaciones. Estas variables son guardadas en celdas, donde el valor de cada una se obtiene con la suma de las probabilidades de todos los caminos que llevan a dicha celda, de la siguiente forma:

$$\alpha_t(j) = \left(\sum_{i=1}^N \alpha_{t-1}(i) a_{ij} \right) b_j(O_t) \quad (6)$$

Algoritmo Forward

Inicialización:

$$\alpha_1(i) = \pi_i b_i(O_1) \quad 1 \leq i \leq N$$

Recursividad:

$$\alpha_t(j) = \left(\sum_{i=1}^N \alpha_{t-1}(i) a_{ij} \right) b_j(O_t) \quad 1 \leq j \leq N, 1 < t \leq T$$

Terminación:

$$P(O | \lambda) = \left(\sum_{i=1}^N \alpha_T(i) \right)$$

3.1.2 Algoritmo Backward

Ahora consideremos una variable $\beta_t(i)$, definida de la siguiente forma:

$$\beta_t(i) = P(O_{t+1}, O_{t+2}, \dots, O_T | q_t = i | \lambda) \quad (7)$$

Que es la probabilidad de ver las observaciones desde el tiempo $t+1$ hasta el final, y estar en el estado i al tiempo t . Estas variables son guardadas en celdas, donde el valor de cada una se obtiene con la suma de las probabilidades de todos los caminos que llevan a dicha celda, de la siguiente forma:

$$\beta_t(i) = \sum_{j=1}^N a_{ij} b_j(O_{t+1}) \beta_{t+1}(j) \quad (8)$$

Para más detalles de la demostración de las recurrencias de los algoritmos consulte [2,4].

Algoritmo Backward

Inicialización:

$$\beta_T(i) = 1 \quad 1 \leq i \leq N$$

Recursividad:

$$\beta_t(i) = \sum_{j=1}^N \alpha_{ij} \beta_{t+1}(j) b_j(O_{t+1}) \quad t = T-1, T-2, \dots, 1, \quad 1 \leq i \leq N$$

Terminación:

$$P(O|\lambda) = \sum_{j=1}^N \pi_j b_j(O_1) \beta_1(j)$$

3.2 Decodificación

El segundo problema del HMM es la decodificación, esto consiste en obtener la secuencia de estados ocultos Q que genere la observación O , es decir, de entre todas las secuencias de estados que puedan generar determinada secuencia de observaciones, se desea encontrar aquella que sea más representativa de la observación O . Para ello tenemos que encontrar cual es la secuencia de estados ocultos con mayor probabilidad. Podemos resolver este problema ejecutando el algoritmo Viterbi que es muy similar al algoritmo Forward.

Definimos la siguiente variable $v_t(j)$, de la siguiente forma:

$$v_t(j) = \max_{q_0, q_1, \dots, q_{T-1}} P(q_0, q_1, \dots, q_{T-1}, O_1, O_2, \dots, O_t = j | \lambda) \quad (9)$$

Como la probabilidad de estar en el estado j después de t observaciones y pasar sobre la secuencia de estados más probables, q_0, q_1, \dots, q_{T-1} . Estas variables son guardadas en celdas, donde el valor de cada una se obtiene con el cálculo del valor máximo de las probabilidades de todos los caminos que llevan a dicha celda, de la siguiente forma:

$$v_t(j) = \max_{i=1}^N v_{t-1}(i) a_{ij} b_j(O_t) \quad (10)$$

Ahora se define también la variable denominada backtrace(bt) similar a la variable del algoritmo de Viterbi (v), en lugar de mantener la probabilidad más alta, esta variable mantiene el número del estado con dicha probabilidad.

$$bt_t(j) = \arg \max_{i=1}^N v_{t-1}(i) a_{ij} b_j(O_t) \quad (11)$$

El valor de cada celda se puede calcular mediante el siguiente algoritmo:

3.2.1 Algoritmo Viterbi.

Inicialización:

$$v_1(i) = \pi_i b_i(O_1) \quad 1 \leq i \leq N$$

$$bt_1(i) = 1 \quad 1 \leq i \leq N$$

Recursividad:

$$v_t(j) = \max_{i=1}^N v_{t-1}(i) a_{ij} b_j(O_t) \quad 1 \leq j \leq N, \quad 1 < t \leq T$$

$$bt_t(j) = \arg \max_{i=1}^N v_{t-1}(i) a_{ij} b_j(O_t) \quad 1 \leq j \leq N, \quad 1 < t \leq T$$

Terminación:

$$P^* = \max_{i=1}^N v_T(i)$$

$$q_T^* = \arg \max_{i=1}^N v_T(i)$$

Para las demostraciones de las relaciones utilizadas en los algoritmos revisar los documentos de las referencias [4,5]

4 Desbalance de cuentas bancarias

4.1 Información seleccionada de la base de datos.

La información contenida en la base de datos se separó por el número de cuenta con sus respectivas transacciones y balance de cuenta. Posteriormente se seleccionaron 2 cuentas bancarias que pudieran aportar diferentes puntos de vista sobre el comportamiento de los movimientos que se realizan. Para el experimento se tomó una cuenta con balance positivo y una cuenta con balance negativo. Las 2 cuentas seleccionadas se muestran en la tabla las cuentas y el estado de balance.

Tabla 1. Cuentas bancarias de la Base de Datos Berka [1]

Número de cuenta	Tipo de balance	Cantidad obtenida del balance	Estado de balance
1069	Balance positivo	25220.50	Positivo
2335	Balance negativo cercano al neutro	2785.50	Negativo

Mostramos a continuación el comportamiento en las transacciones de las cuentas seleccionadas. Nos enfocamos en los montos que representa cada transacción y el balance que tiene la cuenta en cada momento de la transacción.

Cuenta 1069

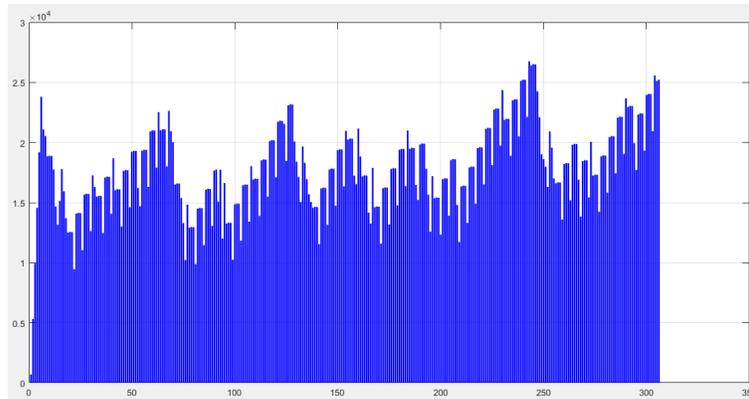


Fig. 1. Comportamiento del balance positivo en la cuenta 1069

Cuenta 2335

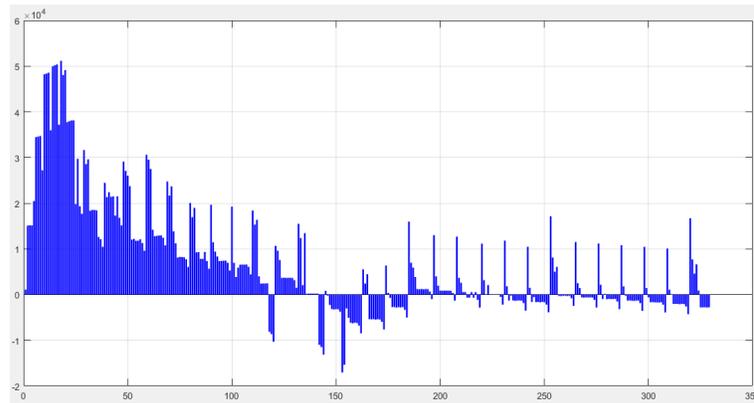


Fig. 2. Comportamiento del balance negativo en la cuenta 2335

4.2 Determinación del Modelo Oculto de Márkov

En el caso sobre el análisis de la Base de datos Berka, se usa la información de Transactions [1], se toman como estados del modelo las variables que contenían en el campo Operation, se añadió una sexta variable dado que la información de la base de datos contenía en ese campo datos faltantes por lo cual se le asigno un estado nuevo a ese campo faltante. Para definir las observaciones del modelo se siguió lo propuesto en el artículo Srivastava (2008) [3], dividir las diferentes cantidades de las transacciones en tres particiones usando el algoritmo del vecino más cercano con tres centroides obteniendo la observación por estado en la forma {1,2,3}.

Se muestra en la figura la determinación del HMM para cada cuenta bancaria.

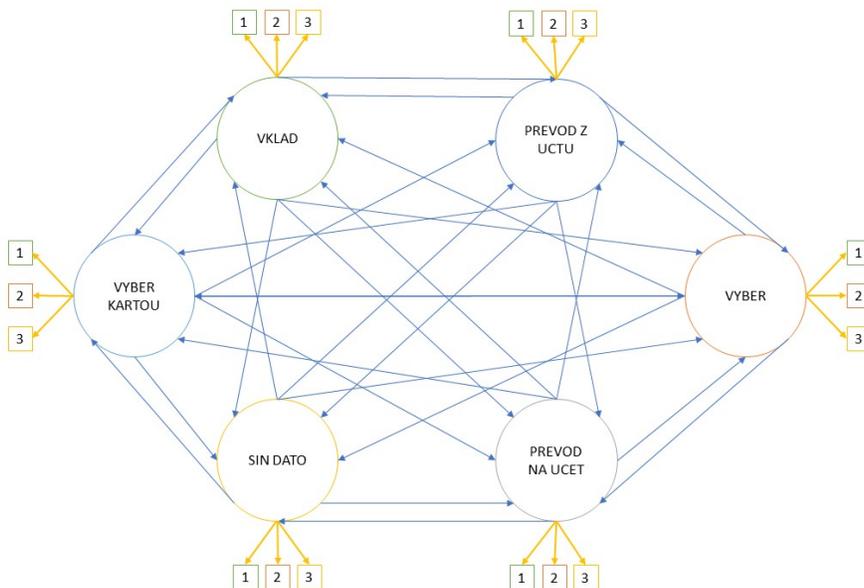


Fig. 3. Modelo Oculto de Márkov para las cuentas bancarias en la base de datos Berka.

4.3 Convergencia de las matrices de transición

Analizando el entrenamiento que se realiza en las matrices A y B del HMM, notamos que entre mayor sea el tamaño de muestra para entrenar estas matrices, se obtiene una convergencia para cada término de la matriz de transición. A continuación, se muestran los valores de la transición del estado i al estado j conforme aumenta el número de observaciones. Se muestra los resultados para una matriz de transición de tres estados.

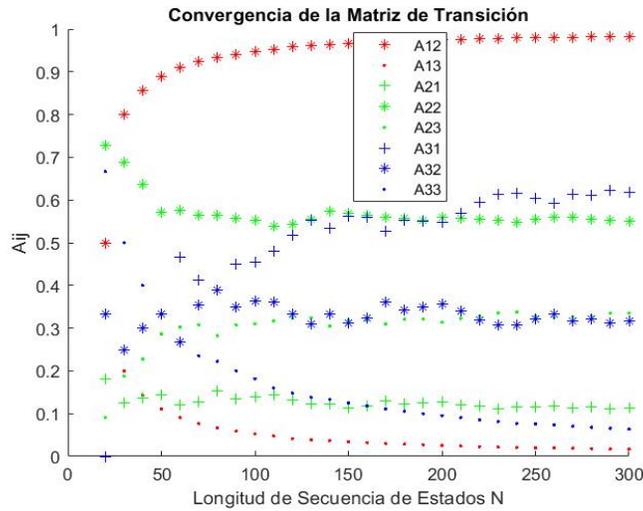


Fig. 4. Convergencia de cada término de la matriz de transición

4.4 Determinación del Desbalance Financiero

Para ésta aplicación se utiliza el Toolbox HMM de MATLAB [6].

4.4.1 Cuenta Bancaria 1069

En el caso de la cuenta 1069 no tenemos ninguna transacción bancaria en la cual se ocasione un balance negativo. Se diseña el siguiente proceso para determinar si existe o no desbalance:

Paso uno: Se determina un número aleatorio, que en las secuencias de observaciones se considera como la observación O_{t+1} que se quiere determinar si es un desbalance o no.

Paso dos: Para entrenar el HMM se calculan las matrices de emisión y transición, se usa la secuencia de observaciones de O_1, \dots, O_t y sus respectivos estados.

```
[MatrizdeTransicion, MatrizdeEmision] = hmmestimate
(Observaciones, Estados);
```

Matriz de transición.

0	0	0	1	0	0
0	0.21052632	0.15789474	0.10526316	0.42105263	0.10526316
0	0	0.08888889	0.33333333	0	0.57777778
0	0.08333333	0.05	0.275	0.4	0.19166667
0.01639344	0.03278689	0.52459016	0.19672131	0.08196721	0.14754098
0	0.03389831	0	0.96610169	0	0

Matriz de emisión.

1	0	0
0.15789474	0.15789474	0.68421053
0	1	0
0.74166667	0.05	0.20833333
0.01639344	0.19672131	0.78688525
1	0	0

Paso tres: Determinar la secuencia de observaciones inicial de tamaño N , O_1, \dots, O_N ,

siendo $O_N = O_t$

Secuencia Observaciones Inicial

2	1	1	3	2	1	1	3	3	2	1	1	3	2	3	1	1	3	2	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Secuencia Estados Inicial

4	5	4	5	3	3	4	5	4	3	5	4	5	3	4	6	4	5	5	6
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Paso cuatro: Determinar la secuencia de estados más probable

A partir de la rutina usada en Matlab (hmmviterbi) se calcula una secuencia de estados con la mayor probabilidad.

EstadosGenerados = hmmviterbi (SecuenciaInicial, MatrizdeTransicion, MatrizdeEmision);

Secuencia de estados más probable obtenida

4	6	4	5	3	6	4	5	5	3	6	4	5	3	4	6	4	5	3	6
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Teniendo esta secuencia de estados generada por la rutina se compara con la secuencia de estados de entrada,

Porcentaje = sum (Estados==EstadosGenerados) /NEJEMPLOS;

Porcentaje obtenido: 0.7000

Paso cinco: Calcular el Logaritmo de la Probabilidad total de la secuencia de estados

Esta se obtiene usando la rutina en MATLAB hmmdecode

[ProEstados, LogSecuencia] = hmmdecode (SecuenciaInicial, MatrizdeTransicion, MatrizdeEmision)

Logaritmo de la probabilidad de la secuencia de estados Inicial: -18.6465

Paso seis: Determinar la secuencia de observaciones final de tamaño N+1 , O_1, \dots, O_{N+1}

, siendo $O_{N+1} = O_{t+1}$ que incluye la observación que se desea determinar si es desbalance financiero

Secuencia Observaciones Final

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Para esta cadena de 21 observaciones se repite los Pasos Cuatro y Cinco para calcular la secuencia de estados más probable, usando hmmviterbi y el logaritmo de la probabilidad usando hmmdecode.

Logaritmo de la probabilidad de la secuencia de estados Final: -19.1147

Paso siete: Se calcula Delta definida como la diferencia de Logaritmo de la probabilidad de la secuencia de estados Final menos Logaritmo de la probabilidad de la secuencia de estados Inicial

Delta: -0.4682

También se calcula la Delta proporcional respecto a Logaritmo de la probabilidad de la secuencia de estados Inicial

Delta proporcional = 0.0251

Del paso tres al siete se realiza para diferentes tamaños de N. En cada una de las corridas se genera un número aleatorio diferente. En la siguiente tabla se reporta el promedio de cinco corridas para cada tamaño de la secuencia de observaciones inicial.

Tabla 2. Comportamiento de la Cuenta bancaria 1069 de la Base de Datos Berka [1], con balance positivo

Longitud	Delta	Delta Proporcional
20	- 0.56176	0.0354
17	- 0.56176	0.04016
14	- 0.56176	0.0544
11	- 0.56176	0.05748
8	- 0.56176	0.0871
5	- 0.56288	0.14836

4.4.2 Cuenta Bancaria 2335

En el caso de la cuenta 2335 encontramos un número considerable de transacciones que generan en algún punto un balance negativo, que después se recupera a positivo sin embargo para efectos del experimento entrenamos el HMM un elemento antes del primer balance negativo.

Paso uno: Encontrar la primera observación donde se genera un desbalance negativo en la cuenta, en las secuencias de observaciones se considera como la observación O_{t+1} .

Paso dos: Para entrenar el HMM se calculan las matrices de emisión y transición, se usa la secuencia de observaciones de O_1, \dots, O_t y sus respectivos estados.

```
[MatrizdeTransicion, MatrizdeEmision] = hmmestimate
(Observaciones, Estados);
```

Matriz de transición.

0	0	0	0	1	0
0	0.11904762	0.0952381	0.23809524	0.35714286	0.19047619
0	0.18181818	0.13636364	0.31818182	0.13636364	0.22727273
0	0.08045977	0.05747126	0.2183908	0.14942529	0.49425287
0	0.2195122	0.09756098	0.18292683	0.45121951	0.04878049
0.0106383	0.07446809	0.0212766	0.38297872	0.13829787	0.37234043

Matriz de emisión.

0	0	1
0.47619048	0.45238095	0.07142857
0.95454545	0.04545455	0
0.71264368	0.10344828	0.18390805
0.75609756	0.09756098	0.14634146
1	0	0

Paso tres: Determinar la secuencia de observaciones inicial de tamaño N , O_1, \dots, O_N ,

siendo $O_N = O_t$

Secuencia Observaciones Inicial

1	1	2	2	1	1	1	1	1	1	1	1	1	2	1	1	3	1	1	1	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Secuencia Estados Inicial

4	3	5	3	3	2	4	6	4	6	5	5	5	5	2	4	4	6	4	6
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Paso cuatro: Determinar la secuencia de estados más probable

A partir de la rutina usada en Matlab (hmmviterbi) se calcula una secuencia de estados con la mayor probabilidad.

EstadosGenerados = hmmviterbi (SecuenciaInicial, MatrizdeTransicion, MatrizdeEmision);

Secuencia de estados más probable obtenida

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Teniendo esta secuencia de estados generada por la rutina se compara con la secuencia de estados de entrada,

Porcentaje = sum (Estados==EstadosGenerados) /NEJEMPLOS;

Porcentaje obtenido: 0.2500

Paso cinco: Calcular el Logaritmo de la Probabilidad total de la secuencia de estados

Esta se obtiene usando la rutina en MATLAB hmmdecode

[ProEstados, LogSecuencia] = hmmdecode (SecuenciaInicial, MatrizdeTransicion, MatrizdeEmision)

Logaritmo de la probabilidad de la secuencia de estados Inicial: -12.5840

Paso seis: Determinar la secuencia de observaciones final de tamaño N+1 , O_1, \dots, O_{N+1}

, siendo $O_{N+1} = O_{t+1}$ que incluye la observación que se desea determinar si es desbalance financiero

Secuencia Observaciones Final

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Para esta cadena de 21 observaciones se repite los Pasos Cuatro y Cinco para calcular la secuencia de estados más probable, usando `hmmviterbi` y el logaritmo de la probabilidad usando `hmmdecode`.

Logaritmo de la probabilidad de la secuencia de estados Final: -14.9128

Paso siete: Se calcula Delta definida como la diferencia de Logaritmo de la probabilidad de la secuencia de estados Final menos Logaritmo de la probabilidad de la secuencia de estados Inicial

Delta: -2.3288

También se calcula la Delta proporcional respecto a Logaritmo de la probabilidad de la secuencia de estados Inicial

Delta proporcional = 0.1851

Del paso tres al siete se realiza para diferentes tamaños de N. En la siguiente tabla se reporta Delta y la Delta proporcional para diferentes tamaños de la secuencia de observación inicial.

Tabla 3. Comportamiento de la Cuenta bancaria 2335 de la Base de Datos Berka [1], con balance negativo

Longitud	Delta	Delta Proporcional
20	- 1.4774	0.1412
17	- 1.4774	0.1726
14	- 1.4774	0.238
11	- 1.4773	0.2767
8	-1.477	0.3033
5	- 1.4739	0.5127

Se observa en la Tabla 2, que cuando no hay desbalance financiero el valor absoluto de Delta es menor que uno y el porcentaje de variación es menor a 10%. Mientras que la Tabla 3 muestra que cuando existe un desbalance financiero, el valor absoluto de la variable Delta es mayor que uno y el porcentaje de variación es mayor a 10%.

5 Conclusiones y trabajos a futuro

Los Modelos Ocultos de Márkov nos permiten modelar la información de las transacciones bancarias de un usuario. Este modelo lo representan las matrices de Transición y Emisión. Se muestra con la base de datos Berka [1], la convergencia de la matriz de transición cuando el tamaño de la secuencia de estados aumenta. También el modelo HMM para una cuenta bancaria, permite determinar si existe un desbalance financiero, comparando dos secuencias de tamaño N y N+1. Cuando no hay desbalance financiero el valor absoluto de Delta es menor que uno y el porcentaje de variación es menor a 10%. Mientras que cuando existe un desbalance financiero, el valor absoluto de la variable Delta es mayor que uno y el porcentaje de variación es mayor a 10%.

Como trabajo futuro se desea aplicar este proceso a una base de datos de tarjetas de crédito para detectar fraude.

Agradecimientos. Este trabajo se realizó en la estancia de Prácticas profesionales en la Facultad de Ciencias de la Computación de la Benemérita Universidad Autónoma de Puebla.

Referencias

1. Base de datos Berka , recuperada de <http://lisp.vse.cz/>, fecha de acceso : marzo de 2019
2. Rabiner, Lawrence R. A tutorial on Hidden MARKov Model and Selected Applications in Speech Recognition. *Proceeding of the IEEE*. Vol. 77 No. 2, pp 257-286 (1989).
3. Pacheco Martínez, M. Redes Neuronales Recurrentes Aplicadas al Reconocimiento de Voz y Traducción Automática de Español a Japonés (Licenciatura). Benemérita Universidad Autónoma de Puebla, (2019).
4. Ángeles Millán, V. Informe de Prácticas Profesionales, Modelos Ocultos de Márkov, (2019).
5. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. Credit Card Fraud Detection Using Hidden Markov Model. *In Dependable and Secure Computing, IEEE Transactions on*, pp. 37-39 (2008).
6. Richard Durbin, Sean R. Eddy, Anders Krogh, Graeme Mitchison. Biological sequence analysis. The Pitt Building. Trumpington Street, Cambridge, United Kingdom: CAMBRIDGE UNIVERSITY PRESS. (1998)

Intercomunicador con Cámara y Conectividad WiFi

Joel Fernando Acevedo Ruiz¹, Aldrin Barreto Flores²,
Salvador E. Ayala Raggi³, Verónica E. Bautista López⁴

^{1,2} Facultad de Ciencias de la Electrónica. Benemérita
Universidad Autónoma de Puebla. Av. San Claudio S/N Puebla,
México.

^{3,4} Facultad de Ciencias Computacionales.
Benemérita Universidad Autónoma de Puebla.
Av. San Claudio S/N Puebla, México.

¹jo_fe_ar@hotmail.com,

²aldrin.barreto@correobuap.mx,

³saraggi@gmail.com, ⁴fccvbalop@gmail.com.

Resumen. El aumento de la inseguridad y delincuencia actual motiva nuevas medidas de cuidado como las que aprovechan el uso de las tecnologías de comunicación a través de internet. Se ha desarrollado un dispositivo de vigilancia capaz de tomar una fotografía al detector movimiento y enviarla a un correo electrónico a través de una conexión WiFi. Se utiliza el nuevo chip ESP32 de Expressif junto con una pantalla OLED de 128*64 pixeles, una cámara o sensor de imagen OV2640 y otros elementos como sensor de movimiento, botones, batería e interruptores. El sistema es capaz de enviar sin problemas una alerta por e-mail, mantener una conexión estable a internet y funcionar autónomamente hasta 8 horas sin superar los \$40.00 USD de costo total por sus componentes. Su pequeño tamaño de 8*3*2.5cm y sus 49g de peso lo hacen portátil y práctico para su uso en cualquier lugar y diversas aplicaciones de vigilancia.

Palabras Clave: Sistemas Embebidos, ESP32, Vigilancia.

1 Introducción

La vigilancia y seguridad son aspectos de gran importancia en el día a día de cualquier persona con la necesidad de proteger o cuidar algún tipo de bien. Su uso se ha visto beneficiado por el desarrollo de la tecnología electrónica y las redes de telecomunicación como el internet, sin embargo, aún existen áreas de oportunidad en el diseño de dispositivos y en su operación e interacción con el usuario.

1.1 Estado del arte

Al mismo tiempo que las cámaras fotográficas comenzaron a integrarse en los teléfonos celulares, aparecieron cada vez más dispositivos enfocados a la visión remota usando distintos canales de radiofrecuencia toda vez que las conexiones WiFi no estaban aún presentes en los hogares y oficinas.

Los primeros esfuerzos en este tipo de desarrollos podrían describirse de forma rápida como pequeñas cámaras empotradas en los portones, como si de una típica mirilla de puerta se tratara, enviando lo que la cámara capturaba a un monitor instalado en el interior de la casa. Si bien, su uso era sencillo y útil, no ofrecía mucho más que una mirilla tradicional a excepción de evitar estar justo detrás de la puerta para observar al visitante.

Por ejemplo, el que se considera el primer sistema de vigilancia por videocámaras en circuito cerrado o CCTV fué diseñado por el ingeniero alemán Walter Bruch para

monitorizar misiles durante la guerra en 1942, pero no fué si no hasta 1998 que se comercializaran de forma popular los sistemas DVR (Digital Video Recorder), actualmente vigentes y muy utilizados en hogares, oficinas, locales comerciales e instituciones de distinta índole.

Más tarde, con el establecimiento de las conexiones a internet, los diseños de estos dispositivos se replantearon surgiendo así las videocámaras IP, primero a través de conexiones por cable ethernet y más recientemente de forma inalámbrica por WiFi.

En el 2013, fue fundada la empresa estadounidense Ring Inc, formalmente registrada como Doorbot, cuyo primer apuesta fué la creación de un nuevo video timbre inteligente. Si bien el desarrollo de su product no gozó de buena salud durante sus primeros años, las mejoras continuaron hasta que en 2017 fue liberada la segunda versión bajo el nombre Ring Doorbell 2, actualmente disponible de forma comercial en tiendas on-line con amplia aceptación entre el público estadounidense.

Otras empresas siguieron el mismo camino para ofrecer sus propios productos con diferencias en diseño y algunas funciones, como las empresas August, Remo y Nest, las tres enfocadas en la domótica y productos inteligentes. De los productos mencionados, e incluyendo el Ring Doorbell 2 se muestra un gráfico comparativo a continuación [1].

Tabla 1. Comparación de características y costo entre timbres inteligentes comerciales.

PRODUCTO	August Doorbell Cam Pro	RemoBell 1 S	Nest Hello	Ring Doorbell 2
Conectividad	Wi-Fi	Wi-Fi	Bluetooth, Wi-Fi	Wi-Fi
Integración con	Amazon Alexa	Amazon Alexa, IFTTT, Google Assistant	Amazon Alexa, IFTTT, Nest	Amazon Alexa, IFTTT, Google Assistant
Angulo de visión	120°	180°	160°	160°
Resolución de video	720p	1,536 by 1,536	1,600 by 1,200	1080p
Resolución de fotografía	720p	1,536 by 1,536	1,600 by 1,200	N/A
Almacenamiento	Cloud	Cloud	Cloud	Cloud
Precio en USD.	\$199.00	\$99.00	\$229.00	\$99.00

Es notable el buen nivel de desarrollo en el que actualmente se encuentran estos dispositivos, cuyo surgimiento vemos a penas hace dos años, en el 2017, sin embargo, su costo es también elevado.

Otro punto interesante, es que en su mayoría, ofrecen un corto periodo de almacenamiento gratuito en la nube, típicamente de un mes, luego, para continuar utilizando el servicio el usuario debe pagar una membresía de hasta \$100.00 USD al año, dependiendo de la zona pues los servidores funcionan principalmente en Estados Unidos y Canadá.

1.2 Áreas de oportunidad en productos comerciales

Existen distintos productos con la capacidad de enviar imagen a distancia a través del internet, algunos de ellos comercialmente populares como los timbres Ring Doorbell 2 [1]

y August Cam Pro, sin embargo, estas y otras opciones, presentan en su mayoría una o varias de las siguientes deficiencias:

- Necesitan estar conectados permanentemente al suministro eléctrico doméstico. En caso de un corte en el suministro el dispositivo deja de funcionar.
- Para acceder a las imágenes que el dispositivo captura, debe utilizarse un servidor de pago.
- Las imágenes son capturadas de forma continua y almacenadas en una unidad de memoria que es llenada rápidamente.
- El dispositivo no cuenta con un sensor de movimiento o de apertura de puerta o ventana.
- El dispositivo es grande y visible, perdiendo discreción.
- No posee la capacidad de alertar al usuario ante un evento específico por correo electrónico o mensajería.
- Alto costo de venta, desde \$99.00 USD, alcanzando un precio de reventa en México desde \$250.00 USD.
- Los usuarios refieren constantes problemas de conexión WiFi que hacen imposible la transmisión de imagen.
- Para usar el servicio de almacenamiento en la nube se requiere pagar una membresía mensual o anual.
- Para utilizar el dispositivo se debe instalar y abrir una aplicación en un teléfono celular. Los usuarios a menudo reportan fallas y lentitud en dichas aplicaciones.

1.3 Conceptualización del nuevo dispositivo.

Pensando en los puntos anteriormente mencionados, se concibe el desarrollo de la propuesta con las siguientes características principales:

- Posibilidad de usar un sensor para activar el funcionamiento, como un sensor de movimiento o un sensor de apertura de puerta o ventana.
- Bajo consumo eléctrico y disposición de batería recargable.
- Envío de la imagen capturada mediante correo electrónico, de forma que quede registrado y almacenado en el buzón de destino.
- Dimensiones pequeñas y peso ligero.
- Portátil.
- Bajo costo.
- Posibilidad de usarse como timbre.
- Posibilidad de usarse como cámara fotográfica de vigilancia activada por movimiento.
- Posibilidad de usarse como cámara fotográfica de emergencia.

2 Desarrollo

En este apartado, se explica acerca de los componentes que conformarán el nuevo dispositivo y características consideradas para el diseño del mismo tanto en el aspecto dimensional como funcional.

2.1 Hardware

Microcontrolador y conexión WiFi. Debe contar principalmente con conectividad WiFi, para ello se consideró en un inicio el chip ESP8266 [2] de Expressif, del cual existe mucha información al respecto y pudo haber sido una buena opción; en su lugar, se decidió trabajar con la nueva y última versión de los chips WiFi de Expressif, el microcontrolador ESP32,

con una mayor velocidad de procesamiento, una memoria RAM y memoria ROM de mayor capacidad, y un consumo de energía mucho menor.

Como desventaja, debido a su reciente liberación comercial, aún no se encuentra finalizada la API por parte del fabricante, sus funciones y en general el código liberado para su uso son básicas o primitivas, y la información al respecto es muy escasa.

Entre muchas de sus características, será de suma utilidad que cuenta con 520kb de memoria RAM, 448kb de memoria ROM, y hasta 16Mb de memoria FLASH, comunicación serial UART, I2C e I2S, opciones de SLEEP en modo ligero con un consumo de 800uA y en modo profundo con un consumo de hasta 4.5uA.



Fig. 1. Microcontrolador ESP32 de Expressif.

Sensor. Principalmente se trabajará sobre la activación ante la presencia de una persona o el movimiento de la misma, para ello se destinará un sensor por infrarrojos tipo PIR de pequeño tamaño, con salida digital y un ángulo de vision de 100 grados y detección de 3 a 5 metros.



Fig. 2. Microsensor de movimiento PIR.

Pantalla. Por su pequeño tamaño, bajo consumo eléctrico, control mediante protocolo I2C y un buen desempeño para mostrar caracteres así como gráficos sencillos, se usará una pantalla de tipo OLED de 128*64 pixeles. Su controlador integrado es el SSD1306.



Fig. 3. Pantalla OLED de 128*64 pixeles controlada por I2C.

Cámara. Para la captura de imágenes, el componente típicamente utilizado en proyectos electrónicos es el modelo OV-7670, una cámara de prestaciones sencillas con una resolución máxima de 640*480 pixeles, es decir, calidad VGA.

En su lugar, utilizaremos una cámara de manufactura más reciente que nos ofrece una resolución de hasta 2 megapíxeles, es decir 1600*1200 píxeles; la cámara OV2640.



Fig. 4. Cámara OV2640 de 2Mp controlada por protocolo I2C.

Alimentación eléctrica. Ya que todos los elementos de hardware seleccionados hasta ahora requieren una alimentación de entre 3.3V a 5V, se aprovecharán las características de una batería recargable de polímero de litio (LiPo) que entrega 3.7V y hasta 1300mAh, pues con esta capacidad mantiene unas dimensiones adecuadas a la vez que varias horas de autonomía de acuerdo al consumo estimado del sistema.

Cuenta con un circuito de protección incorporado para evitar sobrecarga, dimensiones de 9*23*60mm y para cargarse requiere de 4.25V, por lo que podrá alimentar todos los componentes y cargarse mediante conexión USB.



Fig. 5. Batería recargable LiPo de 3.7V y 1300mAh.

Integración de componentes. Con la intención de lograr que el resultado sea pequeño y ligero, en vez de utilizar los componentes en módulos separados que se interconecten, se trabajará sobre una placa de circuito impreso que los contenga, contribuyendo a la

compactación y robustez del proyecto. La compañía LilyGo ha fabricado una tarjeta llamada TTGO T-Camera con los componentes mencionados, con dimensiones de 68*24.9mm.

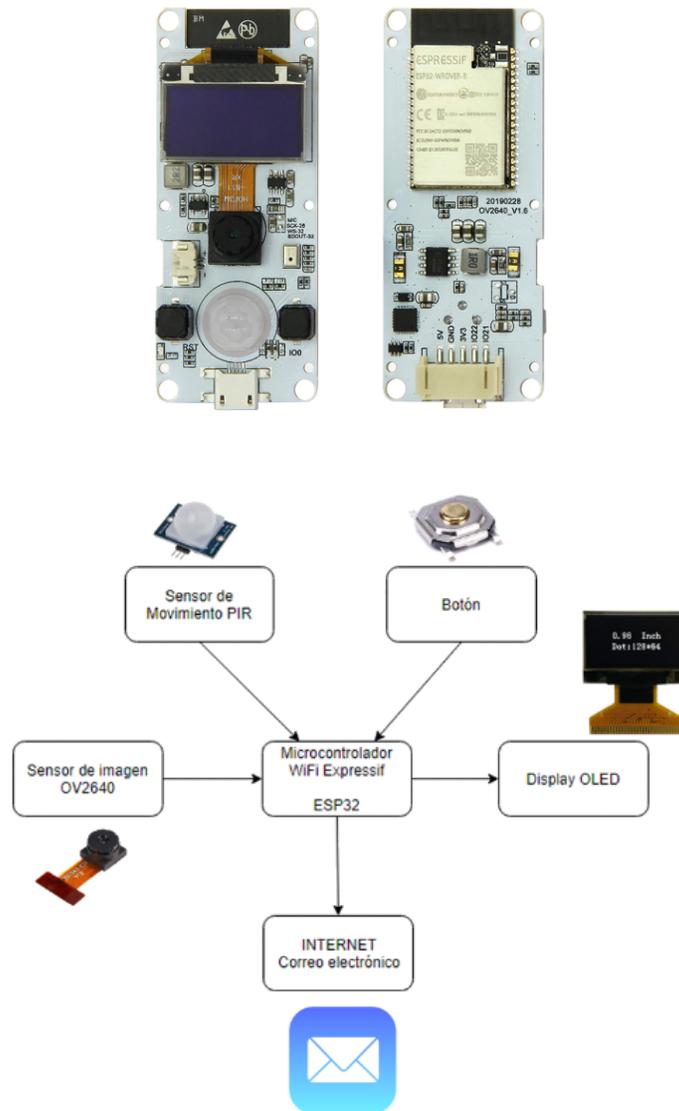


Fig. 6. Implementación de componentes en tarjeta TTGO T-Camera.

El fabricante de la tarjeta, únicamente ha llevado a cabo la integración física de los componentes de hardware, sin embargo, no existen códigos, funciones o documentación para su uso, más que la API en desarrollo del fabricante del microcontrolador Expressif.

Además, la tarjeta cuenta con un conector JST ideal para la conexión con la batería recargable, un botón de reset y un botón que podemos utilizar para cualquier tarea, un puerto USB para la carga de la batería y programación del microcontrolador, así como un puerto de expansion I2C.

2.2 Firmware

El fabricante Expressif ha trabajado en crear una API utilizable desde el IDE Arduino, lo que facilita la programación en lenguaje C++.

La información oficial del microcontrolador ESP32 puede encontrarse en la página web del fabricante [3], donde también se encuentra la referencia a una página web con ligas a hojas de datos y mas información técnica del microcontrolador sobre las *core functions* del SDK de Expressif, así como los distintos repositorios con las API compatibles con el IDE Arduino [4]. En particular, se usará lo referente al modulo ESP32-WROVER.

Tras instalar correctamente dicho SDK en el IDE de Arduino, pueden utilizarse las librerías básicas de la plataforma para el uso de los protocolos UART, I2C, I2S así como para las operaciones matemáticas básicas y el uso y gestión de variables y arreglos en C++ [5].

El microcontrolador se programó para seguir el flujo de instrucciones mostrado en la figura 7.

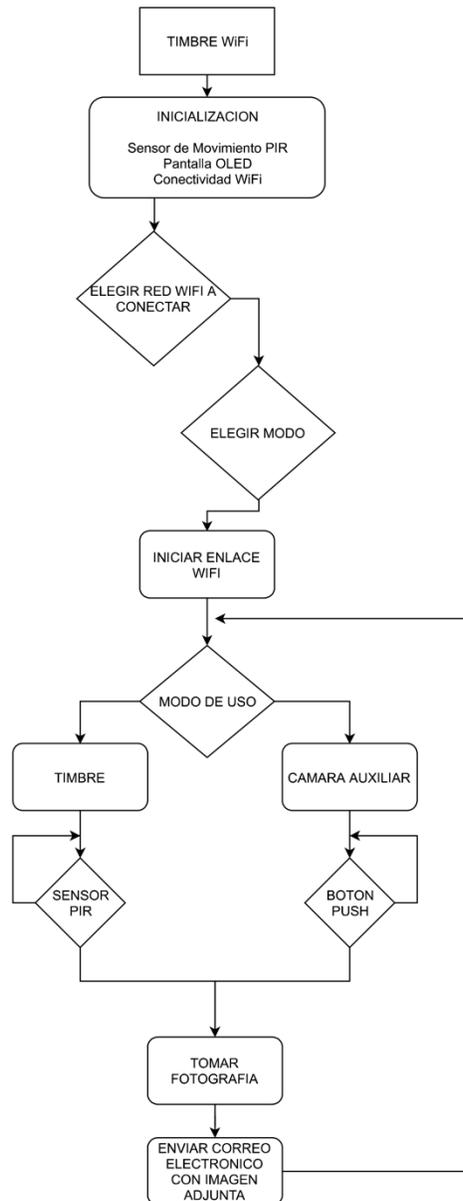


Fig. 7. Funcionamiento del código de programación.

Tras realizar la conexión WiFi, el programa debe enlazarse a un servidor web de correo electrónico, se utilizará el servidor SMTP de Gmail "smtp.gmail.com" en el puerto 465. Primero se realiza la captura de imagen mediante la función `esp_camera_fb_get()` que guardará el cuadro actual en binario en el arreglo de bytes `fb` y luego comienza la conexión por protocolo SMTP. Todas las funciones con prefijo "esp_" pertenecen a la API del fabricante y están descritas y documentadas en la página oficial del mismo.

Fragmento de código 1. Fragmento del código programado para captura de imagen y conexión por protocolo SMTP.

```

fb = esp_camera_fb_get();
fb_len=fb->len;
fr_start = esp_timer_get_time();
if (!fb) {Serial.println("Fallo en cámara");}
else {Serial.println("¡Snap! | Foto tomada! :) |
Cargando...\r\n");
}

Serial.print("Connecting to :");
Serial.println(SMTP_SERVER);

if(!client.connect("smtp.gmail.com", 465)) {
_error = "ERROR EN CONEXION SMTP";
return false;
}

client.println("HELO friend");
if(!AwaitSMTPResponse(client, "250")){
_error = "identification error";
return false;
}

client.println("AUTH LOGIN");
AwaitSMTPResponse(client);

client.println(EMAILBASE64_LOGIN);
AwaitSMTPResponse(client);

client.println(EMAILBASE64_PASSWORD);

```

Posteriormente se envían los datos del mensaje, incluyendo la imagen capturada, la cual también debe enviarse como datos de base 64 de acuerdo a lo definido en el protocolo SMTP [6], para ello, se han creado arreglos temporales de cuatro bytes para agrupar la información de la fotografía, y luego son convertidos mediante el fragmento de código mostrado a continuación.

Fragmento de código 2. Fragmento del código para convertir la imagen capturada en binario a base 64.

```

char b64Chars[] =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
;
void encodeblock( byte *in, byte *out, int len )
{
out[0] = (byte) b64Chars[ (in[0] >> 2) ];
out[1] = (byte) b64Chars[ (in[0] & 0x03) << 4 | (in[1] & 0xf0)
>> 4 ];

```

```
    out[2] = (byte) (len > 1 ? b64Chars[ (in[1] & 0x0f) << 2 |  
    (in[2] & 0xc0) >> 6 ] : '=');  
    out[3] = (byte) (len > 2 ? b64Chars[ (in[2] & 0x3f) ] : '=');  
}
```

Tras enviar el correo electrónico, el dispositivo regresa a su estado inicial a la espera de que el sensor o botón sean activados nuevamente para enviar una nueva alerta y fotografía.

2.3 Interacción con el usuario

El dispositivo cuenta con un botón a disposición del usuario, así como un sensor PIR de movimiento, tras la activación de alguno de ellos (dependiendo el modo de funcionamiento seleccionado) se inicia el envío de la fotografía por correo electrónico, todo el proceso es mostrado mediante distintas pantallas. En las figuras 8 a 11 se muestra el proceso de configuración.



Fig. 8. Selección de resolución de fotografía; VGA o 2MP.



Fig. 9. Selección de modo de funcionamiento como camara auxiliar o como sensor de movimiento.



Fig. 10. Selección de red WiFi a la que se conectará, en este caso, se elige entre dos redes previamente programadas en el código.



Fig. 11. Inicia conexión con la red WiFi seleccionada.

Una vez que se ha configurado el funcionamiento y conectado a la red WiFi elegida, si se eligió el modo de cámara auxiliar, se espera a que el botón disponible sea presionado, la operación en este modo puede observarse en las figuras 12 y 13.



Fig. 12. Pantalla mostrada a la espera de que se presione el botón.



Fig. 13. Si el botón es presionado, se captura la imagen e inicia el proceso de envío.

Por otra parte, el funcionamiento es similar en el modo con sensor de movimiento, con la única diferencia de que la cámara y el envío de la misma son iniciados en caso de que el sensor PIR detecte presencia o cambios en el entorno, mientras que el botón queda deshabilitado. Las pantallas correspondientes se aprecian en las figuras 14 y 15.



Fig. 14. Se revisa constantemente el sensor de movimiento para notar un cambio en el entorno.

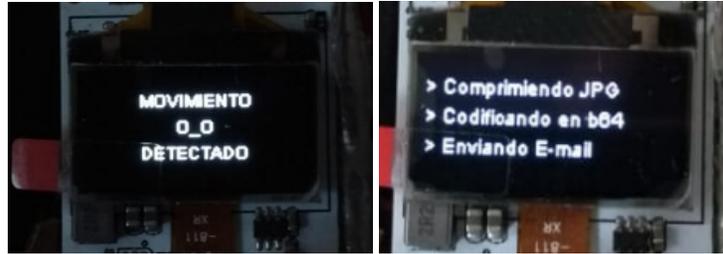


Fig. 15. Si se detecta un movimiento o presencia, se toma una fotografía y se inicia el proceso de envío.

3 Pruebas de funcionamiento

Se probó principalmente con detección de movimiento, se colocó en un sitio estratégico de una habitación aprovechando su pequeño tamaño, y se evaluaron los siguientes aspectos (de forma cualitativa y únicamente como referencia):

- Autonomía – Duración de una carga completa de batería.
- Efectividad al detectar la presencia de alguien en la habitación.
- Rapidez de envío del correo electrónico
- Estabilidad de conexión WiFi.
- Discreción - ¿Cuántas personas notaron el dispositivo y qué opinaron?

3.1 Configuración y pruebas iniciales

Se ha posicionado en una esquina superior de un pasillo, con la intención de que envíe una fotografía cada vez que una persona camine a través de éste.



Fig. 16. Dispositivo montado provisionalmente apuntando a un pasillo durante las pruebas de funcionamiento.

Luego, el dispositivo se configura en modo sensor de movimiento y se activa éste intencionalmente para revisar que la conexión WiFi esté funcionando y se reciba el correo electrónico esperado.

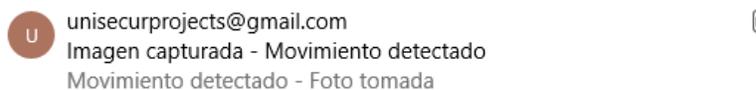


Fig. 17. Correo electrónico recibido tras la activación del sensor de movimiento.

El correo es enviado desde la dirección *unisecurprojects@gmail.com* a un destinatario también programado en el código. Mediante el protocolo SMTP se configura el asunto de los correos generados como: “Imagen capturada - Movimiento detectado” y el texto del mensaje como: “*Movimiento detectado - Foto tomada*”. La imagen llegará adjunta al correo, como se muestra en la figura 17.

Al abrir el correo, puede observarse la imagen adjunta, por ejemplo en la figura 18.



Fig. 18. Fotografía adjunta recibida en el correo electrónico.

Teniendo todo funcionando correctamente, el sistema permaneció bajo observación constante para probar su desempeño.

3.2 Autonomía

Si bien la batería puede mantener funcionando el microcontrolador, la pantalla y el sensor durante un determinado tiempo, el periodo que mantiene funcionando a la conexión WiFi es menor, por lo que se determinó el tiempo operativamente funcional revisando el último correo electrónico recibido con imagen adjunta.

El tiempo de autonomía, desde luego, es afectado por la cantidad de correos electrónicos enviados, es decir, la cantidad de veces que el sensor se activa y por lo tanto, las ocasiones en que una persona pase por el campo de detección.

En la prueba realizada, se registró movimiento y se recibió el correspondiente correo electrónico en un tiempo de 8 horas. Después de éste tiempo, aunque hubieron mas activaciones por parte del sensor, los correos electrónicos no fueron enviados por la disminución de carga en la batería, lo cual afectó la conexión WiFi.

Por lo tanto, se estima la autonomía del dispositivo con una duración promedio de 8 horas de funcionamiento por carga.

3.3 Efectividad de detección

El funcionamiento del sensor tuvo un muy buen desempeño, se recibieron un promedio de dos fotografías por cada persona atravesando el pasillo donde se instaló el dispositivo. Esto es conveniente para contar con distintas imagines que faciliten el reconocimiento de la escena por parte del usuario.

3.4 Rapidez de envío

Se realizaron pruebas utilizando la calidad de fotografía VGA así como UXGA (2MP), pues el tiempo que demora en enviarse el correo electrónico se ve principalmente afectado por el tamaño de archivo de la imagen adjunta.

Tabla 2. Tiempos aproximados de envío de correo electrónico con fotografía adjunta.

Resolución	Tiempo
VGA – 640*480	10 segundos
UXGA – 2MP	30 segundos

3.5 Estabilidad de conexión WiFi

Se observó el funcionamiento durante cada activación del sensor para vigilar la recepción del correo electrónico correspondiente. No se notaron pérdidas de conexión en ningún momento. La fuente de red WiFi se encontraba a una distancia de 20 metros en línea recta con obstáculos como las paredes con un grosor no mayor de 15cm.

3.6 Discreción, dimensiones y peso

Contando con un peso de solo 49g y dimensiones de 8*3*2.5cm resulta en un objeto muy ligero y compacto, el cual puede colocarse prácticamente en cualquier sitio sin dificultad. Puede ser utilizado como un objeto fijo, o bien como un dispositivo portátil.

Adicionalmente, solo dos de las seis personas que asistieron las pruebas realizadas notaron la presencia del dispositivo, coincidiendo ambas en que puede pasar desapercibido y ha sido necesario poner mayor atención para descubrirlo.

3.7 Fotografía

La máxima resolución con que cuenta la cámara utilizada es con calidad de imagen UXGA, es decir de hasta 2MP o 1600*1200 pixeles. Como es sabido, la calidad de la imagen y la utilidad de la misma, no se define únicamente por la resolución o cantidad de pixeles del sensor de imagen, si no que también son de importancia otros factores como la sensibilidad a la luz y la velocidad de obturación.

Los resultados arrojaron que en condiciones de muy poca o nula cantidad de luz, la imagen recibida es de poca utilidad pues es prácticamente negra en su totalidad al no disponerse de un modo de visión nocturna.

Por otro lado, teniendo al menos una fuente de iluminación cercana como una lámpara de al menos 20W, la situación es distinta y la escena es visible en la fotografía adjunta, por ejemplo, la figura 19.



Fig. 19. Fotografía tomada en condiciones de poca luz.

Cabe notar que, con una mayor iluminación o incluso durante el día con la luz natural, las fotografías son capturadas con mucha mayor nitidez y calidad, como en la figura 20.



Fig. 20. Fotografía tomada con buena iluminación en el día.

Respecto a la velocidad de obturación el funcionamiento fue también satisfactorio, capturando buenas imágenes incluso de objetos en movimiento.



Fig. 21. Distintas fotografías capturadas de personas en movimiento.

4 Trabajos a futuro

Continuando con el desarrollo de la propuesta, resultaría útil analizar y controlar la frecuencia con la que el sensor de movimiento es activado por una misma persona en movimiento, para evitar enviar imágenes repetitivas pero sin perder eventos de importancia como la entrada y salida de una persona a una habitación u oficina, por ejemplo.

Aprovechando sus pequeñas dimensiones y peso, para volverlo completamente portátil se añadirá conexión GPRS mediante la red de telefonía celular, contando además con funciones como llamadas telefónicas y envío de mensajes de texto.

También se considera agregar iluminación infrarroja como un apoyo para dar visión nocturna a la cámara y solucionar el problema de las fotografías con bajas condiciones de iluminación.

Finalmente, se contempla dotarlo de capacidades para el envío de información a servidores en la nube aprovechando servicios IoT junto con localización GPS, para convertirlo en un dispositivo de seguridad o rastreador de posición, aumentando su campo de aplicaciones para su utilidad en seguridad familiar, cuidado de mascotas, así como seguridad empresarial para el cuidado de vehículos u otro tipo de bienes.

5 Conclusiones

Se cumplieron los principales objetivos acerca de su tamaño y sus funciones, manteniendo una conexión WiFi estable que alertara a distancia al usuario mediante correos electrónicos.

El costo en componentes del dispositivo no supera los \$40.00 USD, en comparación con otros productos comerciales con un costo de hasta \$200.00 USD, convirtiéndolo en una buena opción para su desarrollo como un producto comercial más accesible.

La integración de un sensor de movimiento junto con la cámara fotográfica crea una herramienta útil para aplicaciones de vigilancia, demostrando ser efectiva al enviar la alerta a distancia a través de internet.

Si bien, su funcionamiento está limitado a la cobertura de una red WiFi, como se mencionó en el apartado cuatro “Trabajos a futuro”, la implementación con la red de telefonía celular resolvería éste inconveniente, haciéndolo completamente portátil y con menor posibilidad de falla ante la pérdida de conexión WiFi o un fallo en la alimentación eléctrica.

Referencias

1. Ring Products. (2019). <https://ring.com/videodoorbells>. Accedido el 2 de Junio de de 2019.
2. ESP8266 based implementation of wireless sensor network with Linux based web-server - IEEE Conference Publication. <https://ieeexplore.ieee.org/abstract/document/7570919>. Accedido el 24 de Enero de 2019.
3. ESP32 | Espressif Systems. (2019). <https://www.espressif.com/en/products/hardware/esp32>. Accedido el 10 de Febrero de 2019.
4. The Internet of Things with ESP32. (2019). <http://esp32.net>. Accedido el 10 de Febrero de 2019.
5. Deitel Harvey; Deitel Paul: Cómo programar en C++. Pearson Prentice Hall 4ta. Ed. 2003.
6. RFC 3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security. <https://tools.ietf.org/html/rfc3207?u=2e9c41d5>. Accedido el 10 de Febrero de 2019.

Solución al Problema de la Programación de Producción - Inventario Usando Código LINGO

Rogelio González Velázquez, María Beatriz Bernabé Loranca, Abraham Sánchez López,
Adriana Méndez Montero

¹ Fac. de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla
Ave. San Claudio y 14 sur, edificio 104 D, Col. San Manuel, Ciudad Universitaria,
Puebla, Pue., México, C. P. 72570

¹{rogelio.gzzvzz, beatriz.bernabe}@gmail.com, ¹yareh_91@hotmail.com, ¹abraham.sanchez@correo.buap.mx

Resumen. En este artículo se presenta la solución a un problema clásico de la investigación de operaciones, el problema de la programación de la producción-inventario (PPI) por medio de un modelo de programación matemática en particular de programación lineal. Se muestra el modelo matemático genérico y se plantea un caso de estudio del cual se obtiene la solución usando código genérico del software de optimización LINGO. El objetivo de este trabajo es el diseño de un código genérico que permita resolver un conjunto de instancias del PPI sólo cambiando los datos. La importancia de implementar un código en el lenguaje LINGO radica en su poder para el manejo de la memoria y la velocidad de cómputo. Se muestran los resultados de la solución del caso de estudio.

Palabras Clave: Modelo de Programación Matemática, Producción, Inventario, Código LINGO.

1 Introducción

Existe una gran variedad de herramientas de tecnologías de información que permiten incrementar la probabilidad de tomar mejores decisiones en cualquier organización, en particular una de estas es la investigación de operaciones (I de O), cuya definición dada en Prawda [1]

‘La investigación de operaciones es la aplicación, por grupos interdisciplinarios, del método científico a problemas relacionados con el control de las organizaciones o sistemas a fin de que se produzcan soluciones que mejor sirvan a los objetivos de la organización.’

En particular la programación lineal (PL) es una herramienta de I de O, para resolver problemas en distintos ámbitos que integran una organización como pueden ser producción, inventario, transporte, asignación, mezclas, asignación de presupuestos entre otras como se menciona en Liberman [2] de la manera siguiente, la PL utiliza la modelación matemática para describir el problema. La palabra lineal significa que todas las funciones matemáticas del modelo deben ser funciones lineales es decir de grado uno y la palabra programación en esencia es sinónimo de planeación. Es decir que la PL determina la mejor planeación de operaciones producción-inventario para la optimización de recursos escasos entre todas las alternativas factibles.

Una simplificación del modelo general de del problema de PL se puede escribir como en Taha [3] y de la manera siguiente: Sean x_1, x_2, \dots, x_n , n variables de decisión, sean c_1, c_2, \dots, c_n los costos asociados con las variables de decisión, sea $(a_{ij}) \forall i = 1, 2, \dots, m, j = 1, 2, \dots, n$ una matriz de tamaño $m \times n$ llamada de coeficiente de tecnología y finalmente sean b_1, b_2, \dots, b_m los recursos escasos, entonces las

componentes son primero la función objetivo $z = \sum_{j=1}^n c_j x_j$ que es la función lineal que representa dos casos la utilidad o los costos por lo cual hay que *maximizar* en el primer caso y *minimizar* en el segundo caso, luego las restricciones que son un conjunto de inecuaciones lineales de cualquier tipo o ecuaciones lineales que son representadas en forma matricial a lo que antecede las palabras *sujeto a* $(a_{ij}) \begin{matrix} \leq \\ \geq \end{matrix} b_i \quad \forall i = 1, 2, \dots, m$, y finalmente las restricciones de no negatividad $x_j \geq 0$.

El plan agregado de operaciones de la producción-inventario se elabora con el fin de determinar los índices de producción por grupo de productos. En la Fig. 1 muestra un esquema de los requerimientos internos de una organización para la planeación de la producción-inventario. El propósito principal según Jacobs [4] del plan de la producción es especificar la combinación óptima de índice de producción, nivel de la fuerza de trabajo e inventario a la mano. El índice de producción se refiere al número de unidades terminadas por unidad de tiempo (por hora o por día).

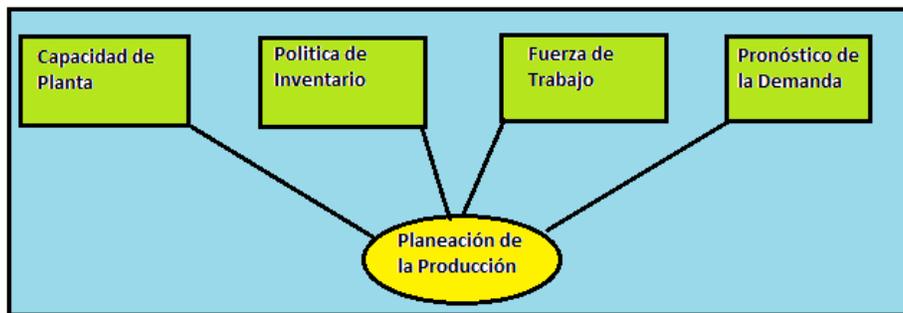


Fig. 2. El esquema muestra la dependencia de la programación de la producción de entidades internas de cualquier organización.

El nivel de la fuerza de trabajo es el número de trabajadores necesario para la producción (producción = índice de producción \times nivel de la fuerza de trabajo). El inventario a la mano es el inventario no utilizado que quedó del periodo anterior y es necesario un buen pronóstico de la demanda.

El planteamiento general del problema de la planeación de la producción-inventario se modela de la manera siguiente: dado el pronóstico de la demanda para cada periodo j en el horizonte de la planeación que abarca n periodos, el objetivo es determinar el nivel de producción, el nivel de inventario y el nivel de la fuerza de trabajo para los periodos $j = 1, 2, \dots, n$ tal que se minimicen los costos relevantes en el horizonte de planeación.

En [5] se desarrolla un modelo teórico de control óptimo, a casos de inventarios determinísticos y dinámicos, propone el nivel de inventario como variable de estado y el nivel de producción como variable de control, en sus resultados reporta información de cuánto producir y cuánto mantener en el inventario. Se realiza la búsqueda de la solución de este caso aplicando el cálculo de variaciones y en su estado del arte muestra antecedentes del PPI desde 2002 hasta 2013. Existen en la literatura otras variante y formas de análisis del PPI como en [6] se estudia el problema del inventario de producción de minimizar el valor actual descontado esperado del control de costos de producción en sistemas de fabricación con demanda estocástica degenerada y adicionalmente desarrolla el modelo óptimo de control de la producción del inventario derivando la dinámica de la

relación inventario-demanda que evoluciona de acuerdo con una ecuación diferencial estocástica

Este artículo está desarrollado de la siguiente forma: en la sección 2 se describe el modelo matemático del PPI, en la sección 3 metodología de la implementación de las palabras reservadas de código LINGO, en la sección 4 se presenta un caso de estudio, el código y resultados y finalmente en la sección 5 se presentan las conclusiones y trabajo futuro.

2 Modelo Matemático

En esta sección se presenta el modelo matemático del problema de la programación de la producción e inventario en su forma genérica para m artículos, definiendo las variables y los parámetros de la siguiente manera: capacidad de producción, costos de producción, costos de inventario, capacidad de almacén y demanda.

El problema consiste en programar la producción e inventario de un conjunto de artículos, en donde cada artículo tiene una demanda por periodo, así mismo se tiene restricciones de capacidad de producción y de almacén. El objetivo es encontrar un programa de producción inventario tal que minimice los costos de producción y de inventario.

Variables y parámetros

x_{ij} = Cantidad de artículos i a producir en el periodo j ; $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

y_{ij} = Cantidad de artículos i en inventario en el periodo j ; $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

d_{ij} = Demanda del artículo i en el periodo j ; $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

p_{ij} = Producción del artículo i a producir en el periodo j ; $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

c_{ij} = Costo de producir el artículo i a producir en el periodo j ; $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

h_{ij} = costo de inventario del artículo i a producir en el periodo j ; $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$.

s_i = espacio físico del artículo i ; $i = 1, 2, \dots, n$;

E = espacio físico disponible de inventario.

$$\text{Minimizar } z = \sum_{j=1}^m \sum_{i=1}^n c_{ij} x_{ij} + \sum_{j=1}^m \sum_{i=1}^n h_{ij} y_{ij} \quad (1)$$

Sujeto a

$$y_{ij} = y_{i,j-1} + x_{ij} - d_{ij} \quad , \quad \forall i = 1, \dots, n; j = 1, \dots, m. \quad (2)$$

$$\sum_{j=1}^m \sum_{i=1}^n x_{ij} \leq p_{ij}, \forall i = 1, \dots, n; j = 1, \dots, m. \quad (3)$$

$$\sum_{i=1}^n s_i y_{ij} \geq E, \forall i = 1, \dots, n. \quad (4)$$

$$\forall x_{ij} \geq 0, y_{ij} \geq 0, y_{i0} \geq 0 \quad (5)$$

La ecuación (1) representa la función objetivo la cual debe ser minimizada, siguen las restricciones, la (2) es la restricción del inventario actual que dice que el inventario actual es la suma del inventario del mes anterior más la producción actual menos la venta de este mes, la (3) son de la demanda que dice que las sumas de los artículos i producidos en el mes j debe ser mayor que la demanda del mes j , la (3) representa la capacidad instalada de producción, la (4) son las restricciones de espacio asignado para acomodar el inventario y finalmente las restricciones de no negatividad y las del inventario inicial.

3 Caso de análisis

En esta sección se describe un problema para plantear de [7] que dice “Una organización desea planear la producción de 2 artículos con demanda estacional alrededor de un periodo de 12 meses. La demanda mensual del artículo 1 es de 100,000 unidades durante los meses de octubre, noviembre y diciembre; 10,000 unidades durante los meses de enero, febrero, marzo y abril; y 30,000 unidades durante el resto de los meses. La demanda del artículo 2 es de 50,000 durante los meses de octubre hasta febrero y 15,000 durante el resto de los demás meses. Suponga que la unidad del costo del producto del artículo 1 y 2 es \$5.00 y \$8.00 respectivamente, siempre que estos sean fabricados antes de junio. Después de junio, los costos por unidad son reducidos a \$4.50 y \$7.00 por que la instalación son un sistema mejorado de fabricación. El total de unidades de los artículos 1 y 2 pueden ser fabricados durante cualquier mes en particular y que no exceda 120,000 para enero hasta septiembre, y 150,000 para octubre hasta diciembre. Más allá, cada unidad del artículo 1 ocupa 2 pies cúbicos, y cada unidad del artículo 2 ocupa 4 pies cúbicos en el inventario. Suponga que el máximo espacio en el inventario de alojamiento de estos artículos es de 150,000 pies cúbicos y manteniendo el costo por pie cubico durante cualquier mes es de \$0.10. Formule la programación de producción del problema así que el costo total de producción y el costo de inventario sean minimizados”.

Sean los doce meses a partir del mes octubre, noviembre, diciembre, enero, febrero, marzo, abril, mayo, junio, julio, agosto y septiembre, equivalentes a la numeración $j = 1, 2, \dots, 12$

x_{1j} = cantidad de producto 1 a producir en el mes j .

x_{2j} = cantidad de producto 2 a producir en el mes j .

y_{1j} = cantidad de 1 producto en inventario en el mes j .

y_{2j} = cantidad de producto 2 en inventario en el mes j .

d_{1j} = demanda del producto 1 en inventario en el mes j .

d_{2j} = cantidad de producto 2 en inventario en el mes j .

El modelo para este caso es el siguiente:

$$\text{Minimizar } Z = \sum_{j=1}^8 5x_{1j} + \sum_{j=1}^8 8x_{2j} + \sum_{j=9}^{12} 4.5x_{1j} + \sum_{j=9}^{12} 7x_{2j} + \sum_{j=1}^{12} 0.2y_{1j} + \sum_{j=1}^{12} 0.4y_{2j} \quad (7)$$

Sujeto a

$$y_{1j} = y_{1,j-1} + x_{1j} - d_{1j} \quad \forall j = 1, \dots, 12, \quad (8)$$

$$y_{2j} = y_{2,j-1} + x_{2j} - d_{2j} \quad \forall j = 1, \dots, 12, \quad (9)$$

$$x_{1j} + x_{2j} \leq 120,000 \quad \forall j = 1, \dots, 9 \quad (10)$$

$$x_{1j} + x_{2j} \leq 150,000 \quad \forall j = 10, 11, 12 \quad (11)$$

$$2y_{1j} + 4y_{2j} \leq 150,000 \quad \forall j = 1, \dots, 12 \quad (12)$$

$$\forall x_{ij} \geq 0, y_{ij} \geq 0, y_{i0} \geq 0 \quad (13)$$

En este caso de estudio el modelo de programación lineal está formado por la minimización de la función objetivo (7) que está seccionada en seis partes cuatro para los costos de producción y dos para los costos de inventario, que está sujeta a las restricciones de desigualdad (10) y (11) que modelan la capacidad de producción en las partes del horizonte de planeación incluyendo las restricciones de desigualdad (11) que modelan el de espacio en almacén y en ambos casos están separadas por el producto 1 y producto 2 .

4 Metodología

Los planteamientos del modelo matemático y el caso de estudio son esencialmente los mismos, pero con las variantes del caso de estudio debido a que hay variabilidad en algunos parámetros en los costos, en la demanda estacional, así como en la capacidad de producción.

La solución se obtuvo por medio de un código de programación en el software de optimización Lingo 17.0 usando las librerías propias del lenguaje para la estructura de datos obtenidas del manual de usuario [8] como son:

SETS... ENDSETS = se utiliza para definir tipos de datos.

DATA... ENDDATA= se utiliza para introducir los datos de set...endsets.

@SUM=representa la sumatoria de variables o parámetros que dependen de un índice que se mueve a lo largo de la sumatoria.

@FOR= es un generador de restricciones que describe un tipo específico de restricciones.

El Algoritmo 1 muestra la implementación de la solución del PPI en código LINGO usando la estructura de datos para simplificar las líneas de código y permita modificaciones sencillas cuando los datos cambien en forma y tamaño, esta es una ventaja de utilizar la programación en código LINGO.

Algoritmo 1. Código LINGO para resolver el PPI.

```

MODEL :
SETS :
    Y/0..12/: Y1,Y2,X1,X2,d1, d2, X;
ENDSETS
DATA :
    d1 =" ";
    d2 =" ";
    X=" ";
ENDDATA
MIN=
0.2*@SUM(Y(I)|I #GE# 2:Y1(I))+ 0.4*@SUM(Y(I)|I #GE# 2:Y2(I))+
5*@SUM(Y(I)| I #GE# 2 #AND# I #LT# 10:X1(I))+
8*@SUM(Y(I)|I #GE# 2 #AND# I #LT# 10:X2(I))+ 4.5*@SUM(Y(I)|I
#GT# 9:X1(I))+ 7*@SUM(Y(I)|I #GT# 9:X2(I));
@FOR(Y(I)|I #LT# 13: Y1(I+1) = Y1(I) + X1(I+1) - d1(I+1));
@FOR(Y(I)|I #LT# 13: Y2(I+1) = Y2(I) + X2(I+1) - d2(I+1));
@FOR(Y(I):X1(I)+X2(I) <= X(I));
@FOR(Y(I)|I #EQ# 1:Y1(I)=0);
@FOR(Y(I)|I #EQ# 1:Y2(I)=0);
END

```

5 Resultados

En este apartado se muestran los resultados del caso de análisis para el PPI en un horizonte de planeación de un año en periodos mensuales, en la primera columna de la Tabla 1 esta aparece el nombre del mes del horizonte de planeación, en la segunda y tercera columna se muestran la planeación de la producción mensual del producto 1 y producto 2 durante el cada mes del año, finalmente en la tercera y cuarta columna se muestran el inventario mensual durante cada mes del año.

Tabla 2. La tabla muestra los resultados de un PPI del caso de analisis para un horizonte de planeación de 12 meses con periodos mensuales.

Periodo	Producción		Inventario	
	Producto 1	Producto2	Producto 1	Producto2
Octubre	100000	50000	0	0
Noviembre	100000	50000	0	0
Diciembre	100000	50000	0	0
Enero	10000	50000	0	0
Febrero	10000	50000	0	0
Marzo	10000	15000	0	0
Abril	10000	15000	0	0
Mayo	30000	15000	0	0
Junio	30000	15000	0	0
Julio	30000	15000	0	0
Agosto	30000	15000	0	0
Septiembre	30000	15000	0	0

6 Conclusiones y trabajos futuros

En este artículo se obtuvo la solución a un problema clásico de la investigación de operaciones, el problema PPI por medio de un modelo de programación matemática. Se planteó el modelo matemático genérico y se modelo un caso de análisis del cual se obtiene la solución usando código genérico del software de optimización LINGO. Se diseñó de un código genérico que permitió resolver un caso de análisis del PPI. La importancia de implementar un código en el lenguaje LINGO radica en su flexibilidad para resolver problemas de muchas variables, restricciones y parámetros, por ejemplo, en este caso el modelo tienes 48 restricciones sin embargo se pudo resolver con solo cuatro líneas de código. Como trabajo futuro se plantea diseñar instancias de mayor tamaño e incluso diversidad de demandas y capacidades de planta y espacio de almacén.

Referencias

1. Prawda J.; Métodos y Modelos de Investigación de Operaciones Vol 1 Modelos Determinísticos. Noriega (Eds): LIMUSA, pp. 7-9 (1990).
2. Hillier F., Liberman G.; Introducción a la Investigación de operaciones. 9ª edición Mc Graw Hill, pp. 21-23 (2010)
3. Taha H.; Investigación de operaciones. 9ª Edición: Pearson, pp. 13-24 (2012)
4. Jacobs F., Aquilano N.; Administración de Operaciones Producción y Cadena de Suministro. 10ª Edición, Mc Graw Hill, pp 515-518 (2009)
5. Cepeda O., Jiménez L.: Modelo de control óptimo para el sistema Producción Inventarios. *Ingeniería Industrial Actualidad y Nuevas Tendencias*, Vol. V, No. 16, pp. 35-44 (2016)
6. Baten, M., Kamil, A.: Production Control in Stochastic Manufacturing Systems with Degenerate Demand. *East Asian Journal on Applied Mathematics*, Vol. 1, No. 1, pp. 89-96 (2011)
7. Bazaraa M.; Linear Programming and Network Flows. 2ª Ed, LIMUSA, pp 55-60 (2005)
8. LINGO, Modeling language and optimizer. 5a Ed, LINDO system INC, pp 66-74 (2003)

Sistema multi sensor para medición, procesamiento y envío de parámetros ambientales en tiempo real

María del Carmen Santiago Díaz¹, Gustavo Trinidad Rubín Linares¹,
Hermes Moreno Álvarez², Antonio Eduardo Álvarez Nuñez¹

¹Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla
14 sur y av. San Claudio, C.U. San Manuel, Puebla, México

²Facultad de Ingeniería, Universidad Autónoma de Chihuahua
{marycarmen.santiago, gustavo.rubin}@correo.buap.mx,
hm1713a@gmail.com, eduard-alvarez@live.com.mx

Resumen. Se propone el diseño y construcción de una plataforma aérea estabilizada en XYZ mediante un conjunto de sensores infrarrojos, ultrasónicos, de temperatura, humedad y acelerómetro, para controlar tres motores de cd. El sistema de control se implementa en un dispositivo reconfigurable FPGA (field programmable gate array) DE2-70 de Altera, lo que nos permite probar algoritmos de control para estabilizar la plataforma y comunicaciones inalámbricas para llevar a cabo trabajo cooperativo con otros sistemas por ejemplo terrestres, así como la capacidad de procesamiento de patrones.

Palabras Clave: Reconfigurable, algoritmos de control, procesamiento..

1 Introducción

En los últimos años la robótica y el control automático han adquirido gran impulso debido a su aplicación en un sin fin de procesos en las grandes empresas optimizando la producción mediante la aceleración de procesos que suelen ser repetitivos y que tienden a fatigar a un empleado. En esta vertiente se han desarrollado sistemas de control cada vez mas autónomos para aplicaciones muy concretas, pero este mismo quehacer ha hecho que se busque desarrollar áreas cada vez mas específicas como robótica móvil, reconocimiento de patrones, visión artificial, robótica cooperativa, etc.[1,2,3].

En este trabajo diseñamos un sistema que consta de diversos sensores para colocarse en un sistema robótico terrestre o aéreo el cual enviará la información de estos en tiempo real a una central de procesamiento.

1.1 Diseño de la plataforma

Ya que uno de los objetivos de este trabajo es el control y estabilización de una plataforma, utilizamos el material mas accesible, pues sólo queremos mantenerla estable y el único peso de interés es el de los motores y sensores. Por ello seleccionamos unicele como material ya que soporta muy bien el peso que tendremos.

La plataforma tiene en la parte baja tres hélices cada una con un motor de corriente directa, por lo que se requiere para cada motor un sistema de control de potencia. Debido a que es posible encontrar diferencias en la potencia de cada motor e incluso en el rendimiento, colocamos en cada motor sensores de temperatura para monitorear si se calienta demasiado alguno de los motores, y sensores de velocidad para analizar el rendimiento.

Ya que la plataforma debe alcanzar una determinada altura utilizamos un sensor de ultrasonido para este fin y un acelerómetro para determinar la inclinación de la plataforma y corregirla.

La figura 1 muestra el diagrama a bloques requerido para que la plataforma alcance determinada altura y se estabilice.

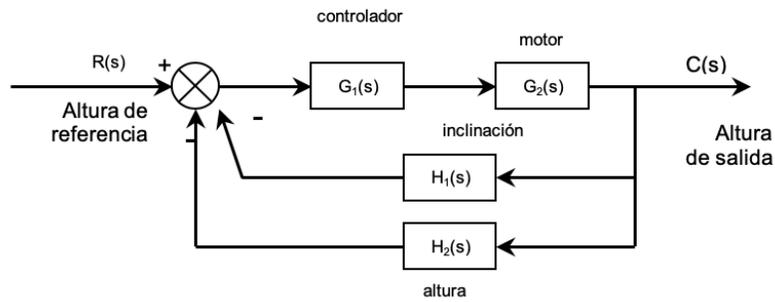


Fig. 1. Diagrama a bloques de la plataforma aerea.

Todo el sistema de control se implementa en una tarjeta de desarrollo DE2-70 de Altera, para lo cual las señales analógicas deben ser llevadas a digitales así como un acoplamiento CMOS-TTL y TTL-CMOS para el caso de la lectura de información en éste caso de los diferentes sensores analógicos[4].

2. Metodología

Para controlar la velocidad de los motores de cd llevamos a cabo la implementación del diagrama de bloques que se muestra en la figura 2 para cada motor, donde $R(s)$ es la señal de referencia de velocidad fijada por el sistema de control de la plataforma para alcanzar determinada altura o bien corregir la inclinación, $G_1(s)$ es el sistema de control de velocidad del motor de cd $G_2(s)$ y $H(s)$ es la función de transferencia del sensor, que en éste caso es un sistema emisor-receptor en infrarrojo.

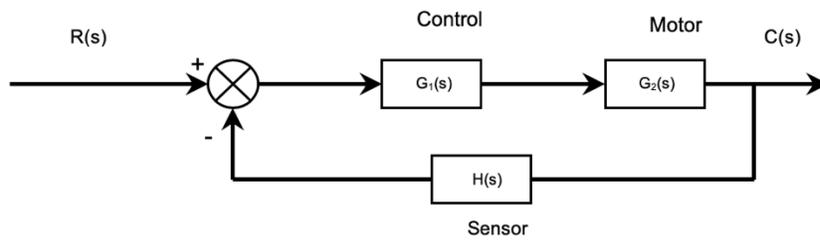


Fig. 2. Diagrama a bloques del control de potencia para cada motor.

Para determinar la función de transferencia de los motores se llevó a cabo el siguiente arreglo, que consta de un encoder y un convertidor frecuencia a voltaje LM2907, así como un BJT como se muestra:

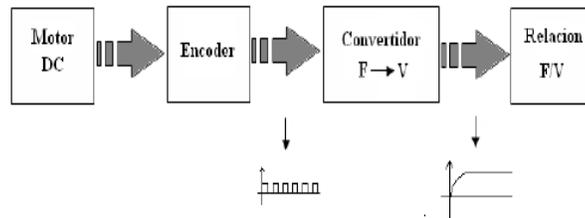


Fig. 3. Esquema para determinar la función de transferencia de los motores.

El control de velocidad se llevó a cabo con un modulador por anchura de pulso ó PWM (pulse-width modulation) mediante un driver L293B para poder suministrar hasta 1 ampere, de esta forma se tiene un control de la velocidad del motor variando el ciclo de trabajo (duty cycle) de una señal periódica en cualquier rango de velocidades, como se muestra en la figura 4[5,6].

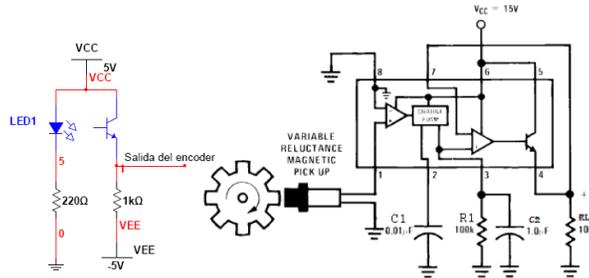


Fig. 4. Arreglo del encoder y el convertidor F/V.

Para medir la temperatura utilizamos los sensores LM35, ya que prácticamente no requieren de acondicionamiento de la señal y brindan una conversión lineal así como bajo ruido, como estos sensores son analógicos se pueden tomar dos alternativas, una es utilizar convertidores analógicos a digital ADC para cada uno y poder procesar la señal digital y otra es utilizar los convertidores de la tarjeta DE2-70, en cualquiera de los dos casos se implementa un sistema de conmutación de las diferentes señales a convertir para utilizar un solo convertidor, ya que las constantes de tiempo de temperatura son relativamente lentas en comparación con las de velocidades se pueden ir leyendo a intervalos fijos no tan pequeños.

Los sensores de velocidad se implementaron con pares emisor receptor en infrarrojo ajustados y decodificadores de disco los cuales nos entregan una señal digital.

1.2 Control de la inclinación y la altura de la plataforma

Para determinar la inclinación de la plataforma se requiere medir mediante un acelerómetro que componente requiere ser ajustada, para este fin utilizamos un acelerómetro ADXL150 de Analog Device, el cual cuenta con dos pines de interés para medir la inclinación en los ejes X y Y.

La información de la altura la realizamos con un sensor ultrasónico SRF05, el cual entrega una señal digital por lo que no requiere mucha instrumentación para acoplarla a la tarjeta DE2-70[7].

1.3 Diseño del sistema de control

Para poder elevar la plataforma a una determinada altura lo primero es garantizar que no se incline a fin de que se vuelva inestable y se pueda voltear, para éste fin aumentamos la velocidad de los motores lentamente verificando que la temperatura máxima de cada uno de ellos sea de 40°C, y midiendo la velocidad de cada uno. En ésta primera etapa suministramos la altura de referencia en pequeños escalones o intervalos discretos de 1cm cada segundo, a fin de poder controlar el sistema, hemos realizado mediciones con una pendiente mayor pero no hemos podido aislar el sistema ante perturbaciones, lo que ha hecho que el sistema se vuelva inestable y no podamos controlar la inclinación.

1.4 Análisis del sistema

Debido a que las constantes de tiempo de los sensores son lo suficientemente pequeñas como para tomarse en cuenta (comparadas con las variables que miden como altura y

velocidad), en los diagramas a bloques de las figuras 1 y 2, los lazos de retroalimentación son de ganancia unitaria.

El diagrama a bloques del control de velocidad de la figura 2 queda entonces como

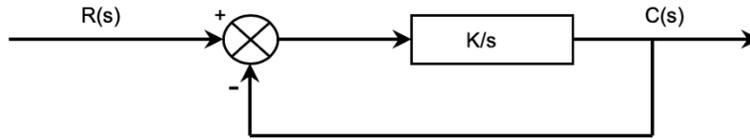


Fig. 5. Diagrama a bloques de control de potencia

Donde la función de transferencia en la trayectoria directa se determina en base a la función escalón aplicada al motor de d.c, con ésta información, tenemos que si aplicamos el teorema del valor final entonces el error en estado estacionario tiene la forma siguiente [8,9,10].

$$e_{ss} = \lim_{s \rightarrow 0} sE(s) = 0 \tag{1}$$

Esto último significa que cuando demos la velocidad de referencia el sistema alcanzará esa velocidad en teóricamente en infinito, pero como las constantes de tiempo son muy pequeñas entonces será casi inmediatamente. Esto es una garantía de que el sistema puede ir a cualquier altura una vez que el sistema de control de velocidad codifique los ajustes en la velocidad de cada motor.

Para asegurar que la inclinación de la plataforma no rebase valores críticos que no se puedan corregir a tiempo, codificamos la información obtenida por el acelerómetro como se muestra en la siguiente figura:

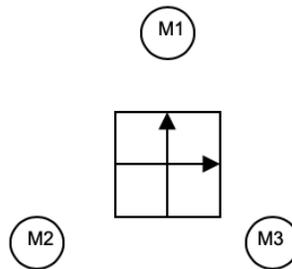


Fig. 6. Arreglo de los motores y el acelerómetro en la plataforma

De esta figura se observa que si se encuentra una inclinación en el eje “+X”, esto se puede corregir mediante el motor M3 en primer lugar y una vez medido el cambio probablemente el motor M1. Si la inclinación es en el eje “-Y”, corrigiendo la velocidad de los motores M2 y M3, será suficiente. Y así sucesivamente. Para implementar el sistema de control en la FPGA se pueden tener diversas alternativas: una es mediante un control sencillo implementado en base a una maquina de estados; la otra que es mas generalizada es utilizando un procesador, el cual nos brinda una capacidad ilimitada de cómputo incluso nos permite realizar multiprocesamiento o procesamiento paralelo lo cual permite también implementar algoritmos de control basados en reconstrucción de la información, algoritmos de planeación de trayectorias e incluso algoritmos genéticos o evolutivos. Cualquiera de estas opciones se pueden implementar debido a la utilización de un dispositivo reconfigurable como la FPGA. Nosotros implementamos un algoritmo

de control sencillo mediante una máquina de estados en VHDL para estabilizar la plataforma en XY a cualquier altura.

Aunque en algunos casos se identifica plenamente un motor o dos para corregir la inclinación, siempre se verifica si la corrección de estos motores es suficiente, sino se varia suavemente también los motores restantes.

2 Conclusiones

En este proyecto logramos elevar una plataforma y estabilizarla en XY a una determinada altura, aunque la altura deseada se alcanza aun lentamente, estamos por conseguir que sea de manera cuadrática en lugar de forma lineal la relación altura a tiempo. El utilizar la tarjeta de desarrollo DE2-70 de Altera, nos ayudó a no tener limitaciones en el momento de implementar las señales de control y codificar la información de los sensores, lo cual habría sido bastante tedioso y además relativamente complicado si se utilizaran controladores discretos para cada etapa. En éste punto es que los sistemas empotrados cobran importancia, ya que los algoritmos implementados en la FPGA se pueden modificar con relativa facilidad.

De igual manera se tienen todos los elementos para implementar reconocimiento de patrones mediante una cámara o incluso comunicaciones inalámbricas al aumentar los módulos a la tarjeta en cualquiera de los puertos de que dispone.

Referencias

1. Jones, J.L., Flynn, A.M., and Seiger, B.A., Mobile Robots, 2nd. Edn. A.K. Peters, 1999.
2. Ghosal, A., Robotics: Fundamental Concepts and analysis, Oxford University Press, 2006.
3. Spong, M.W., Hutchinson, S. and Vidyasagar, M., Robot Modeling and Control, Wiley and Sons, 2006.
4. Pallás, R.A., Sensores y Acondicionadores de Señal, Alfaomega, 2007.
5. Bell, D., Fundamentals and Electronic Devices and Circuits, 5nd. Edn., Oxford University Press; 2008.
6. Catsoulis, J., Designing Embedded Hardware, 2nd. Edn., O'Reilly, 2005.
7. Hamblen, J.O., Hall, T.S. and Furman, M.D. Rapid Prototyping of Digital Systems, Springer, 2008.
8. Nise, N.S., Control Systems Engineering, 4nd. Edn., Wiley and Sons, 2004.
9. Kuo, B.C. and Golnaraghi, F., Automatic Control Systems, Wiley and Sons, 2003.
10. Kulakowski, B.T., Gardner, J.F. and Shearer, J.L., Dynamic Modeling and Control of Engineering Systems, Cambridge University Press, 2007.

Desarrollo de un Robot Interactivo Como Asistente en Terapias para Niños con Autismo.

José Luis Hernández Ameca¹, Gregorio Trinidad García¹, José Ítalo Cortez¹, Juan Chávez Bravo¹

¹Benemérita Universidad Autónoma de Puebla, Facultad de Ciencias de la Computación, Ciudad Universitaria, Edif. CC03-Laboratorio de Sistemas Robóticos “SIRO” 14 Sur y Avenida San Claudio, Fraccionamiento Jardines de San Manuel, C.P. 72570, Puebla, Pue.; México.

amecajl@hotmail.com, tgarcia@cs.buap.mx, jose.italo.cortez@gmail.com, juan.chavez@alumno.buap.mx

Resumen. En el presente trabajo se reporta el uso del modelo de desarrollo incremental para realizar la primera etapa de un robot interactivo, donde el objetivo se ha limitado exclusivamente al desarrollo de la cabeza de dicho robot, el cual se utilizará como una herramienta tecnológica en las terapias para niños con TEA. Como resultado se muestra el primer prototipo del robot humanoide SIRO1.0, el cual se presentó ante 10 niños que, en un futuro cercano podrían utilizar esta herramienta robótica. La cabeza robotica realiza solo tres funciones (sensado de distancia, reproducción de audios y toma de fotos). Después de interactuar con la cabeza del robot se aplicó una encuesta tipo Likert a los niños con la finalidad de recolectar información sobre el grado de amigabilidad que percibieron en este prototipo, los resultados se utilizarán para continuar mejorando este trabajo.

Palabras clave: Autismo, Robot humanoide, Sistema empotrado, Terapia asistida, Trastornos emocionales.

1 Introducción

El autismo es un trastorno del neurodesarrollo que aparece dentro de los primeros tres años de la vida. Es común que las personas con autismo presenten déficits persistentes en la comunicación, interacción social, áreas de integración sensorial y conducta.

Las causas que provocan los Trastorno del Espectro Autista (TEA) aún se desconocen, pero las investigaciones recientes se inclinan hacia un desorden genético, probablemente relacionado con factores biológicos y ambientales [1].

De acuerdo con la Secretaría de Salud del Gobierno del Estado de México, a nivel mundial se calcula que 1 de cada 160 niños padece un TEA. En 2016 en León, Guanajuato, científicos de la organización Autism Speaks realizaron un estudio de prevalencia, donde 1 de cada 115 niños estarían en condiciones de TEA. [2].

En México existen asociaciones que brindan tratamiento a personas que se encuentran en dichas condiciones tales como: La clínica de Intervención de Trastornos Físicos, Sensoriales y del Neurodesarrollo, Centro Autismo Teletón (CAT), Instituto Mexicano de Seguro Social 528-12, Detección y Manejo de Pacientes con Trastornos del Espectro Autista, dentro de las cuales no se reporta el uso de herramientas tecnológicas.

En la presente investigación se han revisado algunos trabajos donde se utilizan diversas herramientas tecnológicas particularmente los robots, los cuales se reportan dentro de las terapias interactivas como en la Universidad de tecnología MARA (UiTM), que presenta el desarrollo de un experimento piloto en el que los niños con TEA fueron expuestos al robot humanoide NAO, que ofrece una plataforma de investigación ideal para la interacción humano-robot (HRI), como resultados muestran la frecuencia con que los niños observan al robot y el tiempo que el robot capto su atención [3].

La Universidad de Vigo, España, presenta un robot con forma de oso equipado con una pantalla táctil que puede registrar información del paciente con discapacidad. Se realizaron experimentos piloto en 73 sesiones terapéuticas con 29 niños, donde los

resultados muestran una rápida adaptación de los niños a interactuar con la nueva herramienta y buenos resultados en áreas fonológicas, morfosintácticas y semánticas [4]. El blog de noticias del Instituto de Ingenieros Eléctricos y Electrónicos IEEE Spectrum, reporta el inicio de la construcción en 2016 del prototipo de robot terapeuta QTrobot de la LuxAI, con la finalidad de auxiliar a los terapeutas en la enseñanza de habilidades sociales. En base a los especialistas se diseñó un robot intermediario, con un cuerpo visualmente agradable, que pueda enseñar cómo interactuar confortablemente con sus compañeros humanos. Actualmente se encuentran realizando pruebas desde el 2018 en varios centros de Luxemburgo, Francia y Alemania [5].

En 2016 el Tecnológico de Monterrey desarrolló el robot Mexicano Teco que pretende funcionar como una herramienta de terapia para el tratamiento de niños con autismo, con el objetivo de enseñar a los infantes a expresar sus emociones, mejorar sus habilidades sociales ayudando a entender las expresiones [6].

2 Metodología

Se ha utilizado el modelo de desarrollo incremental, los clientes (terapeutas) se identifican a grandes rasgos los servicios que proporciona el prototipo. Identifica qué funciones son más importantes y cuáles menos. Una vez que los incrementos del prototipo se han identificado, los requerimientos para las funciones que se van a entregar en el primer incremento se definen en detalle, y este se desarrolla. Durante el desarrollo, se puede llevar a cabo un análisis adicional de requerimientos para los requerimientos posteriores, pero no se aceptan cambios en los requerimientos para el incremento actual. Tan pronto como se contemplan los nuevos incrementos, se integran en los existentes de tal forma que la funcionalidad del prototipo mejora con cada incremento entregado. En la figura 1 se muestra el modelo utilizado [7].

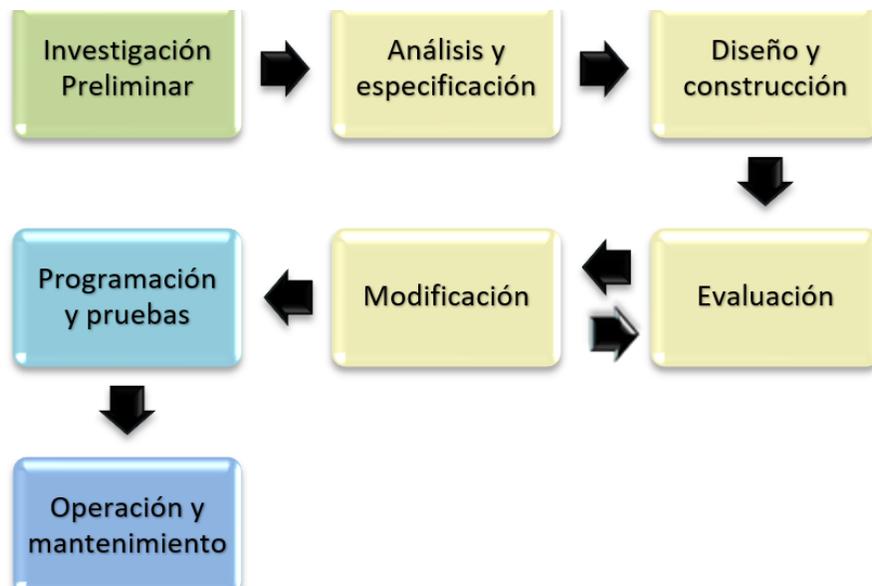


Fig. 1. Modelo de desarrollo incremental

- *Esbozo de requerimientos*: Los requerimientos de funcionalidad se muestran en un diagrama a bloques para representar las acciones que actualmente realiza la cabeza del robot. El sensor de ultrasonido (instalado en la boca del prototipo), detecta la presencia de objetos, a continuación, se envía una señal digital al sistema empotrado (SE). Si la evaluación de las condiciones resulta verdadera, se encienden los leds de los ojos, se reproducen tres audios de manera consecutiva (grabados previamente en

la memoria micro SD) y se toma como evidencia una foto de la reacción del niño mediante la cámara, este funcionamiento se muestra en la figura 2.

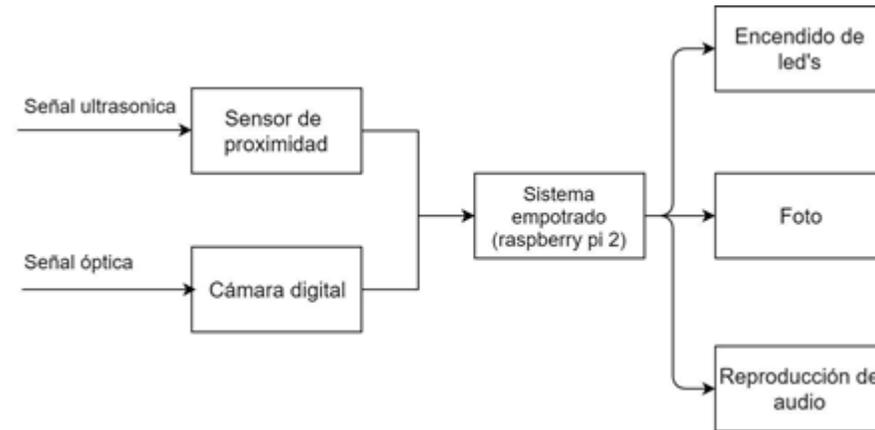


Fig. 2. Diagrama a bloques de las funciones realizadas por la cabeza del robot

- Asignación de requerimientos a los incrementos: Los requerimientos que hasta la fecha se reportan son: grado de amigabilidad de la cara del robot, distancia de sensado, reproducción de tres audios de tipo Waveform Audio Format (wav) con frases de apertura (Hola, ¿Cuál es tu nombre? ¿Cómo estás?).
- Diseño de la arquitectura del prototipo: La arquitectura del prototipo se divide en 3 partes, estructura física, funcionamiento lógico y hardware.
- La estructura física se diseñó en un programa informático multiplataforma, dedicado al modelado y creación de gráficos tridimensionales. En la figura 3 se muestra el diseño realizado en polímero termoplástico.

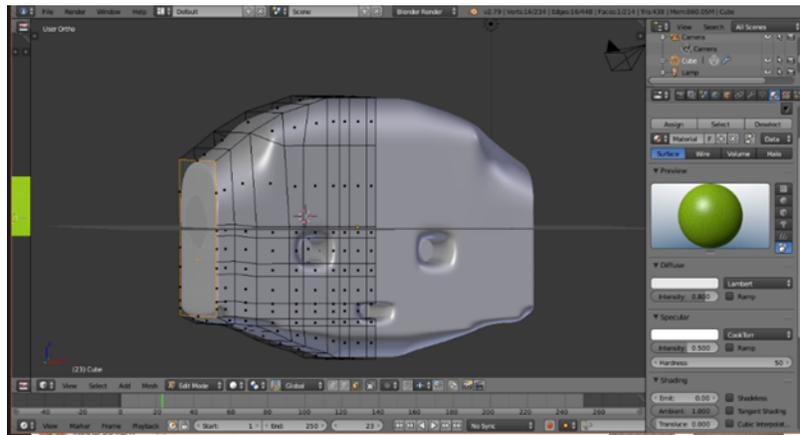


Fig. 3. Diseño estructural de la cabeza del robot SIRO1.0

El funcionamiento lógico se modeló con una máquina de estados finitos, donde el estado inicial es: “Encendido”. El siguiente estado es “Detección de proximidad”, se asigna un “0” si no detecta ningún objeto frente al sensor y seguirá esperando durante un tiempo indeterminado en el estado actual, en caso contrario se asigna el valor “1”, y continúa al estado siguiente llamado “Reproducción de Audio y encendido de Leds”, una vez terminado, se procede al siguiente estado que es “Apagado de Leds y stop del audio”. Por último, se regresa al estado de detección en el cual volverá a esperar para pasar al siguiente estado cuando detecte un objeto. La máquina de estados finitos, se

implementó en un sistema empujado (raspberry pi 2) de arquitectura tipo Reduced instruction set computing (RISC), en el lenguaje de programación Python. En la figura 4 se muestra la máquina diseñada.

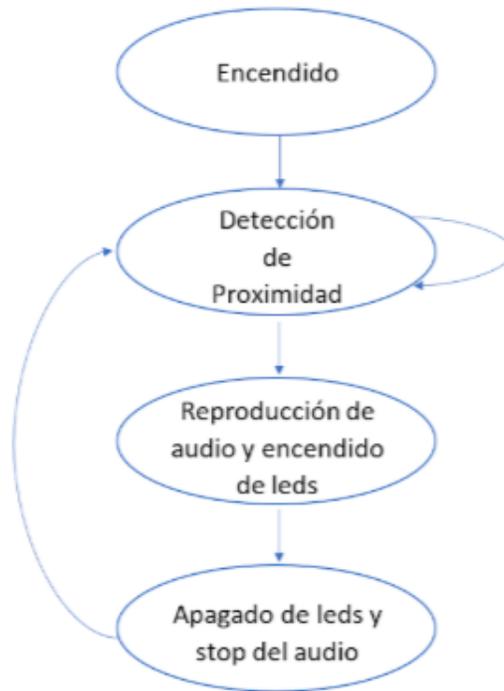


Fig. 4. Máquina de estados finitos diseñada para el robot SIRO1.0

- Desarrollo de incrementos del prototipo: Una vez que se realizó el diseño estructural mediante software, se procedió a imprimirlo en una máquina capaz de realizar réplicas de diseños en 3D. El prototipo realizado tiene 10.5 cm de altura, 13 cm de ancho y 12 cm de profundidad, como se muestra en la figura 5.

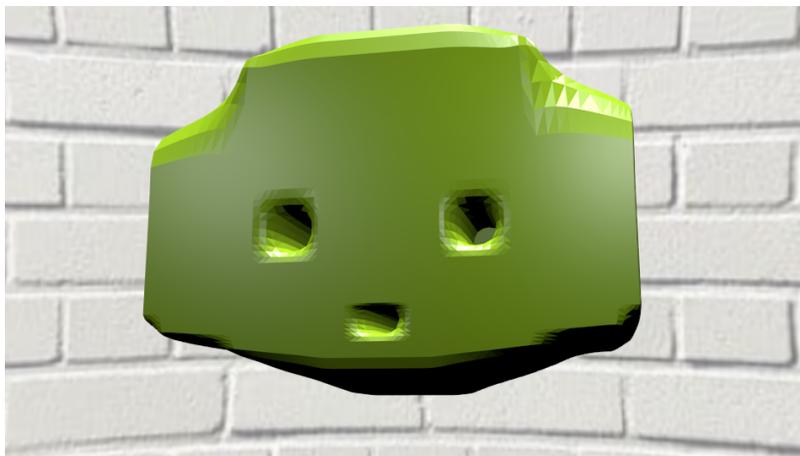


Fig. 5. Cabeza de robot interactivo.

El hardware o etapa electrónica se implementó con un sensor ultrasónico HC-SR04, SE (raspberry Pi 2 B), driver LM298n, bocina de 8 ohmios, un par de leds y cámara digital Pi NoIR. El diagrama de conexión se muestra en la figura 6.

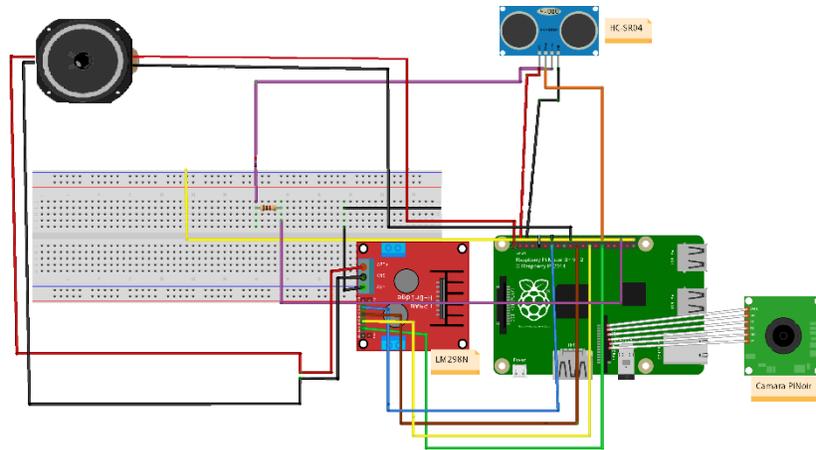


Fig. 6. Raspberry pi 3 Modelo B 1Gb con elementos del hardware.

- Validación de incrementos: Esta etapa consistió en exponer la cabeza del robot ante diez usuarios potenciales (3 niños y 7 niñas con edades entre 6 a 12 años, que presentan TEA y pertenecen al Centro de Atención Múltiple CAM campus Chignahuapan) de manera individual durante un tiempo de 10 segundos. Donde mediante un instrumento de recolección de datos el terapeuta y profesor registraron sus apreciaciones. Después de esta experiencia, se aplicaron un par de encuestas a los niños con la finalidad de medir sus reacciones ante la cabeza del robot.
- Integración de incrementos: Esta etapa está en cambios iterativos que van desde funciones, colores, dimensiones, intensidades de audio, distancia de sensado, hasta familiaridad con el prototipo.
- Validación de prototipo: Para validar el prototipo, se están utilizando listas de cotejo, entrevistas, estadísticas y encuestas. Esta información está a cargo del terapeuta y profesores responsables del CAM Chignahuapan.

3 Resultados

Como resultados de la etapa de evaluación se obtuvieron el tiempo de trabajo y tiempo de reacción, los parámetros se obtuvieron desde la interfaz gráfica del sistema operativo Raspbian con el que trabaja el SE raspberry Pi 2 B y se muestran en la tabla 1.

Tabla 1. Funciones evaluadas

Función	Tiempo de trabajo	Tiempo de reacción
Encendido de Led's	Indefinido	0.1 seg.
Reproducción de Audio	5 a 10 seg.	1 seg.
Toma de fotografías	1 seg.	0.4 seg.

Se aplicaron dos encuestas a una población de 10 niños de entre 6 a 12 años, con la finalidad de medir la percepción amigable del rostro del robot. Las respuestas se evaluaron mediante una escala tipo Likert, que va desde nada satisfactorio hasta satisfacción total, los resultados se muestran gráficamente en la figura 7.

La escala de Likert es un tipo de instrumento de medición o de recolección de datos que se dispone en la investigación social para medir actitudes. Se le conoce como escala sumada debido a que la puntuación de cada unidad de análisis se obtiene mediante la sumatoria de las respuestas obtenidas en cada ítem.

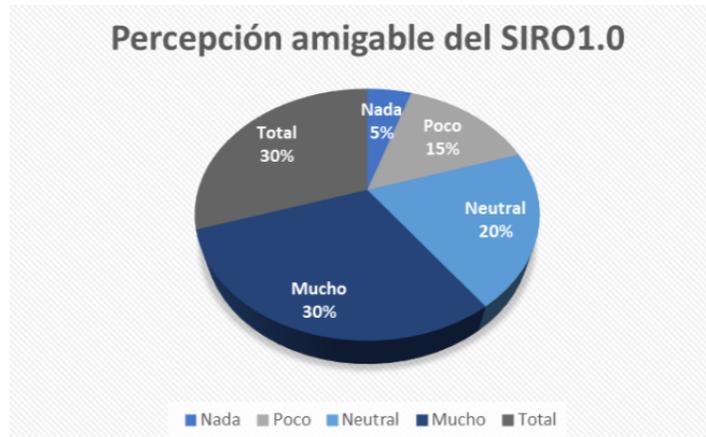


Fig. 7. Resultado de la prueba Likert percepción amigable del SIRO1.0.

La segunda encuesta se aplicó a los mismos niños sobre la reacción del robot ante la presencia humana, los resultados se muestran en la figura 8.

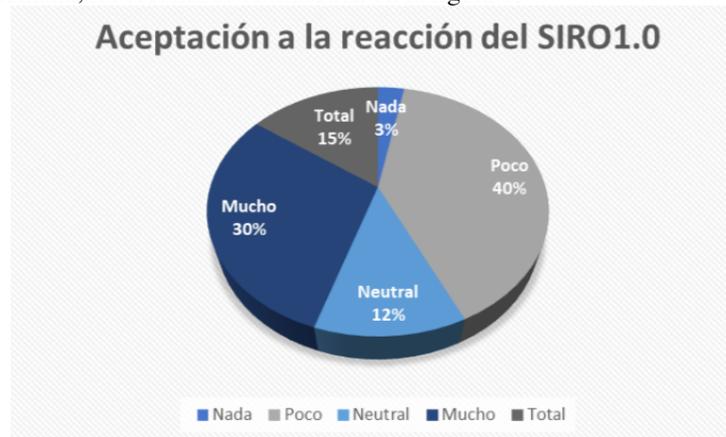


Fig. 8. Resultado de la prueba Likert de aceptación a la reacción del SIRO1.0.

4 Conclusiones y trabajos futuros

Los resultados obtenidos en esta primera versión del SIRO1.0 muestran que el objetivo de la investigación se alcanzó, mediante el diseño e implementación de este prototipo, con rostro amigable y reacción a la presencia de objetos.

De acuerdo con los resultados de las gráficas de pastel, se propone como trabajo futuro mejorar el diseño amigable, mejorar los espacios internos para la adaptación de dispositivos electrónicos, así como generar orificios que permitan una adecuada ventilación, aumentar cuello, hombros y brazos al robot para asemejarse al humano, mejorar y aumentar el número de reacciones que realiza actualmente este robot.

Se espera poder desarrollar terapias basadas en la convivencia constante de los niños con el robot, ya que la falta de expresiones del robot permitirá crear lazos y facilidad de interacción por parte de los niños.

Se desea estudiar las reacciones que los pequeños tengan al convivir con el SIRO1.0 y basados en esto, planear técnicas y adaptar el sistema del robot.

Agradecimientos. Agradecemos a la Facultad de Ciencias de la Computación por prestarnos la infraestructura para trabajar. Al Laboratorio de Sistemas Robóticos SIRO y sus

integrantes por el apoyo recibido y el conocimiento compartido durante la realización del presente trabajo.

Referencias

1. Autismo ARENA - ¿Qué es el autismo? (s.f.). Recuperado 24 junio, 2019, de <http://www.autismoarena.org.mx/autismo.html>
2. Autismo Visión Cevece. (s.f.). Recuperado 24 junio, 2019, de <http://salud.edomex.gob.mx/cevece/documentos/difusion/tripticos/2017/Semana%2024.pdf>
3. Syamimi Shamsuddin, S. S., Hanafiah Yussof, H. Y., Luthffi Ismail, L. I., Fazah Akhtar Hanapih, F. A. H., Salina Mohamed, S. M., Hanizah Ali Piah, H. A. P., & Nur Ismarrubie Zahari, N. I. Z. (2012, 25 marzo). Initial Response of Autistic Children in Human-Robot Interaction Therapy with Humanoid Robot NAO. Recuperado 24 junio, 2019, de <https://ieeexplore.ieee.org/document/6194716>
4. Robles-Bykbaev, V. B. R. Vladimir, Ochoa-Guaraca, M. G. O. Mario, Carpio-Moreta, M. C. M. Marco, Pulla-Sanchez, D. S. P. Daniel, Serpa-Andrade, L. A. S. Luis, Lopez-Nores, M. N. L. Martín, & García-Duque, J. D. G. Jorge. (2016, 11 noviembre). Robotic assistant for support in speech therapy for children with cerebral palsy. Recuperado 24 junio, 2019, de <https://ieeexplore.ieee.org/document/7830603>
5. Emily Waltz, E. W. (2018, 8 agosto). Therapy Robot Teaches Social Skills to Children With Autism. Recuperado 24 junio, 2019, de <https://spectrum.ieee.org/the-human-os/biomedical/devices/robot-therapy-for-autism>
6. Tec Review. (2017, 22 noviembre). Robot mexicano que ayuda a niños con autismo. Recuperado 24 junio, 2019, de <https://tecreview.tec.mx/robot-mexicano-ayuda-a-ninos-autismo-sale-a-la-venta/>
7. Sommerville, I., & Galipienso, M. I. A. Ingeniería del software. Londres, Reino unido: Pearson Educación. pp. 66-68 (2005).
8. Fernández P. Ignacio (1982) Construcción de una escala de actitudes tipo Likert. Recuperado 9 agosto, 2019, de https://www.insst.es/documents/94886/326853/ntp_015.pdf/2f5dff8-a6f7-4c22-a101-28a0c13e1730

Diseño de un Shield con microcontrolador ARM-Cortex-M0 para la implementación de redes automotrices (CAN-BUS), para apoyar el proceso de enseñanza-aprendizaje.

Saul Luna Minor, Nicolás Quiroz Hernández, Juan Carlos Ramírez Morales.
Laboratorio SLED, Benemérita Universidad Autónoma de Puebla,
Puebla, México.

sual.lunam@alumno.buap.mx , nicolas.quirozh@correo.buap.mx , jcarlos.ram04@gmail.com

Resumen. Se diseñó un Shield para apoyar el proceso enseñanza-aprendizaje en redes automotrices (CAN-BUS^[1]) para estudiantes que requieren comunicar sensores y actuadores, en diversas aplicaciones como la automotriz. El Shield es un módulo especializado para implementar una comunicación CAN-BUS, integra un microcontrolador ARM-Cortex^[2] M0, el cual posee: un controlador CAN (Controller Area Network), un transceptor CAN MCP2551 que permite acoplarse a los niveles físicos del bus, además de prevenir daños por corto-circuitos en dicho bus, un sensor de temperatura, un potenciómetro, pines de entrada-salida para conectar diversos sensores, actuadores o señales que se requieran trabajar, adicionalmente un regulador de voltaje para alimentar al microcontrolador. Este fue desarrollado en el laboratorio de SLED, ubicado en la Facultad de Ciencias de la Electrónica. Para la verificación del correcto funcionamiento, se realizaron dos pruebas, implementando una comunicación entre dos microcontroladores (ARM-Cortex M y PIC), y la otra comunicándose a un automóvil JETTA Hybrid, a través del protocolo OBD-II, con el fin de obtener estos parámetros: RPMS, velocidad, presión y temperatura del automóvil, visualizándolos en una interfaz gráfica.

Palabras Clave: CAN-BUS, arnés, MCP2551, Redes automotrices, ARM Cortex-M, OBD-II.

1 Introducción

El parque vehicular ha ido en aumento en los últimos años, como se observa en la Figura 1, por consiguiente, la demanda de estudiantes y personas especializadas en el área automotriz, ha crecido considerablemente.

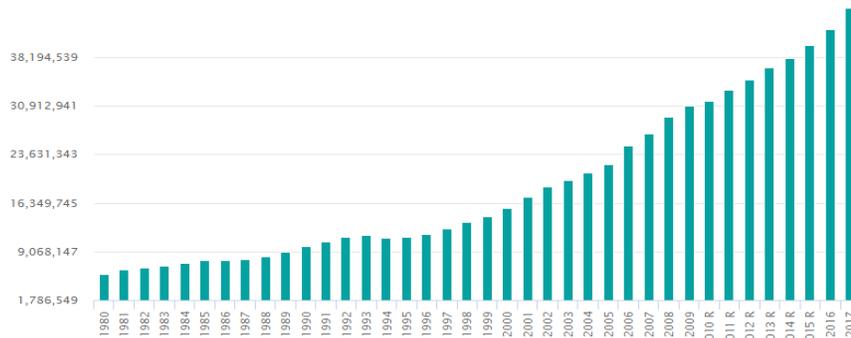


Fig.1. Incremento del parque vehicular reportado por el INEGI^[3] desde el año 1980 hasta el año 2017, donde se nota un crecimiento tipo exponencial.

En México se han alojado diversas empresas enfocadas al sector automotriz, como Continental, que requieren personal con conocimientos en redes automotrices, para

diversos proyectos. En el estado de Puebla, tiene a disposición Volkswagen y Audi, quienes son empresas automovilísticas internacionales, las cuales ofrecen oportunidades de trabajo y prácticas profesionales a un gran número de estudiantes. A partir de lo mencionado surge la idea de hacer un Shield que facilite la interacción de una red CAN-BUS, de manera práctica y cómoda, para así, fortalecer los conocimientos adquiridos por el estudiante a lo largo de la carrera, de modo que aumentan sus posibilidades de éxito, al estar mejor preparados para el campo laboral y educativo.

Este Shield al tener un ARM-Cortex se tiene acceso a periféricos, como: I2C, SPI, RS-232, CAN, LIN, ADC, entre otros, permitiendo la flexibilidad para implementar comunicación con sensores analógicos o digitales, que puedan tener incluso protocolos como los aludidos anteriormente, permitiendo al Shield, ser competitivo con los existentes en el mercado.

Entre las diferentes arquitecturas existentes, se revisaron para la selección del microcontrolador, las basadas en ARM-Cortex, por las siguientes ventajas:

- Menor precio.
- Mayor número de periféricos en un reducido tamaño.
- Bajo consumo de energía.
- Extenso rango de temperatura^[10] (-40°C hasta 85°C).
- Amplia gama de IDE's para su programación (Keil, Atollic, IAR, etc.)
- Considerable información en internet (Manuales, libros, documentos, esquemáticos, tutoriales y páginas web), que ayuda al uso de esta tecnología.

Sin embargo, esta arquitectura es fabricada por varias compañías (Freescale, Texas Instruments, NXP, etc.) que desarrollan gran gama de microcontroladores, por lo cual, se selecciona a STMicroelectronics, por la gran variedad de información que ofrecen en internet, como, el software de configuración (STM32CubeMX), que permite de una manera amigable al usuario, especificar el microcontrolador y los periféricos a usar, generando plantillas de código que facilitan la programación, para los diversos IDE'S existentes.

1.1 Comparativa con respecto a otros Shields

En el mercado existen diferentes Shields, por ello se exponen algunos en la Tabla 1, con el fin de comparar características de una manera más clara, cabe mencionar, que la mayoría crean bibliotecas para ser compatibles con la plataforma de Arduino, debido a que es un IDE bastante famoso y sencillo de usar.

Como se muestra en la Tabla 1, los módulos **RobotDyn CAN-BUS** y **Arduino CAN-Bus Shield with uSD Card Holder V2**, son Shields que tienen bibliotecas dedicadas para su uso con Arduino, pero estos no poseen comunicación LIN. Mientras que los módulos **dsPIC33EV 5V CAN-LIN STARTER KIT** y **Teensy 3.2 CAN Bus And LIN Bus Breakout Board**, si tienen incluyen este protocolo y su propio programador. La tarjeta desarrollada es similar a los Shields anteriores, teniendo como mejora el configurar el protocolo LIN, como maestro o esclavo, además de incluir potenciómetro dentro de la misma tarjeta y sensor de temperatura, con el fin de que el alumno no tenga que conectar estos componentes externamente, si es que llegase a necesitarlos.

El Shield diseñado tiene un costo de \$920, en su primera versión, la cual no integra un programador. Es conveniente que, para su venta al público, este sea sometido a un análisis de mercado, donde se considera que bajaría su costo por su fabricación en serie. Otro factor para definir el costo, está dado por los precios de los demás Shield existentes, que dan una referencia para ser competitivos con ellos.

Tabla 1. Comparativa de los Shield con respecto a las existentes en el mercado.

Shield	Microcontrolador	CAN	PWM	ADC	SPI	I2C	Precio aprox. Pesos
Arduino CAN-Bus Shield with uSD Card Holder V2 ^[4] 	MCP2515 con controlador SPI a CAN-BUS (10 MHz)	Salida CAN-BUS con transceptor incluido CAN conector DB9	No cuenta	No cuenta	No cuenta	No cuenta	\$550
RobotDyn CAN-BUS ^[5] 	CP2515 con controlador SPI a CAN-BUS (10 MHz)	Salida CAN-BUS con transceptor incluido. CAN conector DB9	No cuenta	No cuenta	No cuenta	No cuenta	\$285
Teensy 3.2 CAN Bus And LIN Bus Breakout Board ^[6] 	MK20DX256 32 bit ARM Cortex-M4 72 MHz	Salida CAN-BUS con transceptor incluido Bomeras	12	21	1	2	\$1450.80
dsPIC33EV 5V CAN-LIN STARTER KIT ^[7] 	dsPIC33EV256GM106 Con programador PICKIT 2 incluido.	Salida CAN-BUS con transceptor incluido Bomeras CAN conector DB9	6	4	2	2	\$1528.16
Sled CAN v1.0 	M32F042C6T6 48 MHz	Salida CAN-BUS con transceptor incluido Bomeras	6	4	3	2	\$920

2 Redes de comunicación automotriz

Las complejidades de los vehículos actuales necesitan de varias redes de comunicación, siendo divididas en función de su desempeño. La primera es la red de Tracción encargada de controlar el tren motriz, los frenos ABS y la transmisión, la segunda es la red de Confort encargada de la comodidad de los pasajeros, que corresponde al habitáculo (aire acondicionado, luces, etc.). La tercera es la red Infoentretenimiento que proporciona información y entretenimiento a los pasajeros.

Para la comunicación de estas redes con los sensores y/o actuadores del vehículo, se utilizan protocolos específicos como: CAN (*Controller Area Network*), LIN (*Local Interconnect Network*), MOST (*Media Oriented System Transport*) y Flexray. Estos están diseñados para soportar ruido eléctrico, ciertos rangos de temperaturas que soporta el automóvil, así como en el caso del CAN-BUS, indicar por medio de los faros si ha ocurrido algún fallo en la red.

2.1 Red CAN-BUS

El CAN-BUS permite interconectar los diferentes actuadores y sensores del vehículo, así como consumir menor energía, al no usar un rango de voltaje de 12 V, sino tenido un rango de 1.5 V - 3.5 V.

Es una Red robusta, tolerante a fallos, con las siguientes características:

1. Se conforma de un par trenzado de dos cables, donde CAN-HIGH es de color negro con naranja y CAN-LOW es de color marrón con naranja (Figura 2). El que sea trenzado ayuda a reducir el efecto de Crosstalk^[1].



Fig. 2. Cable típico CAN-BUS.

2. Se considera bit dominante a un cero lógico y un bit recesivo a un uno lógico. Es un protocolo diferencial, ya que la diferencia de voltajes de la línea CAN_LOW y CAN_HIGH nos representa ya sea, un bit dominante o recesivo. Esto facilita la detección de un bit. En la Figura 3 se aprecia lo señalado.

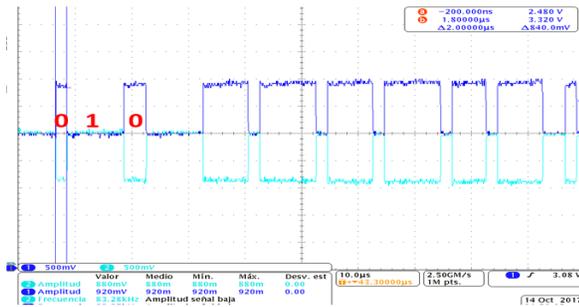


Fig. 3. Trama CAN-BUS capturada en un osciloscopio donde la línea azul oscuro es CAN_HIGH y la de azul claro es CAN_LOW.

3. La Figura 4, se muestran los niveles de tensión respectivos al CAN_HIGH y CAN_LOW. Si se les llegase afectar una señal parasito, que consecuentemente hiciera variar el voltaje, se asume una tolerancia de variación permitida del ± 0.5 V.

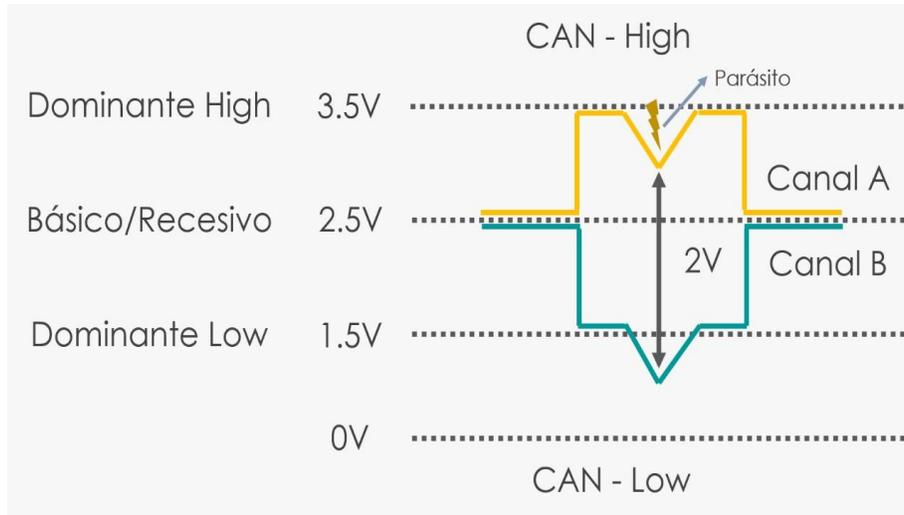


Fig. 4. Compensación de influencias parásitas.

- Una red CAN-BUS está compuesta por dos resistencias de $120\ \Omega$ conectadas en paralelo. Los dispositivos conectados a sus extremos, se les denomina “nodos” (Figura 5), estos son actuadores y sensores del vehículo.

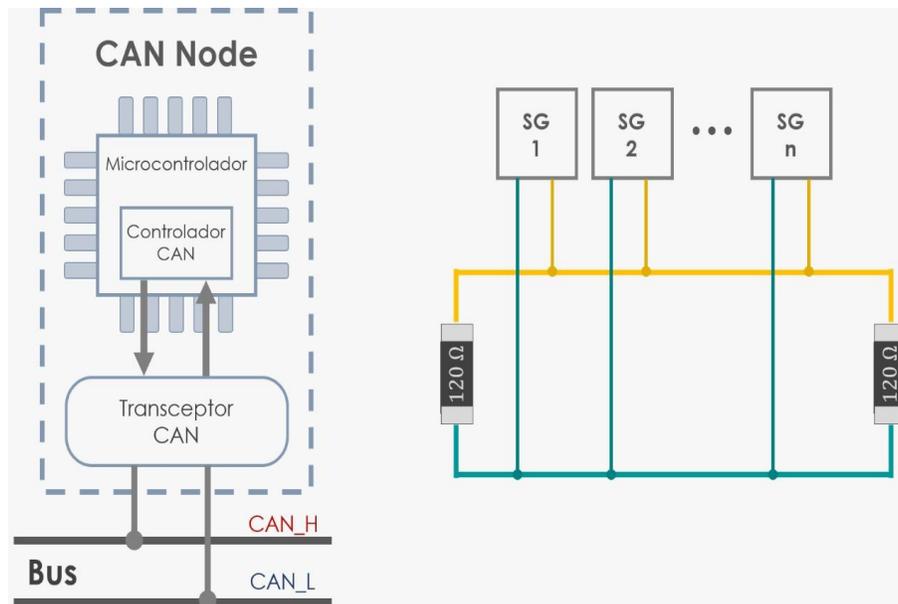


Fig. 5. Composición interna de un nodo (parte izquierda) y una red CAN-BUS (parte derecha)

- Un nodo (Figura 5) se conforma de un microcontrolador que posea internamente un controlador CAN ó maneje uno externo, así como el transceptor^[1] CAN (Figura 6), siendo éste el que acopla los niveles de tensión mostrados en la Figura 4.



Fig. 6. Transceptor CAN MCP2551 superficial montado en una tarjeta para conexión al protoboard.

En vehículos que no tenían CAN-BUS, el cable que requerían para interconectar los diversos dispositivos, llegaba a equivaler a 1km de largo, por esta razón, el CAN-BUS al usar solo dos cables para interconectar varios nodos (hasta 114 nodos si es que se usa el transceptor MCP2551), se reduce el cableado utilizado para comunicar las diferentes redes del automóvil.

3 Desarrollo del Shield

3.1 Características del Shield

La tarjeta está diseñada para que el usuario pueda crear una RED-CAN con facilidad, al disponer de borneras para la fácil conexión con un arnés eléctrico, además de probar todas las funciones correspondientes al protocolo. Se analizaron diferentes modelos de microcontroladores ARM-Cortex, se seleccionó un ARM-Cortex M0, por su reducido tamaño, bajo costo, bajo consumo energía y por las características que se requieren, se enlistan las características que posee el Shield(Figura 7):

- 14 ADC con una resolución de 12 bits.
- 6 Timers configurables para PWM, comparación,
- Puerto dedicado para la programación del microcontrolador.
- 14 Pines de propósito general, para el uso libre del usuario.
- Comunicación Serial.
- Protocolo de comunicación I2C y SPI.
- Comunicación *CAN-BUS* con borneas para fácil conexión y transceptor CAN MCP2551.
- Un potenciómetro que puede ser conectado a cualquier ADC del microcontrolador para hacer pruebas en la misma tarjeta.
- Un sensor de temperatura LM35D analógico conectado a un ADC para su prueba en la misma tarjeta.
- Tiene un cristal de 8 MHz, que puede alcanzar mediante el PLL, hasta los 48 MHz.



Fig. 7. Tarjeta de desarrollo SLED CAN v1.0 vista superior.

El Shield es programado utilizando el programador ST-LINK V2, el cual está incluido en la mayoría de tarjetas de desarrollo de STMicroelectronics, este puede programar diferentes familias de microcontroladores ARM, al utilizar la tarjeta como Shield no se requiere programador, permite reducir costos, debido a la fabricación y a su vez esto permite reducir contaminación generada por la creación del programador. En la Figura 8, se muestra el momento en el Shield se programó utilizando el ST-LINK V2 que tiene la tarjeta NUCLEO-F302R8.

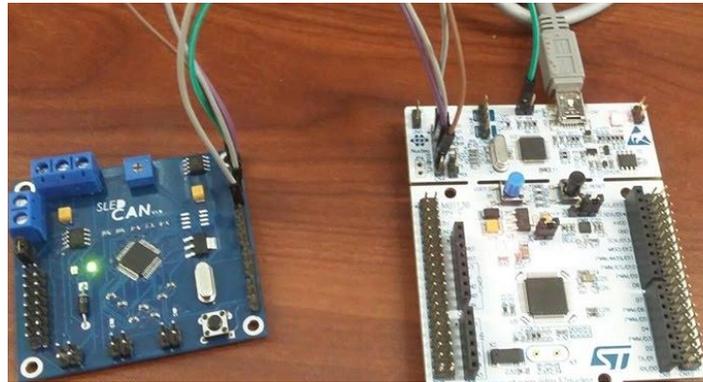


Fig. 8. Shield programado por el ST-LINK V2, donde el led verde indica alimentación en la tarjeta.

4 Pruebas realizadas

Para corroborar el correcto funcionamiento del Shield, se hicieron dos pruebas, en ambas se considero la comunicación entre dos nodos, siendo un nodo la tarjeta desarrollada y en el caso de la primera prueba se considera al PIC como otro nodo. En la segunda, se estableció comunicación con un auto (Jetta Hybrid), por medio del OBD-II^[1], el cual también se consideró con otro nodo.

4.1 Primera prueba, envío de un contador binario hacia un PIC.

Esta prueba consiste en enviar un contador binario a través de CAN-BUS hacia un PIC18F4480, el cual está insertado en la tarjeta de desarrollo SPUTNICK, transmitiendo un contador binario del 0-255. El esquema se ve en la Figura 9. Como la tarjeta no dispone de un transceptor CAN-BUS integrado, entonces se usa el de la Figura 6. Visualizado a más detalle en la Figura 10, él envió-recepción de datos entre ambos dispositivos.

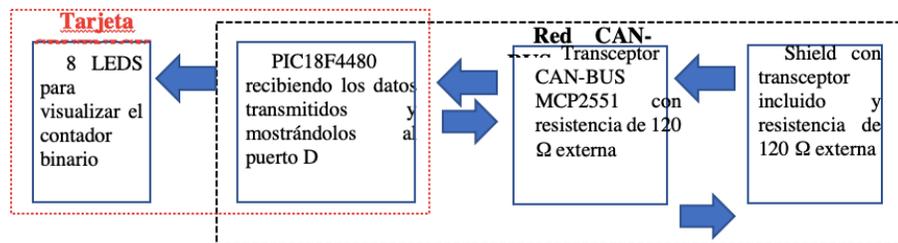


Fig. 9. Diagrama a bloques de los componentes usados para la primera prueba.

Entre los softwares existentes para programar microcontroladores de STMicroelectronics, KEIL es uno de los más completos, ya que, permite seleccionar entre los diferentes programadores desarrollados para las correspondientes marcas de microcontroladores, el específico para la tarjeta NUCLEO-F302R8 (en este caso el ST-LINK V2), además de dar varias opciones de configuración. En la Figura 11, se muestra un fragmento del código usado en la prueba.

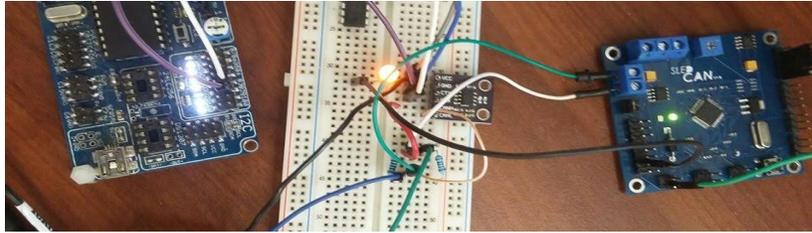


Fig. 10. Los datos son mostrados en los leds que están conectados al puerto D, del PIC.

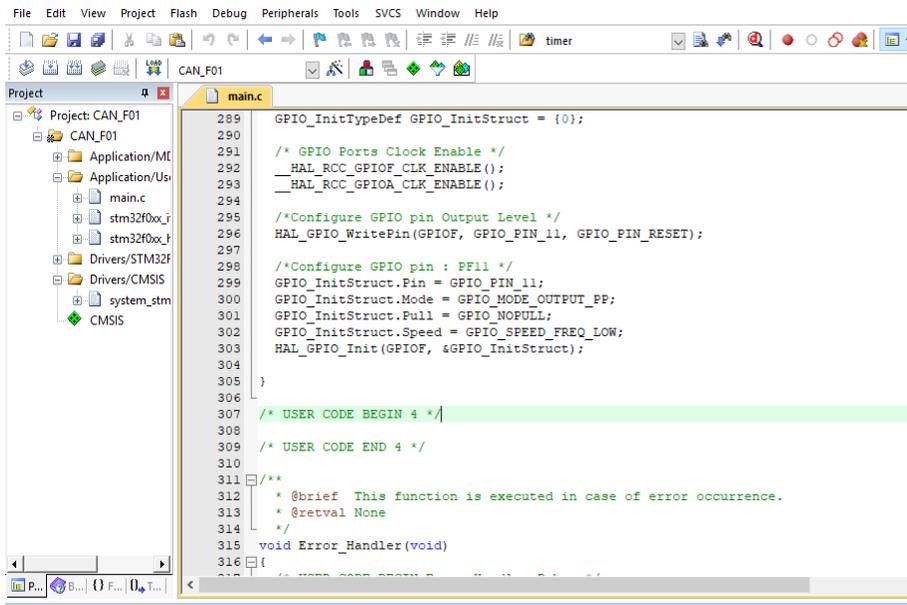


Fig. 11. IDE de desarrollo KEIL que permite una configuración completa para la programación del dispositivo.

La configuración de los periféricos se hace en el software STM32CubeMX, ofreciendo una interfaz de usuario interactiva. La Figura 12, se encierra en un círculo rojo, los parámetros de tiempos que necesita el microcontrolador, para que transferir datos a una frecuencia de 500 kbps.

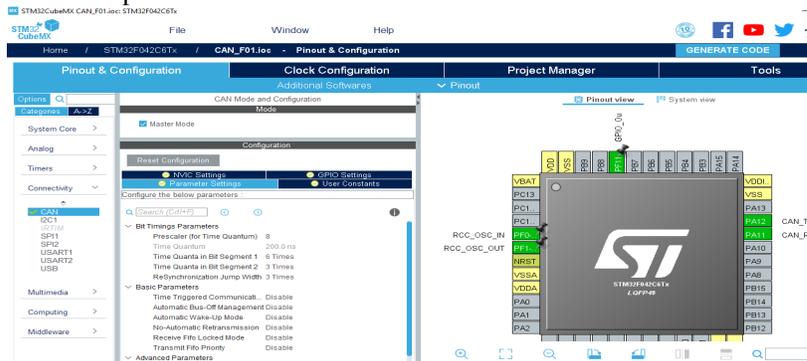


Fig. 12. STM32CubeMX permite configurar los pines del microcontrolador de una manera gráfica, facilitando la ubicación de estos, sin tener que revisar el datasheet.

Estas medidas de tiempo se les llama “Bit timings” y los valores correspondientes, se pueden obtener mediante el complemento CANCELATOR (Figura 13), este viene

integrado en el software de desarrollo MikroC, donde cabe mencionar, que en este IDE se hizo la programación del PIC. Estos tiempos permiten tener una sincronización más fina, cuando se recibe un bit y no malinterpretar si es “uno” ó “cero”, por tanto, hay nula información errónea. En el complemento, es necesario ingresar la frecuencia a la que trabaja el dispositivo (en este caso el Shield fue configurado a 40 Mhz) y la velocidad del CAN-BUS (500 kbps), que se desee trabajar.

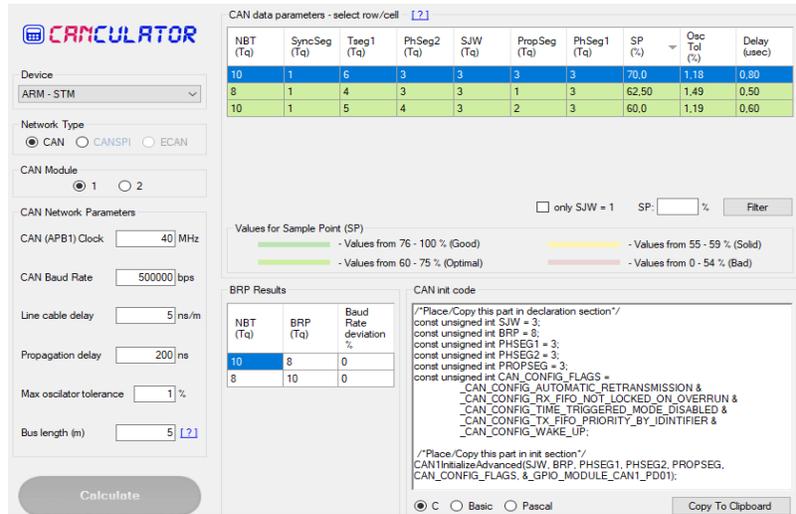


Fig. 13. Completo CANCELATOR, que dispone de una gran variedad de dispositivos que puede configurar, entre ellos PIC'S.

A través del osciloscopio, podemos observar la trama del CAN-BUS transmitida desde el Shield al PIC (Figura 14). El identificador^[1] es un parte de la trama del CAN-BUS que sirve para etiquetar un nodo, por ejemplo, la mayoría de vehículos existentes tienen el identificador 0x7E8, el cual es un estándar para comunicarnos mediante OBD-II^[8]. Se sugiere que si se arma una red CAN-BUS, cada nodo, tenga un diferente identificador.



Fig. 14. Fragmento de trama enviada, donde el primero dato es 0x01, siendo este, el que procesa y representa el PIC en los leds.

4.2 Prueba realizada en un auto real

Mediante el protocolo OBD-II^[1], se realizó una prueba en el auto híbrido (Figura 16). Obteniendo datos como las RPM, velocidad, presión del aceite y temperatura del motor. Para esto el identificador del Shield debe ser 0x7DF y el del auto debe responder con el 0x7E8. En la figura 15, se observa en bloques, los dispositivos involucrados en esta prueba.

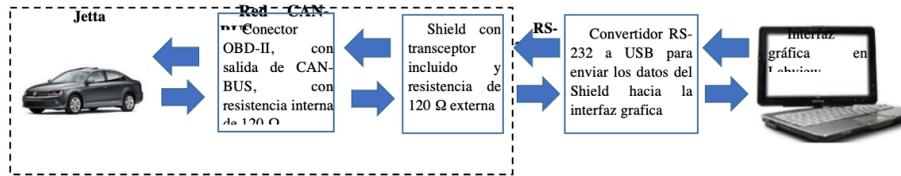


Fig. 15. Diagrama a bloques de los componentes usados para la primera segunda prueba.

El OBD-II especifica que valores se espera recibir y la forma de cómo tratar esta información, para después ser procesada y visualizada, por medio de algún software. Por practicidad se usó LabVIEW^[9], donde se le realizó la interfaz gráfica de la Figura 17.

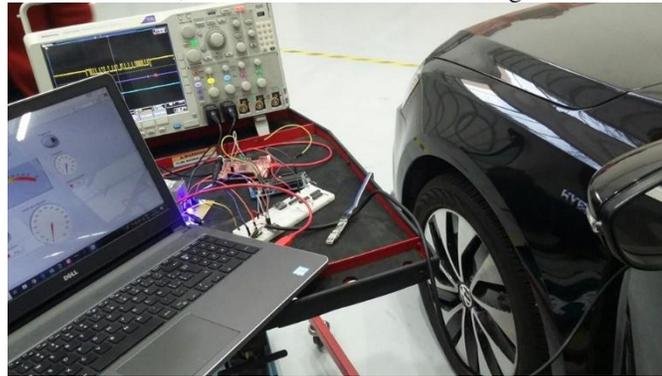


Fig. 16. Pruebas realizadas al auto híbrido.

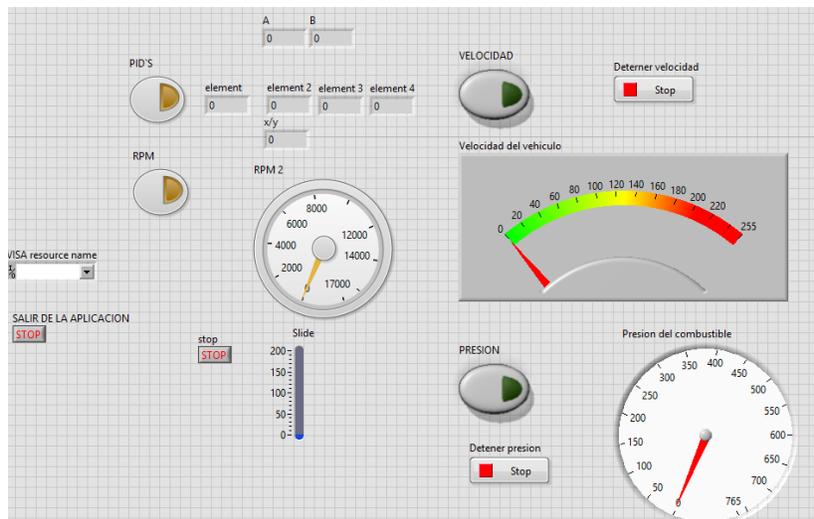


Fig. 17. Interfaz gráfica hecha en labVIEW.

5 Resultados

5.1 Resultados de la primera prueba.

En la Tabla 1, se comparan los datos enviados y los recibidos donde, como se observó en la Figura 14, se aprecia el dato enviado que debe corresponder al visualizado en los leds de la tarjeta SPUTNICK.

Tabla 2. Comparativa de algunos datos enviados.

Dato enviado del Shield	Dato recibido en el PIC
0x01	0x01
0x92	0x92
0xD3	0xD3

5.2 Resultados de la segunda prueba.

En la segunda prueba, considérese que algunos de los datos solicitados, se necesitan tratar antes de mostrarlos, como ya se mencionó, por lo que, por ejemplo para obtener las “rpm”, primero se manda el PID^[1], el cual es un código que solicita el dato de las rpm y el vehículo responde con dos datos, A y B, entonces con la siguiente fórmula se obtiene el dato real, que debería ser casi igual al representado por el vehículo.

$$rpm = \frac{256 * A + B}{4}$$

Tabla 3. Comparativa de los datos solicitados con los que se visualizan en el cuadro de instrumentación.

Datos enviados del Shield		Datos enviados del Jetta Hybrid		Dato registrado en la interfaz gráfica en Labview.	Dato visualizado en el cuadro de instrumentación del Jetta Hybrid.
Identificador	Dato solicitado(PID ^[1])	Identificador	Dato enviado		
0x7DF	0x0C(rpm)	0x7E8	A= 0x49 B= 0x54	4693 rpm	4967 rpm
0x7DF	0x0D(Velocidad)	0x7E8	A= 0x20	21 km/h	19 km/h
0x7DF	0x0F(Temperatura de la toma de aire)	0x7E8	A= 0x3F	23°C	23°C

Hay cierta incertidumbre en los datos enviados y recibidos, puesto que, Labview recibe un dato digital y el visualizado en el Jetta es analógico, la variación obtenida depende del mecanismo de representación del auto, ya que este tiene cierto offset, así como, el dispositivo que transmite y adquiere la información, ya que, en ciertos parámetros, como en la rpm, se tienen variaciones más rápidas, contrastando con la temperatura.

6 Apoyo del proceso enseñanza-aprendizaje de protocolos automotrices para los alumnos.

Se trabajó con dos grupos de alumnos, durante 8 secciones, cada sección de dos horas, al grupo A trabajaron con el módulo **Arduino CAN-Bus Shield with uSD Card Holder V2**^[4] y el grupo B con el Shield desarrollado. La primera sección se les explicó a ambos grupos, que se les iba a dar un curso sobre redes automotrices (CAN-BUS y LIN) para esto como material de apoyo, al grupo A se les dio el Arduino UNO y el Shield ya aludido, mientras que al B el dispositivo descrito en este artículo.

Ambos grupos se les explico el protocolo CAN-BUS y LIN, además de armar un arnés eléctrico, comunicando hasta 4 nodos. Al final se les pidió que dieran su opinión con respecto al material de trabajo, donde en la Tabla 2, se comparan desventajas y ventajas del material usado. Como tal el grupo A, fue el que se le facilito más establecer comunicación con dos nodos, sin embargo, el grupo B, se le hizo más practico la conexión, además de que pudieron configurar paramentos, como los tiempos quanta, que son indispensables cuando se tiene aplicaciones críticas, como es el caso del sistema de frenado del auto (ABS), donde se requieren tiempos muy precisos.

Tabla 2. Comparativa de los dos grupos con respecto a los dos Shields ya mencionados.

Grupo A		Grupo B	
Ventajas	Desventajas	Ventajas	Desventajas
Bibliotecas que ofrecen una configuración rápida y sencilla del protocolo CAN-BUS.	No se puede configurar tiempos quanta.	La configuración es bastante completa configurando tiempos quanta y filtrado de mensajes.	El tiempo de configuración fue el doble en comparación al grupo A.
No se necesitan amplios conocimientos de lenguaje C.	No se puede eficientar los procesos del microcontrolador, ya que varias funciones ya están preterminadas.	Se puede eficientar varios procesos del micrcontrolador, ya que el alumno define funciones y estructuras, dependiendo a sus necesidades.	El alumno necesita tener un conocimiento solido del lenguaje C.
No se necesita programador externo.	El uso del Shield para poder comunicarse con CAN-BUS, así como el de un protoboard, ya que el Shield no cuenta con bornera.	Necesita programador externo.	El Shield tiene todo lo necesario para establecer comunicación CAN-BUS.
	El alumno no comprende en su totalidad todos los parámetros del CAN-BUS, e incluso del mismo Arduino.	El alumno comprende en su totalidad todos los parámetros del CAN-BUS, e incluso del mismo ARM-Cortex M0, asi como las ventajas que ofrece.	

7 Conclusiones

En base a las pruebas realizadas se considera que el Shield es funcional, ya que, permite la interacción con cualquier dispositivo que disponga CAN-BUS, así también, con cualquier tarjeta de desarrollo, sensor y actuador, que disponga de los protocolos ya mencionados (I2C, SPI, RS-232 y CAN). Con el respaldo de la prueba realizada en el Jetta Hybrid, da garantía, al Shield, de realizar comunicación con los diversos dispositivos que posee internamente un automóvil, considerando que, estén interconectados a una red CAN-BUS.

Cabe recalcar, que las diferentes marcas de vehículos, usan diferentes estándares para la implementación de una red CAN-BUS, contemplando esto, los identificadores y códigos varían dependiendo la compañía del auto. Añadiendo, el CAN-BUS es un protocolo ideal para comunicaciones donde la información no puede ser errónea y malinterpretada, por lo tanto, es usado en la ingeniería aeroespacial y en medicina. Es por ello que se le plantea al usuario una revisión más a fondo del protocolo y del microcontrolador para sacar el máximo provecho del Shield.

Se tiene considerado hacer mejoras al diseño, tales como: incluir un microcontrolador que trabaje a mayor frecuencia y pueda manejar comunicación USB para la realización de prácticas con interfaz gráfica hacia la computadora, sin necesidad de usar un convertidor, además de estar ser la fuente de alimentación principal.

Crear compatibilidad con “Arduino”, para ser usado a través de las bibliotecas que dispone, para CAN-BUS, así ampliando numerosamente el mercado del Shield, de manera que, el usuario no necesite grandes conocimientos del microcontrolador, ni del protocolo CAN-BUS, solo use las funciones ya diseñadas.

Referencias

1. Miguel Ibáñez Galindo. *Integración de un sistema para la obtención de datos de vehículos automotrices basados en los protocolos CAN-BUS y OBD-II*. Tesis de maestría, Universidad Nacional Autónoma de México, 2015.
2. *The Definitive Guide to ARM® CORTEX®-M3 and CORTEX®-M4 Processors*. Elsevier, 2014.
3. ——. (2017). *Parque vehicular*. INEGI. [Online]. Disponible: <https://bit.ly/2QnbYGQ>. (Consultado el 30/05/2019).
4. Toni_K. (2015, Oct.) *CAN-BUS Shield Hookup Guide*. Spark Fun Electronics. [Online]. Disponible: <https://bit.ly/2wrLckf>. (Consultado el 30/05/2019).
5. ——. *Can-bus shield for arduino (assembled)*. RobotDyn. [Online]. Disponible: <https://bit.ly/2KgVDz1>. (Consultado el 30/05/2019).
6. ——. *Teensy 3.2 can bus and lin bus breakout board*. COPPERHILL technologies. [Online]. Disponible: <https://bit.ly/2wvI3jI>. (Consultado el 30/05/2019).
7. ——. *dsPIC33EV 5V CAN-LIN STARTER KIT*. [Online]. Disponible: <https://bit.ly/2MfqvCR>. (Consultado el 30/05/2019).
8. J.-S. Jhou, S.-H. Chen, W.-D. Tsay, and M.-C. Lai, “The implementation of OBD-II vehicle diagnosis system integrated with cloud computation technology,” in *2013 Second International Conference on Robot, Vision and Signal Processing*. IEEE, dec 2013.
9. C. ELLIOTT, V. VIJAYAKUMAR, W. ZINK, and R. HANSEN, “National instruments LabVIEW: A programming environment for laboratory automation and measurement,” *Journal of the Association for Laboratory Automation*, vol. 12, no. 1, pp. 17–24, feb 2007.
10. *STM32F0x1/STM32F0x2/STM32F0x8 advanced ARM®-based 32-bit MCUs*, Revision 9, STMicroelectronics, Enero. 2017.

Seguridad Mediante un Plan de Auditorías

Héctor Joab Ibarra Caballero, Ana Claudia Zenteno Vázquez, María del Carmen Santiago Díaz, Gustavo Trinidad Rubín Linares
Facultad de Ciencias de la Computación, BUAP
14 sur y Av. San Claudio, Jardines de San Manuel,
Puebla, México
{joab.hector, anaclau.zenteno, mcsantiagodiaz, gtrubin}@gmail.com

Resumen. La seguridad se ha convertido en un proceso dentro del desarrollo de las aplicaciones web que ha tomado importancia en los últimos años, Laravel provee características de seguridad a los desarrollos de aplicaciones web. En este trabajo se usan herramientas de análisis de vulnerabilidades para evaluar la seguridad y comprobar la eficiencia del desarrollo de software obteniendo como resultado un plan de auditoría sugerido para mitigar las vulnerabilidades: caso de estudio sobre una aplicación web.

Palabras Clave: Laravel, Aplicaciones Web, Auditorías, ZAP, Burp Suite

1 Introducción

Los planes de auditoría en seguridad son una serie de pruebas de penetración y análisis de vulnerabilidades que tiene como objetivo evaluar la seguridad y las posibles vulnerabilidades de diseño, falta de configuraciones adecuadas o establecidas por defecto, la carencia de validaciones en un sistema, etc. Una evaluación de vulnerabilidades proporciona una amplia visión sobre las fallas existentes en los sistemas.

Los actuales modelos de seguridad implementados por las compañías durante los procesos de desarrollo y liberación de una aplicación web lleva a solucionar las fallas de seguridad desarrollando parches a sus sistemas en base a los reportes de fallos. En la Fig. 1 se observa que este tipo de prácticas son consideradas por los especialistas de la seguridad como una práctica ineficaz ya que existe una ventana de vulnerabilidad y explotación entre los tiempos que se descubre la falla, se crea y envía el reporte, para después notificar al usuario de la falla, generar un análisis de la falla, crear el parche, la posterior liberación del parche, para finalizar con la instalación. Es por estas prácticas que en la actualidad se ve un incremento en los reportes de fallas en seguridad de los sistemas de las empresas y otros organismos. En un reporte del “*El financiero*” menciona que *México es la segunda nación en Latinoamérica que se ha visto afectada por el cibercrimen y a nivel mundial se encuentra en los 10 países con mayores daños por este fenómeno, lo que representa pérdidas por 3 mil millones de dólares anuales*[1].



Fig. 1. Ventana de Vulnerabilidad; OWASP Testing Guide V4 [2]

Por otro lado, la seguridad web está definida como el conjunto de procedimientos, prácticas y herramientas tecnológicas para la protección web, servidores, usuarios y organizaciones. [3] Las pruebas de penetración son una serie de ejercicios en seguridad donde se busca identificar las vulnerabilidades de un sistema, fallas en seguridad que podrían ser aprovechadas durante un ataque cibernético, ataque cibernético es un acto intencional por parte de un usuario malicioso con el fin de aprovecharse de una vulnerabilidad en el diseño de una aplicación con el fin de explotar estas fallas, la explotación consiste en la elaboración o implementación de herramientas que aprovechan la falla encontrada para obtener un beneficio, que van desde el robo de información hasta la pérdida en el control del sistema. En la Fig. 2 podemos observar de forma gráfica el proceso de una prueba de penetración, que parte desde el análisis del sistema web a sus diferentes métodos o funciones en búsqueda de alguna vulnerabilidad, para la posterior explotación y aprovechamiento del sistema mediante herramientas, al establecer que un sistema cuenta con la seguridad web adecuada es probable que un ataque cibernético no pueda causar algún impacto en el sistema evitando la explotación del mismo.

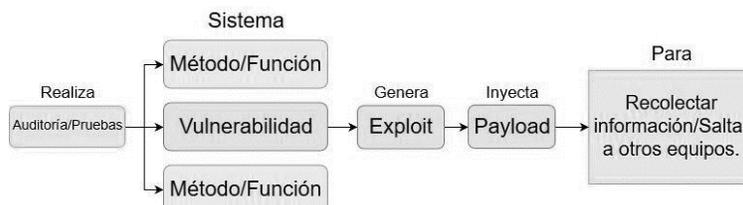


Fig. 2. Ejemplo de un ataque cibernético

1.1 Herramientas para la detección de vulnerabilidades

Para equipos de desarrollo que no tienen la suficiente experiencia ni conocimientos en realizar pruebas de penetración de forma manual se recomienda el uso de herramientas automáticas especialistas en estos temas que cumplan con alguno plan de auditorías profesional, por ejemplo, OWASP Testing Guide V4, así como también brindan al evaluador la posibilidad de presentar los resultados de forma que personas sin conocimientos en seguridad puedan entender. OWASP ZAP y Burp Suite trabajan bajo

las normativas de seguridad de OWASP por lo que se recomienda su uso dentro de los equipos de desarrollo.

OWASP Zed Attack Proxy Project (ZAP) es una aplicación liberada de forma gratuita que trabaja con un proxy de intercepción, lo que nos permite realizar pruebas activas y pasivas a la aplicación web, cuenta con un escáner automático de vulnerabilidades que permite tener un resultado aproximado de las fallas encontradas dentro de una aplicación web.

Burp Suite es otra herramienta para el análisis de vulnerabilidades, cuenta con funciones para conocer las vulnerabilidades encontradas dentro del sistema. Es un programa complejo con una consola que nos permite ver, editar y enviar los mensajes interceptados con el proxy, así como enviar partes de los mensajes interceptados a otras herramientas dentro de Burp Suite para obtener una evaluación más completa de la aplicación web.

El framework Laravel permite el desarrollo de aplicaciones web seguras, es objeto de este artículo, conocer el grado de cumplimiento de estos estándares de seguridad. Comentaremos sobre la aplicación web desarrollada en Laravel con fines de pruebas para realizar el escaneo de vulnerabilidades utilizando las herramientas ZAP y Burp Suite. En la sección dos se describe la estructura de desarrollo de aplicaciones seguras propuesta por Laravel. En la sección 3 se describe el plan de auditorías para analizar la aplicación desarrollada, y en la sección 4 se muestran conclusiones y trabajo futuro.

2 Desarrollo de Aplicación en Laravel

Es de conocimiento general que el uso de los distintos Framework y metodologías del desarrollo nos facilitan los procesos de desarrollo. Para determinar qué tan seguro es usar un Framework en un proyecto y por qué es necesario evaluar la seguridad de las aplicaciones web se propone analizar la seguridad y las herramientas de desarrollo que provee el Framework Laravel. En la Fig. 3 se muestra cómo se realizó una instalación pura del Framework utilizando la distribución Debian 8, además de los componentes necesarios para utilizar Laravel.

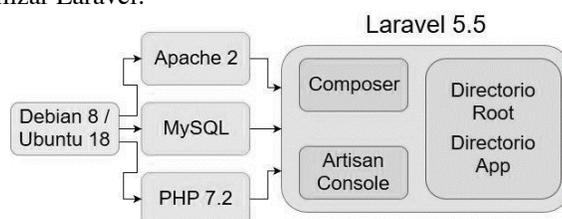


Fig. 3. Entorno de trabajo para Laravel Framework en Debian 8/Ubuntu 18

2.1 Estructura de la aplicación

La mayoría de los servicios web en línea trabajan con un sistema de entrada y registro dentro de sus estructuras principales, por lo que durante el desarrollo de nuestro proyecto se crearon vistas básicas y se usan las diferentes herramientas proporcionadas por Laravel para realizar una aplicación segura, así como añadir funciones para validar la información recibida. En la Fig. 4, se muestra estructura de la aplicación siguiendo las recomendaciones de desarrollo propuestas por Laravel, el esquema Ruta, Modelo, Vista, Controlador (RMVC).

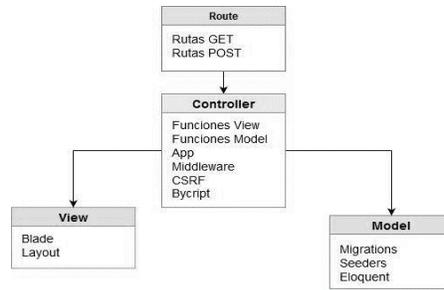


Fig. 4. RMVC de la aplicación web usando Laravel

Dentro de las rutas declaradas en el sistema podemos encontrar dos tipos de peticiones, las peticiones tipo GET son las que retornan las vistas de los formularios al usuario, mientras que las peticiones de tipo POST que realiza llamadas al controlador para la modificación y actualización del modelo. Para el desarrollo con formularios se incluyen *token csrf*, que permiten la validación de entrada y salida, donde es posible comprobar que no se incluya código javascript o sql. También se recomienda el uso de token de sesión el cual se mantiene hasta que el usuario cierra la sesión actual.

3 Plan de auditoría

Se propone un plan de auditoría con una serie de pruebas de penetración para analizar vulnerabilidades en la aplicación desarrollada basado en los 11 puntos principales de la seguridad web de la OWASP Testing Guide V4:

1. Recopilación de Información
2. Gestión de Configuración e Implementación
3. Gestión de identidad
4. Autenticación
5. Autorización
6. Gestión de Sesión
7. Validación de entrada
8. Manejo de errores
9. Criptografía
10. Lógica de negocios
11. Lado del Cliente

3.1 Mapeo de aplicación

Consiste en hacer una navegación manual de la aplicación web que se desea evaluar, para realizar un mapeo del sitio de forma pasiva se utiliza con Burp Suite. Este tipo de exploración dentro de la aplicación nos ayuda a tener un panorama de cómo responde el sistema, muestra las peticiones que trabaja, los tipos de entradas que recibe y la tecnología que usa. Burp Suite muestra un árbol de navegación con las carpetas y archivos a los que se han accedido por esta navegación.

ZAP crea un mapa del sitio al hacer una exploración activa con el escáner, donde podemos obtener distintas rutas como archivos a los cuales se puede acceder y evaluar.

3.2 Seguridad de Métodos de entrada y salida de datos

Es conveniente evaluar los distintos escenarios en los métodos de entrada y salida de la aplicación, agregando campos no esperados a los formularios del sitio para ver su respuesta. Un Spider (herramienta automatizada creada para el reconocimiento y mapeo de sitios web) puede ayudar a recorrer cada uno de los formularios.

3.3 Seguridad en las sesiones

Pruebas masivas de ingreso en los campos de usuario y contraseña son vulnerados cuando no se define un límite de intentos fallidos con ataques de fuerza bruta. Los inicios de sesión con guardados en tokens que suelen usar cifrado hash o valores hexadecimales y pueden ser descifrados con la herramienta decoder de Burp Suite.

Auditar consultas a las bases de datos con plugin CO2 de Burp suite para intentar hacer inyecciones SQL muestra si el sitio ha sido asegurado o no.

Además, ZAP realiza pruebas de activas y pasivas de vulnerabilidades sobre las generalidades del sitio como errores en los encabezados, manejo de cookies, protección del navegador deshabilitada, entre otras.

4 Conclusiones y trabajos futuros

En este trabajo concluimos que es recomendable utilizar un Framework del lado del servidor (Back-End), ya que facilita la incorporación y uso de herramientas que nos permiten generar aplicaciones web seguras. Herramientas que incluyen el cifrado de contraseñas, validación de datos de entrada a la base de datos, etc. Después de evaluar las herramientas que utiliza Laravel Framework llegamos a la conclusión que éste es un Framework que cubre los requisitos básicos de seguridad, mediante sus herramientas y su metodología de desarrollo RMVC. Las funciones del Framework se encuentran bien documentadas y son fáciles de usar, por lo que se recomienda trabajar con Laravel Framework en proyectos profesionales de desarrollo web. ZAP es una herramienta útil para el análisis de vulnerabilidades, proporciona información de la falla y cómo puede solucionarse facilitando la corrección de errores. Burp Suite es una herramienta compleja, puede ayudarnos a encontrar vulnerabilidades más específicas y complejas de una aplicación Web así como proporcionarnos las herramientas para la explotación de la vulnerabilidad. Juntas estas dos herramientas nos permiten generar reportes de seguridad basados en análisis de vulnerabilidades. Finalmente se propone un plan de auditorías basado en realizar dos pasos, primero implementar el uso de ZAP para la evaluación mediante el escáner activo de vulnerabilidades y evaluar los resultados con las más comunes fallas en seguridad en una aplicación web listadas en OWASP Top 10 The Ten Most Critical Web Application Security Risks. El segundo paso es usar Burp Suite e implementar el uso del proxy para evaluar las peticiones a aplicación web, la función de la herramienta Spider nos ayuda a obtener un mapeo completo del sitio, permitiendo la búsqueda de errores de diseño. El uso de algoritmos de fuerza bruta que se incluyen en el programa permite evaluar la seguridad de los controladores y las herramientas de sesión. Como trabajo futuro es posible realizar un proyecto de investigación donde se apliquen planes de auditoría a los diferentes Framework basados en diferentes lenguajes de programación, incluyendo pruebas a los entornos de trabajo en donde son almacenadas las aplicaciones web, además de realizar comparaciones entre los distintos Framework. Proponer nuevos planes de auditoría basados en distintas herramientas en pruebas de penetración y metodologías para el análisis de vulnerabilidades, así como crear manuales para el uso de distintas herramientas de penetración

Referencias

1. Brian Hatch & James Lee (2003). *Hackers en Linux. Secretos y Soluciones para la Seguridad del Linux* 2 Edición. España: McGraw Hill.
2. Pecoraro C. (2015) *Mastering Laravel*, Packt Publishing.
3. Negus C. (2015) *Linux Bible* Eighth Edition, John Wiley & Sons, Inc.
4. Spafford G.(2001) *Web Security, Privacy & Commerce* 2nd Edition, O'Reilly Media Inc
5. Niederst J. (2012). *Learning Web Design* Fourth Edition, Canada, O'Reilly Media, Inc.
6. Stauffer M. (2016) *Laravel: Up and Running: A Framework for Building Modern PHP Apps*, O'Reilly Media.
7. Bean M. (2015) *Laravel 5 Essentials*, Packt Publishing.
8. Offensive Security OSCP (2019). *OWASP Testing Guide V4* Extraído de https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
9. Pastor O. (2010). *Aplicaciones Web , Un enfoque práctico*, Editorial Omega.
10. Kim P. (2015). *The Hacker Playbook 2: Practical Guide to Penetration Testing*, Secure Planet LLC.
11. Hertzog R. (2015) *The Debian Administrator's Handbook*.

Desarrollo de un Descriptor Invariante a la Rotación Basado en HOGs para Detección de Puntos de Interés en Radiografías de Manos.

Mauricio Longinos Garrido ¹, Salvador Eugenio Ayala Raggi ¹, Alba Maribel Sánchez Gálvez ² Ricardo Álvarez Gonzales¹

¹ Facultad de Ciencias de la Electrónica, ² Facultad de Ciencias de la Computación,
Benemérita Universidad Autónoma de Puebla,
Av. San Claudio y 18 sur, Col. Jardines de San Manuel, C.P 72570 Puebla, Puebla, México
{longinos.200918526, saraggi, algor7691} @gmail.com
albadifusa@gmail.com

Resumen. En el área de visión por computador resulta esencial poder identificar características en las imágenes, la mayor parte del tiempo se implementa un algoritmo que define puntos de interés ó *landmarks* de forma automática, tal es el caso de algoritmos como SIFT en donde se eligen como puntos de interés los denominados blobs, secciones de imagen con niveles de gris similares. Pero en ocasiones puede resultar de utilidad el seleccionar de manera manual cuáles serán estos puntos. En el presente artículo se propone un modelo de descriptor invariante a la rotación basándose en histogramas de gradientes orientados (HOG) una posterior evaluación implementando análisis de componentes principales o PCA.

Palabras Clave: Procesamiento de Imágenes, HOGs, *Landmarks*, Análisis por Componentes Principales, PCA.

1 Introducción

La localización de puntos de interés seleccionados de forma manual en imágenes no resulta muy común, ya que normalmente se emplean mecanismos para procesar grandes volumen de datos de manera automática, es aquí cuando la implementación de algoritmos de detección de puntos de interés, o características, como: SIFT [3] y descriptores basados en HOGs [2] juegan un papel importante, en contraste, cuando se pretende encontrar algún punto específico en una imagen, el cual puede no contener características relevantes para los algoritmos antes mencionados, por lo que podría resultar más desafiante la ubicación de los puntos deseados a partir de las características obtenidas. Es por esto, que se desea proponer un descriptor capaz de reconocer secciones de imagen que puedan ser seleccionadas por el usuario y reconocidas dentro de otras imágenes.

El presente trabajo surge como requerimiento del área de la salud, en donde, por medio de radiografías de manos se realiza una estimación de la edad ósea, esto con el fin de poder detectar padecimientos congénitos en los pacientes, los cuales, de ser detectados con suficiente anticipación podrían ser tratados para reducir sus efectos. Actualmente se utilizan métodos manuales, en donde expertos, realizan una comparación directa de características de las radiografías, de las cuales, las secciones de las articulaciones son las que aportan mayor información para la determinación de la edad ósea, ya que el desarrollo y desgaste del cartílago nos proporciona una mejor aproximación de la edad del individuo.

Debido a la extensión del problema antes mencionado, la presente publicación se limitará a proponer y probar un modelo de descriptor que pueda ser invariante a la rotación, así mismo cabe destacar que la aplicación de este descriptor no se restringe al uso en radiografías, ya que su implementación en otros campos podría ser beneficiosa.

2 Antecedentes

En la publicación [1] Banda et al. presentan un método para el cálculo de la edad ósea utilizando regresiones basadas en el algoritmo K-NN, aquí se describe un método para detectar los puntos de interés, el cual consiste en alienar secciones cuadradas de la imagen de acuerdo al histograma de gradientes, una vez hecho esto se procede a la proyección de estas secciones en un eigen-espacio, el cual se crea a partir de los puntos de interés que conforman el set de entrenamiento, esto se logra por medio del algoritmo PCA. Una vez hecho esto, se obtiene una medida de similitud, según la cual se puede determinar si la imagen proyectada tiene características similares a las secciones de imagen almacenadas en la etapa de entrenamiento.

En “Histogram of Oriented Gradients for Human Detection” [2], se establece un descriptor basado en HOGs, estos se utilizan en conjunto con máquinas de soporte vectorial o SVMs para realizar la detección de humanos en fotografías. En este artículo se menciona una comparación con algunos métodos como SIFT [3] y contexto de formas [4], se menciona también que estos métodos trabajan sobre rejillas de celdas densas uniformemente espaciadas y utilizan metodologías de normalización local del contraste superponiendo las celdas, para mejorar el desempeño, pero plantean el uso de las SVMs por su simplicidad y velocidad.

En “Multiscale Histogram of Oriented Gradient Descriptors for Robust Character Recognition” [5], se demuestra que combinando descriptores HOG a diferentes escalas se puede mejorar el desempeño de reconocimiento de caracteres, este trabajo, en parte se basa en “Scale Space Histogram of oriented gradients for human detection” [6] He et al., en donde se demuestran que combinando descriptores HOG a diferentes escalas en una misma codificación, el desempeño puede ser mejorado en el contexto de detección de personas, de manera similar en “A multi-scale generalization of the HOG and HMAX image descriptors for object detection” [7] Bileschi presenta dos esquemas de extensión de HOGs, en el primero se extiende los histogramas a través del espacio de escalas, mientras que en el segundo combina pares de gradientes a diferentes escalas para formar lo que llama una columna de gradientes orientados, similar a lo que se abordará en esta publicación.

En otros trabajos como [8] los descriptores consisten en proyecciones de imágenes de gradientes que se realizan a bases adquiridas de las imágenes de entrenamiento utilizando PCA.

3 Desarrollo

En esta sección se describe la metodología implementada para la realización de este proyecto, como paso inicial, se realizó la propuesta del descriptor, posteriormente se implementó en un proceso similar al descrito en Banda Et all[1] con el fin de probar su viabilidad. Dentro de la etapa de prueba se distinguen tres partes, la primera, que consta del tratamiento de las imágenes, previo a poder ser procesadas, denominada preprocesamiento, posterior a este paso procedemos al entrenamiento, en el cual se acumularán regiones etiquetadas previamente para la extracción de sus descriptores y posteriormente construir los denominados eigen-espacios del algoritmo PCA[9],[10],[12], finalmente se realiza la clasificación, la cual comienza con el mismo tratamiento de la imagen tal como en el preprocesamiento y posteriormente se extraerán porciones de esta, que serán proyectadas a los eigen-espacios creados en el entrenamiento para encontrar el punto que más se parezca a los elementos del espacio seleccionado.

3.1 Propuesta de descriptor

En el algoritmo propuesto, con el fin de cumplir con la característica de ser invariante a la rotación, se propone que cada sección de imagen que se pretenda clasificar, debe ser rotada de acuerdo a su ángulo dominante, tal como en Banda et al.[1], en donde se realiza una gráfica polar del histograma de gradientes, para posteriormente realizar una suma de las componentes dentro de un rango de tamaño fijo, que para este caso es de 90° con esto se logra una gráfica más uniforme y se facilita la apreciación de un ángulo dominante.

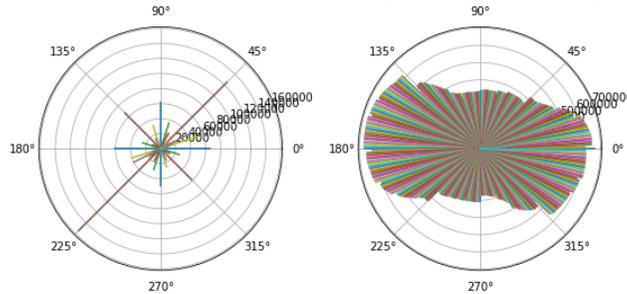


Fig. 1. Histograma de gradientes polar (izquierda), sumatoria de componentes del histograma de gradientes polar utilizando una ventana de 90° (derecha).

Ya que como se puede notar en las Fig. 1, el ángulo dominante tiene un ángulo contrario de magnitud similar, será importante localizarlo, por lo que una vez identificado el ángulo dominante se eliminará una porción de 180° centrado en el ángulo dominante encontrado, con lo que podremos ser capaces de distinguir un segundo ángulo dominante, como se muestra en la Fig. 2.

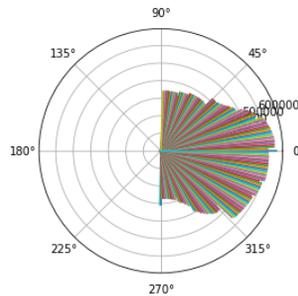


Fig. 2. Histograma de gradientes polar retirando los 180° alrededor del ángulo dominante detectado.

Una vez encontrados los ángulos mencionados, se hará uso del centro de masa de la imagen, el cual, nos servirá como discriminante, para seleccionar cualquiera de los dos ángulos anteriores como el ángulo dominante. Esto se logrará, realizando la proyección del vector que describe el centro de masa sobre los dos vectores de los ángulos dominantes Fig. 3.

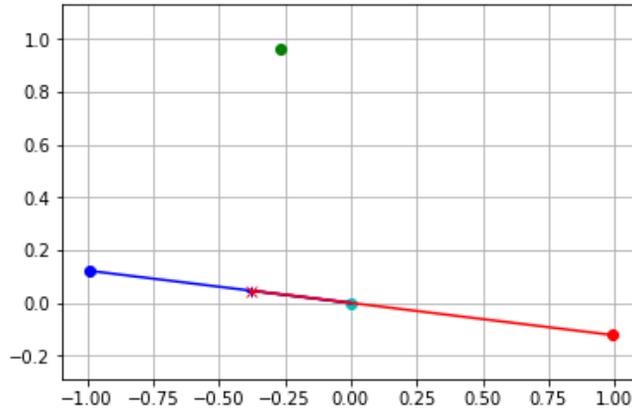


Fig. 3. Grafica de ángulo dominante (rojo), segundo ángulo dominante (azul), y centro de masa (verde) y representados con "x" las proyecciones del centro de masa sobre cada ángulo dominante.

Con lo anterior se pueden reducir errores de rotación a la hora de alinear las imágenes.

Se realizaron algunas pruebas para comprobar que la alineación de las imágenes era la correcta.

Una vez alienas las imágenes se procede a la extracción del descriptor, el cual, consta de 2 histogramas de gradientes normalizados y posteriormente concatenados, el primero describe la totalidad de los gradientes de la porción de imagen a evaluar, mientras que el segundo describe un área concéntrica menor dentro del primero, con lo que se pretende obtener una relación de cambio. Esto finalmente consiste en un vector de 270 elementos.

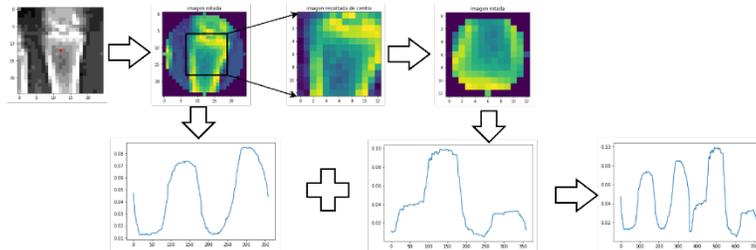


Fig. 4. Ilustración del proceso de extracción del descriptor.

Una vez obtenidos los descriptores, se realizaron pruebas para verificar que estos describieran partes similares de las imágenes, en estas pruebas se tomó un punto dentro de la imagen el cual corresponde a la parte superior del hueso metacarpiano, y se realizó la búsqueda de este por toda la imagen, obteniendo como resultado las coordenadas de las 20 porciones de imagen con un descriptor que se asemejan más al original, esto se repitió rotando el área de búsqueda, obteniendo resultados similares.

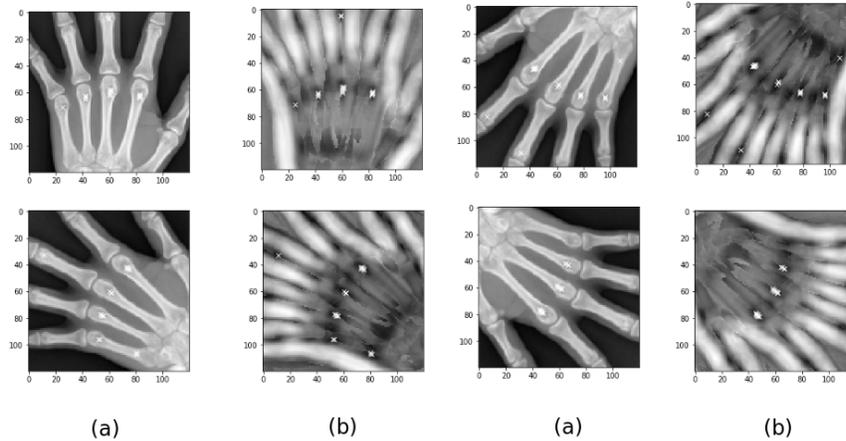


Fig. 5. Resultados de las búsquedas en secciones rotadas de la radiografía (a) ilustración del área de búsqueda. (b) ilustración de la gráfica de distancias del descriptor de cada sección de imagen al descriptor original, mostrando con "x" los veinte puntos más parecidos.

Una vez validado el modelo de descriptor procedemos a realizar una evaluación del desempeño de este similar al procedimiento descrito en Banda et all [1].

3.2 Preprocesamiento

Como primer paso para la evaluación, se tuvo que seleccionar la base de datos con la que se trabajaría, que para este caso se seleccionó la proporcionada por KAGGLE[11], la cual consta de 12.8K elementos con etiquetas de género y edad, desafortunadamente, las imágenes no cuentan con una ecualización adecuada y en ocasiones contienen marcos u otros objetos, por lo que se decidió partir del conocimiento previo de que todas estas imágenes contienen la radiografía de una mano, la cual es el objeto principal en cada una de ellas, partiendo de esta premisa, al calcular el centro de masa de los bordes en cada imagen nos situamos en un punto dentro de la mano, una vez obtenido dicho punto se extrae un recorte, de proporciones empíricas(60*60 píxeles), alrededor de dicho punto, para de este modo reducir el área de búsqueda.

3.3 Entrenamiento

Para este proceso se utilizaron 600 imágenes del set [11], en donde, por medio de una interfaz, se seleccionaron de forma manual puntos en los extremos del tercer metacarpiano como se muestra en Fig. 5, en base a estos puntos se calcularon los descriptores para cada sección de hueso.



Fig. 5. Colocación manual de landmarks.

Como se mencionó anteriormente para la extracción del descriptor se precisa rotar la imagen a su ángulo dominante, de modo que todas estas queden alineadas de la misma manera, para esto se utiliza el procedimiento descrito en la sección anterior, al procesar

las imágenes del set de entrenamiento se consiguieron resultados como los descritos en la Fig.6.

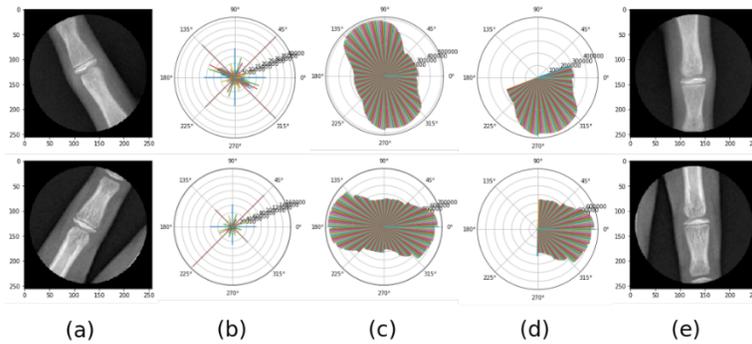


Fig. 6. Determinación del ángulo dominante, (a)Imagen de entrada, (b)Histograma de gradientes polar, (c)Histograma de gradientes después de aplicar la suma de sectores, (d)Mitad del plano donde se busca el segundo vector máximo, (e) Imagen rotada acorde a su ángulo dominante.

Una vez obtenidos los descriptores de cada punto de interés, son agrupados y evaluado en el algoritmo PCA[9],[10],[12], de este modo se crean eigen-espacios para la parte superior e inferior del hueso respectivamente.

4 Clasificación

Después de haber obtenidos los descriptores y sus respectivos eigen-espacios procedemos a realizar la búsqueda en las imágenes de prueba, las cuales forman parte del set [11], esto se realizó evaluando cada sección de la imagen, extrayendo su descriptor y posteriormente proyectarlo a cada eigen-espacio, a continuación se mide el error, el cual se considerará a partir de la distancia euclidiana de los pesos obtenidos de la proyección en los eigen-espacios contra la matriz de pesos obtenida en el entrenamiento, esta distancia se almacenará en un arreglo de las mismas dimensiones que el área de interés, finalmente se seleccionarán el punto con menor error, Fig. 7.

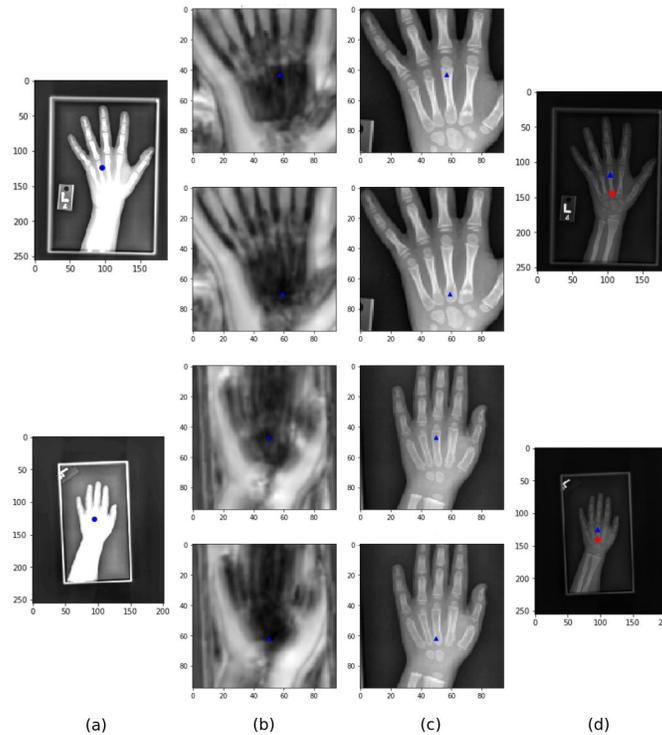


Fig. 7. Proceso de evaluación de radiografías en el algoritmo, (a) Imágenes de entrada normalizadas, con el centro de masa marcado con el punto azul, (b) Matriz de distancias con el mínimo marcado con un punto azul, (c) Ventana de la imagen evaluada marcando el mínimo con un punto azul, (d) Imagen original marcando los diferentes eigen-espacios con un triángulo azul y un círculo rojo respectivamente.

5 Resultados

Al aplicar el procedimiento descrito anteriormente se utilizaron 600 imágenes etiquetadas manualmente en las cuales se seleccionaron puntos extremos del tercer hueso metacarpiano, posteriormente se aplicó el algoritmo del PCA para la creación de los eigen-espacios, con esto se logró una reducción a solo 16 eigen-valores, con lo que se evaluaron las imágenes de prueba. Fig. 8.

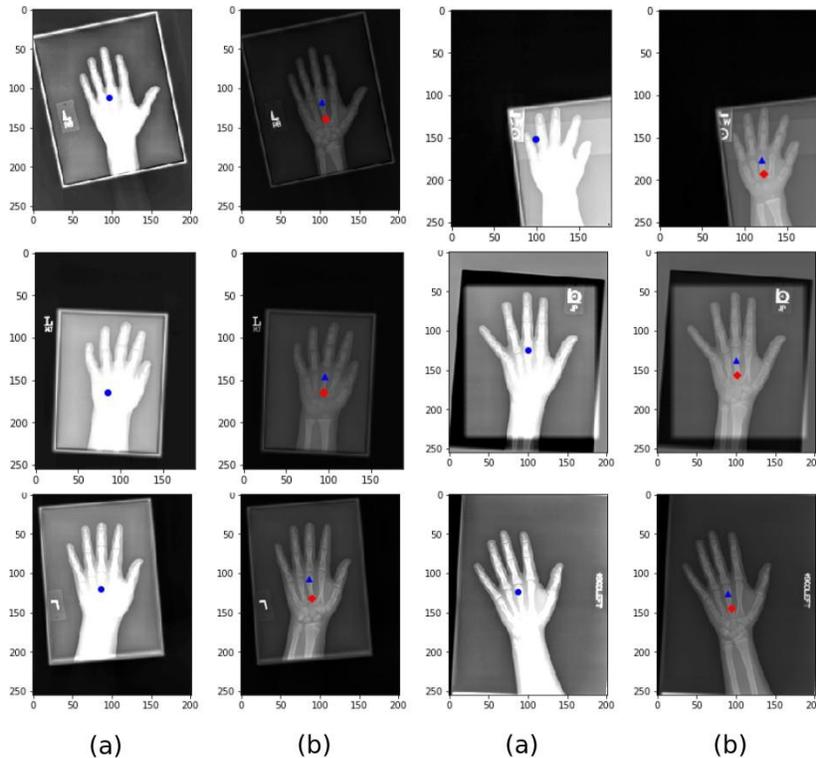


Fig. 8. (a)Imágenes de entrada posterior a la ecualización y centro de masa ilustrado con un punto azul, (b)Imagen con color original y señalización de ambos extremos del tercer hueso metacarpiano.

6 Conclusiones y trabajos futuros

Al aplicar el procedimiento antes descrito se redujo considerablemente el uso de memoria, no así el tiempo de procesamiento, ya que los algoritmos están escritos en lenguaje Python en alto nivel sin compilar en lenguaje de programación C.

Como se puede apreciar en las imágenes anteriores se obtuvieron resultados satisfactorios, en la evaluación de un gran número de las imágenes de prueba, será necesario cuantificar el error obtenido sobre el esquema actual y probar diferentes configuraciones del mismo para continuar mejorando el desempeño de este.

Agradecimientos

Agradezco a Jamid Israel Saenz por su apoyo y a mis asesores Salvador Eugenio Ayala y Alba Maribel Sánchez por sus comentarios y dirección en la realización de este proyecto.

Referencias

- 1 Banda,J.L.T.: Sistema automático de aprendizaje incremental supervisado para reconocimiento de la edad ósea. Benemérita Universidad Autónoma de Puebla, 2018.
- 2 Dalal N. and Triggs B.: Histograms of oriented gradients for human detection, 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA, 2005, pp. 886-893 vol. 1. doi: 10.1109/CVPR.2005.177
- 3 Lowe D. G.: Distinctive image features from scale-invariant keypoints. IJCV 60(2):91-110 2004.

- 4 Belongie S., Malik J. and Puzicha J.: Matching shapes. textitThe 8th ICCV Van- couver, Canada, pages 454-461 2001.
- 5 Newell A. J. and Gri n L. D.: Multiscale Histogram of Oriented Gradient Descriptors for Robust Character Recognition, 2011 International Conference on Document Analysis and Recognition, Beijing, 2011, pp. 1085-1089. doi: 10.1109/IC- DAR.2011.219
- 6 He N., Cao J. and Song L.: Scale space histogram of oriented gradients for human detection International Symposium on Information Science and Engineering - Vol. 02 pp. 167-170 2008.
- 7 Bileschi S.M.: A multi-scale generalization of the HoG and HMAX image descriptors for object detection. CSAIL Technical Report MIT-CSAIL- TR-2008-019 2008.
- 8 Ke Y. and Sukthankar R.: Pea-sift: A more distinctive representation for local image descriptors. CVPR Washington DC USA pages 66-75 2004.
- 9 Turk, M.; Pentland,A.: Eigenfaces for Recognition. Journal of Cognitive Neuro- science, vol. 3, no. 1, pp. 71-86, (1991).
- 10 Turk,M.;Pentland,A.: Face recognition using eigenfaces. International Conference on Pattern Recognition, pp. 586-591,(1991).
- 11 Mader, K.: RSNA Bone Age Predict Age from X-Rays. Kaggle. <https://www.kaggle.com/kmader/rsna-bone-age> (2017). Accedido el 28 de Mayo de 2019.
- 12 Jolli e,I.T.:Introduction: Principal Component Analysis. Springer, pp. 1-9 (2002).

Estudio de Algoritmos para la Detección de Rostros

Nayeli Pamela Perales Soto, Kenneth Mejía Pérez, Diana Margarita Córdova Esparza
Universidad Autónoma de Querétaro, Facultad de Informática,
Av. de las Ciencias S/N, Campus Juriquilla, Querétaro, Qro. México, C.P. 76230
naye.ps@outlook.com, ickennethmp@gmail.com, diana_mce@hotmail.com

Resumen. En este trabajo, se presenta una revisión bibliográfica de algoritmos existentes en la literatura para la detección automática de rostros mediante técnicas de Inteligencia Artificial. Se proporciona una tabla comparativa de los algoritmos donde específicamente se enfatiza en los datos utilizados, el tipo de técnica implementada, los principales resultados obtenidos, así como ventajas y desventajas. De acuerdo con la revisión, los algoritmos para la detección de rostros han aumentado significativamente siendo utilizados en diversas aplicaciones como seguridad, identificación, autenticación y reconocimiento de personas, entre otras. Muchos de los algoritmos revisados están basados en el método de Viola & Jones el cual presenta limitaciones en entornos no controlados. Métodos más recientes basados en redes neuronales profundas resuelven estas restricciones a expensas de un mayor costo computacional.

Palabras Clave: Detección de Rostros, Aprendizaje Automático, Visión por Computadora.

1 Introducción

1.1 Detección de rostros

La detección de rostros es una etapa esencial para el reconocimiento de rostros en imágenes digitales o video. Tiene diversas aplicaciones como el acceso a sistemas bancarios [1], identificación y autenticación de personas en dispositivos móviles [2], reconocimiento de expresiones faciales [3], lectura de labios [4], detección de puntos característicos que parte de la idea de localizar puntos clave en el rostro como lo son ojos, nariz y boca [5], entre otras. Sin embargo, para realizar estas aplicaciones se encuentran en la literatura diferentes métodos basados en aprendizaje automático. En la Fig. 1 se muestra un ejemplo de los resultados obtenidos para la detección de rostros.

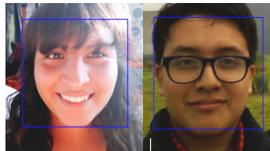


Fig. 1. Ejemplo sobre la detección de rostros de personas en imágenes.

1.2 Aprendizaje automático: supervisado y no supervisado

El aprendizaje automático es una técnica de la Inteligencia Artificial que enseña a las computadoras a aprender de la experiencia. Los algoritmos de aprendizaje automático utilizan métodos computacionales para "aprender" información directamente de los datos sin depender de una ecuación predeterminada. Los algoritmos mejoran su rendimiento de manera adaptativa a medida que aumenta el número de muestras disponibles para el aprendizaje [6].

El aprendizaje automático tiene por objetivo desarrollar técnicas de modelado por computadora para el análisis de datos como pueden ser documentos, imágenes, audio, etc., [7]. El modelo se refiere a la forma de generalizar un comportamiento a partir de la información. Para encontrar este modelo de forma automática se requiere de un proceso de inducción al conocimiento conocido como aprendizaje a través de una etapa de entrenamiento, como se muestra en la Fig. 2.



Fig. 2. Proceso del aprendizaje automático [7].

El aprendizaje supervisado que se refiere a entrenar un modelo con datos de entrada y salida conocidos, es decir, se utilizan datos que han sido etiquetados previamente para indicar cómo tendría que ser clasificada la nueva información o para predecir resultados futuros, este tipo de aprendizaje requiere de la intervención humana para proporcionar retroalimentación al entrenamiento y ajuste del modelo [8].

El aprendizaje no supervisado encuentra patrones ocultos o estructuras intrínsecas en la información [6]. Se utiliza para extraer inferencias de conjuntos de datos que no han sido previamente etiquetados, es decir el método por sí mismo tendría que buscar la forma de categorizar los datos, por lo tanto, no requiere de la intervención humana.

1.3 Técnicas basadas en aprendizaje automático

Existen diversas técnicas dentro de *Machine Learning* (aprendizaje automático) como se muestra en la Fig. 3.

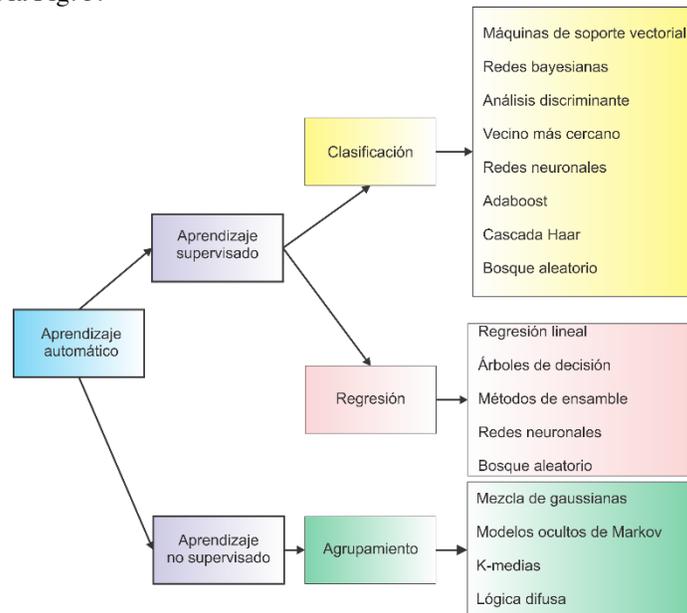


Fig 3. Técnicas de aprendizaje automático [6].

2 Metodología

En esta sección se describen los algoritmos para la detección de rostros que se seleccionaron para su análisis destacando sus principales características (ver Tabla 1).

Tabla 1. Tabla comparativa de algoritmos para la detección de rostros.

Título: <i>Robust Real-time Object Detection</i> Año de publicación: 2001 Autor y referencia: Viola & Jones [9]	
Datos utilizados	Se utilizaron 4916 imágenes de rostros (24x24 píxeles). Base de datos MIT-CMU.
Método	<ul style="list-style-type: none"> • Haar. • Imagen integral. • Selección de características basada en AdaBoost. • Clasificador en cascada.
Resultados	La imagen integral redujo considerablemente el tiempo de detección de objetos. El detector en cascada es 15 veces más rápido que el detector Rowley-Baluja-Kanade [10] y 600 veces más rápido que el detector Schneiderman-Kanade [11].
Ventajas	<ul style="list-style-type: none"> • Minimiza el tiempo de detección. • Bajo costo computacional. • Método robusto y eficiente para detectar rostros en tiempo real. • Gracias al entrenamiento puede usarse para detectar diferentes objetos. • La escala para detección no varía (24 x 24 px).
Desventajas	<ul style="list-style-type: none"> • Presenta una baja detección para rostros donde el ángulo de apertura es amplio (no se está viendo de frente). • Sensibilidad a cambios de luz. • Baja detección en imágenes de calidad deficiente.
Título: Aplicación de los diferentes espacios de color para detección y seguimiento de caras Año de publicación: 2003 Autor y referencia: C. Pérez , M. A. Vicente, C. Fernández, O. Reinoso, A. Gil [12]	
Datos utilizados	Se usaron imágenes de rostros denominadas <i>mug shots</i> las cuales son fotografías donde solo se ve un plano frontal del rostro, estas imágenes fueron tomadas con iluminación controlada y siempre a la misma escala.
Método	<ul style="list-style-type: none"> • En este sistema de visión se utilizó un detector mixto: para la detección de características y reconocimiento de patrones, el cual busca la región de interés (color de piel) y después utiliza un clasificador para determinar qué regiones corresponden a rostros y cuáles no (discrimina a los falsos positivos como lo serían manos, o cualquier otro objeto con un color similar de piel). • La red neuronal que se utiliza es un perceptrón multicapa con entrenamiento hessiano, basado en el algoritmo de Levenberg - Marquardt [13]. • Para el reconocimiento de caras se usan técnicas basadas en la proyección de las imágenes en diferentes subespacios, mediante análisis de componentes principales (PCA, por sus siglas en inglés) y análisis de componentes independientes, (ICA, por sus siglas en inglés).

Resultados	Basándose en el aprendizaje de la apariencia cromática (color de piel) se obtuvo un sistema capaz de reconocer rostros, con una aplicación en el seguimiento de caras.
Ventajas	<ul style="list-style-type: none">• Se realiza una adecuada segmentación de la región de interés (cara).
Desventajas	<ul style="list-style-type: none">• Solo se realizaron pruebas para <i>mug shots</i> (fotos vistas de frente).• Por sí sola la detección por espacios de color es deficiente, puede detectar falsos positivos (piel que podría corresponder a brazos, manos, etc.)• El color y contraste necesario para detectar varía según la etnia del sujeto y el lugar en donde se toma la foto.

Título: *FloatBoost Learning and Statistical Face Detection*

Año de publicación: 2004

Autor y referencia: Stan Z. Li and ZhenQiu Zhang [14]

Datos utilizados	Los datos que se usaron para la comparación de clasificadores débiles, falsa alarma y detección fueron imágenes de tamaño 20x20. Se recolectaron 5,000 imágenes de caras frontales de varias fuentes y 5,000 imágenes de no-caras. De cada conjunto se usaron 4,000 imágenes para entrenamiento y los 1,000 restantes para pruebas. Datos de comparación: Base de datos MIT-CMU, con 125 imágenes que contienen 481 caras.
Método	<ul style="list-style-type: none">• FloatBoost• AdaBoost
Resultados	FloatBoost tuvo una mayor tasa de detección. Los sistemas basados en FloatBoost requieren un menor número de clasificadores débiles en comparación con aquellos basados en AdaBoost. Se propone FloatBoost incorporando pirámide de detectores para la detección eficiente de varias caras en tiempo real.
Ventajas	<ul style="list-style-type: none">• Utiliza menos clasificadores débiles que los requeridos por AdaBoost.• FloatBoost logra una mayor detección.• Se realizan pruebas con rostros de frente y en diferentes ángulos.• La arquitectura del detector en pirámide acelera la detección de rostros en diferentes ángulos.
Desventajas	El tiempo de entrenamiento es cinco veces más en comparación con AdaBoost.

Título: Un nuevo método para la detección de caras basado en Integrales Difusas

Año de publicación: 2007

Autor y referencia: Antonio Rama, Francesc Tarres [15]

Datos utilizados	Se utilizó una base de datos propia compuesta de un total de 3325 imágenes de caras. Para los ejemplos negativos (no caras) se utilizaron más de 2000 imágenes de diferentes resoluciones que no incluyen caras.
Método	<ul style="list-style-type: none">• Redes neuronales.• Cascada de clasificadores basados en Integrales Difusas.• Haar.• Adaboost (comparación).

Resultados	En este artículo se hizo una comparación con el método AdaBoost como resultado se obtuvo que, las integrales difusas tienen una mayor tasa de éxito en las 4 etapas de la cascada.
Ventajas	<ul style="list-style-type: none"> • La cantidad de falsos positivos filtrados es muy baja desde la tercera etapa. • Para las pruebas realizadas, la detección en cascada es claramente superior en las primeras 4 etapas respecto a Adaboost.
Desventajas	<ul style="list-style-type: none"> • La tasa de detección es similar a la resultante con el algoritmo Adaboost.

Título: Detección de rostros en imágenes digitales usando clasificadores en cascada
 Año de publicación: 2008
 Autor y referencia: Guevara Marta Lucía, Julián David Echeverry and William Ardila Urueña [16]

Datos utilizados	Se utilizaron 50 imágenes de la base de datos FEEDTUM.
Método	<ul style="list-style-type: none"> • Imagen integral. • Extracción de características usando filtros Haar. • Clasificación en cascada.
Resultados	Se obtuvieron porcentajes de detección de 96% a 100%, en un corto tiempo de procesamiento por lo que el sistema se puede implementar en una aplicación en tiempo real.
Ventajas	<ul style="list-style-type: none"> • Altos porcentajes de detección de rostros. • Poco tiempo de ejecución.
Desventajas	<ul style="list-style-type: none"> • La eficiencia del algoritmo disminuye al hacer la detección de ojos. • Solo se realizan pruebas con imágenes de frente.

Título: Análisis y procesamiento de imágenes para la detección del contorno labial en pacientes de odontología
 Año de publicación: 2014
 Autor y referencia: César Osimani [17]

Datos utilizados	Se utilizó una red neuronal ya entrenada contenida en las librerías de Open CV, además de sus respectivos archivos XML, para detección de rostros frontales.
Método	<ul style="list-style-type: none"> • Clasificadores cascada Haar (para clasificadores débiles). • Utilización de clasificadores entrenados incluidos en la librería CascadeClassifier de OpenCV para C++ (clasificadores fuertes).
Resultados	Reducción del tiempo de procesamiento para imágenes cuando se utiliza una selección basada en reglas.
Ventajas	<ul style="list-style-type: none"> • Se utilizan aproximaciones a las regiones de interés (ojo izquierdo, derecho y boca), de esta forma se disminuye considerablemente el tiempo de procesamiento y aumenta la exactitud de la detección. • La elección del espacio de color Lab y el uso de las fórmulas correspondientes, logran que la detección sea independiente de la iluminación en el entorno y del color de piel que pueden tener distintas personas. • Selección de áreas de interés basada en reglas.

- Se determinan puntos claves para realizar el seguimiento de éstos, por lo que la cara puede tener cierta libertad de rotación.
- Desventajas
- El algoritmo está diseñado para funcionar en un ambiente controlado, con imágenes tomadas de una cámara web y para un entorno clínico.

Título: *A Convolutional Neural Network Cascade for Face Detection*

Año de publicación: 2015

Autor y referencia: Haoxiang Li, Zhe Lin, Xiaohui Shen, Jonathan Brandt, Gang Hua [18]

Datos utilizados	<p>Bases de datos usadas:</p> <ul style="list-style-type: none"> • <i>Annotated Faces in the Wild (AFW)</i> contiene 205 imágenes. • <i>Face Detection Data Set and Benchmark (FDDB)</i> [19]: contiene 2,845 imágenes y 5,171 caras.
Método	<ul style="list-style-type: none"> • Son 6 CNNs en cascada, 3 clasificadores de caras o no caras y 3 para la calibración del cuadro delimitador: <ul style="list-style-type: none"> → 12-net → 12-calibration-net → 24-net → 24-calibration-net → 48-net → 48-calibration-net
Resultados	Los clasificadores desechan las regiones sin rostro, centrándose en la precisión del cuadro delimitador del rostro, lo que hace que la detección de rostros sea rápida.
Ventajas	<ul style="list-style-type: none"> • Su tiempo de ejecución es mínimo. • Opera en múltiples resoluciones.
Desventajas	<ul style="list-style-type: none"> • Mayor costo computacional.

Título: Algoritmos de detección y seguimiento de rostro dirigidos a videojuegos

Año de publicación: 2016

Autor y referencia: Cuervo, Juan Camilo, and Daniel Alarcón [20]

Datos utilizados	<p>Para el tiempo de ejecución se usó un solo rostro en 10 iteraciones para cada algoritmo.</p> <p>Para la estabilidad de detección se usaron 3 rostros con diferentes características.</p> <p>Tono de piel: morena, blanca y trigueño.</p> <p>Tipo de rostro: ovalado y triangular.</p>
Método	<p>Algoritmos:</p> <ul style="list-style-type: none"> • Viola & Jones • Camshift • Kanade-Lucas
Resultados	El algoritmo Camshift obtuvo los mejores resultados, siendo el más estable y con un buen tiempo de ejecución.
Ventajas	<ul style="list-style-type: none"> • Usaron diferentes tipos de cámaras en las pruebas. • Se realizaron pruebas para determinar el tiempo de ejecución, estabilidad y rango de detección.

- Desventajas • Se utilizaron pocos datos para la validación de las pruebas.

Título: *Face Detection with the Faster R-CNN*

Año de publicación: 2017

Autor y referencia: Huaizu Jiang, Erik Learned-Miller [21]

Datos utilizados	Se utilizaron 2 bases de datos (<i>datasets</i>), primero se entrenó el algoritmo Faster R-CNN [22] utilizando la base de datos WIDER, haciendo uso de 12,880 imágenes y 159,424 rostros para el entrenamiento [23]. Se probaron los resultados con la base de datos FDDB [19], además también se entrenó el modelo de detección de rostros basándose en el modelo VGG16 de ImageNet [24].
Método	Para la comprobación del estado del arte sobre la detección de rostros utilizado Redes Neuronales Convolucionales Profundas (del inglés, <i>CNNs</i> , <i>convolutional neural networks</i>) usan los modelos: R-CNN, Fast R-CNN y Faster R-CNN.
Resultados	Como resultado final se demostró que los sistemas que se usaron <i>Faster R-CNN</i> , obtuvieron un mejor rendimiento en las pruebas realizadas, demostrando el mejoramiento del estado del arte en comparación a las generaciones pasadas.
Ventajas	<ul style="list-style-type: none"> • Mayor tasa de detecciones en comparación a los algoritmos anteriores (R-CNN, Fast R-CNN). • La cantidad de falsos positivos es menor en comparación a otros algoritmos comparados.
Desventajas	• Mayor costo computacional.

Título: *Survey of Face Detection on Low-quality Image*

Año de publicación: 2018

Autor y referencia: Yuqian Zhou, Ding Liu, Thomas Huang [25]

Datos utilizados	Base de datos: FDDB (<i>Face Detection Data Set and Benchmark</i>). Esta base de datos contiene 5171 caras en un total de 2845 imágenes [19].
Método	Para la evaluación de este estudio se utilizaron diversos métodos, los cuales se agrupan en: <p>Métodos clásicos:</p> <ul style="list-style-type: none"> • Viola-Jones [9]. • HoG-SVM [26]. <p>Métodos de aprendizaje profundo:</p> <ul style="list-style-type: none"> • Faster R-CNN [21]. • S^3FD [27].
Resultados	El propósito central de este estudio fue verificar la eficiencia de los métodos clásicos y los basados en aprendizaje profundo para la detección de rostros en imágenes de baja calidad, centrándose en imágenes con poco brillo, contraste, difuminación y ruido. Después de la implementación se realizó la comparación de los cuatro algoritmos, determinando que ninguno es lo suficientemente robusto para el reconocimiento de rostros en imágenes de baja calidad. Sin embargo, cabe mencionar que los algoritmos que tuvieron una mejor tasa de eficiencia fueron S^3FD y Faster R-CNN, respectivamente.

- | | |
|-------------|--|
| Ventajas | <ul style="list-style-type: none"> Realiza pruebas con imágenes con poco brillo y contraste, desenfoque y ruido. Demostrando que los métodos de aprendizaje profundo mejoran la tasa de detección bajo estas condiciones. |
| Desventajas | <ul style="list-style-type: none"> Los algoritmos clásicos no son lo suficiente robustos para realizar la detección de rostros en imágenes de baja calidad. |

Título: *Machine vision quality assessment for robust face detection*

Año de publicación: 2019

Autor y referencia: Rajiv Soundararajan, Soma Biswas, [28]

- | | |
|------------------|--|
| Datos utilizados | Imágenes con diversos tipos de distorsión (iluminación, contraste, ruido, etc.). |
| Método | <ul style="list-style-type: none"> Se utilizó el método de Viola & Jones para detectar rostros. Sin embargo, se aplicaron adaptaciones individuales para mejorar la calidad de la imagen tales como: MVQ, NIQE, y BRISQUE las cuales se explican a continuación: MVQ (<i>Machine vision quality</i>): Es una técnica para la evaluación de la calidad de imágenes, mediante algoritmos de detección. NIQE (<i>natural image quality evaluator</i>): es un índice genérico para la evaluación de la calidad de imágenes sin referencia, el cual se ha comprobado que se correlaciona con la detección de rostros [29]. BRISQUE (<i>The blind reference less image spatial quality evaluator</i>) es un método de calidad de la imagen basado en características extraídas utilizando estadísticas de escenas naturales. |
| Resultados | <p>La curva de PR (<i>precision-recall</i>) demuestra que, si se aplican técnicas para mejorar la calidad de la imagen, se optimiza el rendimiento en la detección en comparación con la aplicación directa del algoritmo de detección de rostros en imágenes distorsionadas.</p> <p>La mejora del rendimiento obtenida con MVQ, es mejor que la alcanzada con los índices de calidad perceptiva de NIQE y BRISQUE para el DPM (<i>deformable parts model</i>) y en los algoritmos de detección de rostros basados en el aprendizaje profundo, esto se representa gráficamente en la curva de PR.</p> |
| Ventajas | <ul style="list-style-type: none"> El mejoramiento de las imágenes previo al procesamiento, permite incrementar la tasa de la detección en imágenes con baja resolución o con algún tipo de distorsión. |
| Desventajas | <ul style="list-style-type: none"> El mejoramiento de la imagen conlleva un mayor costo computacional, para imágenes estáticas podría no representar un problema importante. Sin embargo, puede ser considerable para videos en baja resolución. |

Título: *Improved Viola-Jones face detection algorithm based on HoloLens*

Año de publicación: 2019

Autor y referencia: Jing Huang, Yunyi Shang and Hai Chen [30]

- | | |
|------------------|---|
| Datos utilizados | Para las pruebas se usaron varias bases de datos: OrL, Yale, Ar, Stanfords, Jaffe y Cit, con imágenes de rostros con diferentes características. |
| Método | <ul style="list-style-type: none"> Modificación de Haar, expansión de la característica del rectángulo. Imagen integral. AdaBoost. |

Resultados	La implementación del algoritmo de Viola & Jones con HoloLens disminuyó el tiempo de detección de rostros, modificándose de acuerdo al tamaño del rectángulo de Haar.
Ventajas	<ul style="list-style-type: none">• Las bases de datos usadas contienen imágenes variadas, diferentes expresiones, rostros con gafas, personas de nacionalidades diferentes, etc.• Aceleración y optimización del algoritmo.
Desventajas	<ul style="list-style-type: none">• Las imágenes tienen que ser de un tamaño específico por lo que se requiere previamente modificar la resolución para ejecutar el algoritmo.

3 Discusión

En este trabajo se analizaron 12 artículos referentes a la detección de rostros, descritos en la Tabla 1. Las principales observaciones de estos métodos, se presentan a continuación:

- a) El trabajo desarrollado por Soundararajan & Biswas [28], realiza una mejora en las imágenes con baja resolución o algún tipo de distorsión utilizadas para la detección de rostros, comprobando que el tratamiento de las mismas permite incrementar la tasa de la detección de rostros obtenida mediante un algoritmo clásico como el de Viola & Jones [9]. Sin embargo, en el artículo de Zhou, et al. [28] demuestra que los métodos de aprendizaje profundo como S^3FD y *Faster R-CNN* mejoran la tasa de detección en imágenes con dichas características.
- b) El algoritmo propuesto por Viola & Jones [9] es frecuentemente utilizado para comparar su efectividad con nuevas propuestas desarrolladas para la detección de rostros. Por ejemplo, mediante el uso de integrales difusas [15] y el clasificador mejorado FloatBoost [14], que buscan optimizar el tiempo de procesamiento y la tasa de detección.
- c) La base de datos FDDB (*Face Detection Data Set and Benchmark*), la cual contiene 5,171 rostros en un total de 2,845 imágenes es una de las más utilizadas por los métodos basados en aprendizaje profundo para la detección de rostros [18], [21] y [25].
- d) En los trabajos presentados por Li & Zhang [14] y Rama & Tarres [15] utilizaron imágenes que contienen rostros y otro tipo de objetos, para corroborar el desempeño de clasificadores mejorados con respecto al de Adaboost.
- e) Las investigaciones desarrolladas por Li et al. [18] y Jiang & Learned-Miller [21], hacen uso de redes neurales convolucionales para la detección de rostros, obteniendo con este método un mejor desempeño del algoritmo con respecto a la tasa de detección. Sin embargo, su implementación implica un mayor costo computacional.

4 Conclusiones y trabajos futuros

De acuerdo con la revisión de la literatura, se puede observar que un número considerable de los métodos consultados hace referencia al algoritmo propuesto por Viola & Jones [9], el cual se integra por el clasificador de cascada Haar y el meta-algoritmo de aprendizaje Adaboost.

En particular, los trabajos [15], [20] y [25] realizan una comparación del algoritmo de Viola & Jones [9] y otras técnicas. Mientras que [14], [16], [17], [28] y [30] buscan mejorar su rendimiento y/o precisión.

Como se puede observar, aun después de 18 años de su publicación el algoritmo de Viola & Jones [9], sigue siendo utilizado en la comunidad científica que busca mejorar el rendimiento en la detección de rostros. El algoritmo ha demostrado ser robusto para la detección en imágenes controladas (fotografías con rostros viendo al frente, contraste y

brillo controlado). Sin embargo, no es lo suficientemente robusto para todas las aplicaciones prácticas como lo podría ser la detección en cámaras de seguridad o en imágenes de baja calidad [28], o con algún tipo de distorsión [25] pudiendo mejorar estos aspectos, además de incluirse un ángulo de inclinación en el rostro más amplio.

Durante este tiempo, se ha realizado un esfuerzo para hacer más eficiente el algoritmo de Viola & Jones [9]. Sin embargo, existen otras opciones efectivas que presentan mejor rendimiento como lo son los métodos de aprendizaje profundo, en este caso S3FD [27] y Faster R-CNN [21], pero son computacionalmente más costosos. Se han revisado también otras propuestas interesantes para la detección de rostros como lo son: Integrales Difusas [15] y espacios de color [12].

Las bases de datos que se utilizaron en estos trabajos fueron:

- Fddb [19].
- WIDER [23].
- ImageNet [24].
- AFW.
- FEEDTUM.

Finalmente, se puede concluir que la detección de rostros ha sido un tema muy estudiado en años anteriores, pero aún puede mejorarse para ser funcional en entornos no controlados. Cada aplicación implica nuevos retos y, por lo tanto, crear un método general capaz de cumplir con todas las demandas representa una tarea complicada.

Agradecimientos. Los autores agradecemos por el apoyo brindado a la Universidad Autónoma de Querétaro (UAQ) mediante el proyecto FIF-2018-06.

Referencias

1. Albaloooshi, F. A.; Smith-Creasey, M.; Albastaki, Y.; & Rajarajan, M.: Facial Recognition System for Secured Mobile Banking. *KnE Engineering*, pp. 92-101 (2018)
2. Fathy, M. E.; Patel, V. M.; & Chellappa, R.: Face-based active authentication on mobile devices. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1687-1691 (2015)
3. Happy, S. L.; & Routray, A.: Automatic facial expression recognition using features of salient facial patches. *IEEE transactions on Affective Computing*, Vol. 6, No. 1, pp. 1-12 (2014)
4. Chung, J. S.; Senior, A.; Vinyals, O.; & Zisserman, A.: *Lip reading sentences in the wild*. In *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 3444-3453 (2017)
5. Ranjan, R.; Patel, V. M.; & Chellappa, R.: Hyperface: A deep multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 41, No. 1, pp. 121-135 (2017)
6. What is machine learning? 3 things you need to know. <https://www.mathworks.com/discovery/machine-learning.html>. Accedido el 06 de Marzo de 2019
7. Kim, P.: Matlab deep learning. *With Machine Learning, Neural Networks and Artificial Intelligence*, Vol. 130 (2017)
8. Rouhiainen, L.: *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*. Grupo Planeta (2018)
9. Viola, P.; Michael Jones.: Detección robusta de objetos en tiempo real. *Revista internacional de visión por ordenador*, pp. 137-154 (2001)
10. Rowley, H. A., Baluja, S., & Kanade, T.: Neural Network-Based Face Detection. *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 20, No. 1, pp. 23-38 (1998)
11. Schneiderman, H.; & Kanade, T.: *A statistical approach to 3D object detection applied to faces and cars*. Carnegie Mellon University, the Robotics Institute, pp. 0-6 (2000)
12. Pérez, C.; Vicente, M. A.; Fernández, C.; Reinoso, O.; & Gil, A.: Aplicación de los diferentes espacios de color para detección y seguimiento de caras. *Proceedings of XXIV Jornados de Automatica* (2003)

13. Hagan, M. T.; & Menhaj, M. B.: Training feedforward networks with the Marquardt algorithm. *IEEE transactions on Neural Networks*, Vol. 5, No. 6, pp. 989-993 (1994)
14. Li, S. Z.; & Zhang, Z.: Floatboost learning and statistical face detection. *IEEE Transactions on pattern analysis and machine intelligence*, Vol. 26, No. 9, pp. 1112-1123 (2004)
15. Rama, A.; & Tarrés, F.: Un nuevo método para la detección de caras basado en integrales difusas. *XII Simposium Nacional de la Unión Científica Internacional de Radio* (2007)
16. Guevara, M. L.; Echeverry, J. D.; & Urueña, W. A.: Detección de rostros en imágenes digitales usando clasificadores en cascada. *Scientia et technica*, Vol. 1, No. 38 (2008)
17. Osimani, C.: Análisis y procesamiento de imágenes para la detección del contorno labial en pacientes de odontología. En *2do Congreso Nacional de Ingeniería Informática y Sistemas de Información (CoNaIISI 2014)*, San Luis, Argentina (2014)
18. Li, H.; Lin, Z.; Shen, X.; Brandt, J.; & Hua, G.: A convolutional neural network cascade for face detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 5325-5334 (2015)
19. Jain, V.; & Learned-Miller, E.: Fddb: A benchmark for face detection in unconstrained settings (2010)
20. Cuervo, J. C.; & Alarcon, D.: Algoritmos de detección y seguimiento de rostro dirigidos a videojuegos. *U@ CSIS* (2016)
21. Jiang, H.; & Learned-Miller, E.: Face detection with the faster R-CNN. In *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, pp. 650-657 (2017)
22. Ren, S.; He, K.; Girshick, R.; & Sun, J.: Faster r-cnn: Towards real-time object detection with region proposal networks. In *Advances in neural information processing systems*, pp. 91-99 (2015)
23. Yang, S.; Luo, P.; Loy, C. C.; & Tang, X.: Wider face: A face detection benchmark. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 5525-5533 (2016)
24. Simonyan, K.; & Zisserman, A.: Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014)
25. Zhou, Y.; Liu, D.; & Huang, T.: Survey of face detection on low-quality images. In *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018)*, pp. 769-773 (2018)
26. Kazemi, V.; & Sullivan, J.: One millisecond face alignment with an ensemble of regression trees. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. pp. 1867-1874 (2014)
27. Zhang, S.; Zhu, X.; Lei, Z.; Shi, H.; Wang, X.; & Li, S. Z.: S3fd: Single shot scale-invariant face detector. In *Proceedings of the IEEE International Conference on Computer Vision*, pp. 192-201 (2017)
28. Soundararajan, R.; & Biswas, S.: Machine vision quality assessment for robust face detection. *Signal Processing: Image Communication*, 72, pp. 92-104 (2019)
29. Mittal, A.; Soundararajan, R.; & Bovik, A. C.: Making a Completely Blind Image Quality Analyzer. *IEEE Signal Processing Letters*, 20, pp. 209-212 (2013)
30. Huang, J.; Shang, Y.; & Chen, H.: Improved Viola-Jones face detection algorithm based on HoloLens. *EURASIP Journal on Image and Video Processing*, Vol. 2019, No. 1, p. 41 (2019)

Aprendizaje Supervisado para la Detección de Plagas y Enfermedades en los Cultivos de Aguacate

Marcos Emiliano López Pérez¹, Luis F Columna Álvarez²,
Guadalupe Michelle Ojeda Pérez³
Universidad Nacional Autónoma de México
Facultad de Ingeniería

¹lopezp.marcose@gmail.com, ²fernando_gearsof_95@hotmail.com, ³opmitch.g@gmail.com

Resumen. Se pierde aproximadamente un tercio de producción de aguacate debido a plagas y enfermedades, por lo que se diseñó un sistema que ayude a distinguir oportunamente este mal. Se hizo uso de un algoritmo de árbol de decisión de tipo ID3, donde se obtuvieron 20 reglas de derivación que permiten la predicción deseada con un porcentaje de error del 4.42%, se diseñó una aplicación que permite tener un diagnóstico oportuno, con lo que se logre disminuir el porcentaje de pérdida de cultivos de aguacate.

Palabras Clave: Árboles de Decisión, Plagas, Aguacate, Inteligencia Artificial.

1 Introducción

1.1 El aguacate

El aguacate es uno de los productos más exitosos de la exportación nacional. México es el principal proveedor con 45.95% del valor de las exportaciones mundiales. De acuerdo con la Asociación de Productores Empacadores y Exportadores de Aguacate de México (APEAM), durante el último medio año de 2017 se exportaron 353.517 toneladas de fruto fresco, tan solo a Estados Unidos, no solo se exporta a este país, si no, también a Canadá, Guatemala, el Salvador, España, Francia, Países Bajos, Japón, inclusive llega a países con los cuales no hay tratado de libre comercio [1].

Al ser uno de los principales productores de aguacate, y sobre todo exportadores, se tiene la responsabilidad de llevar productos de calidad y sin ninguna plaga o enfermedad. En la Figura 1 se muestra a los principales importadores mundiales de aguacate, donde se observa que Estados Unidos es el principal importador, dado que en el 2018 adquirieron cerca de 100 mil toneladas de aguacate mexicano [2].

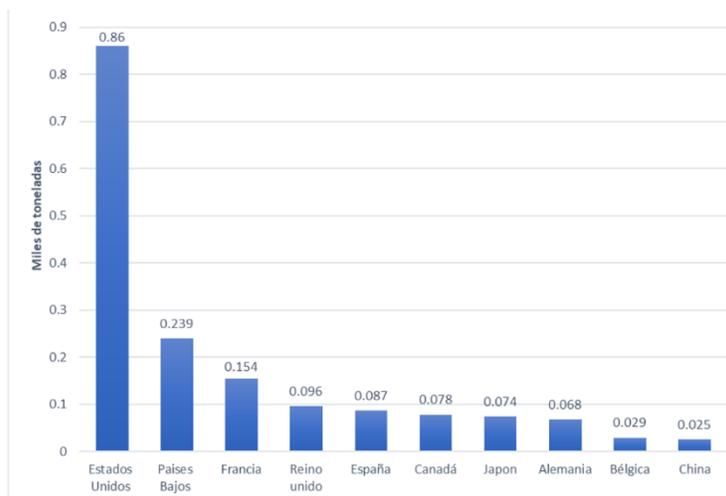


Fig. 1. Principales importadores de aguacate.
Fuente: Planeación agrícola nacional 2017-2030 SAGARPA.

La Figura 2 muestra una tabla del crecimiento promedio anual, con datos desde 2016 y una estimación hasta 2030. Esto demuestra que el área aguacatera tiene un amplio potencial, con lo que se pretende impulsar, además del crecimiento inercial estimado, con cuidado y buen aprovechamiento de la producción.

AÑO/PERIODO	ESTIMACIONES				CRECIMIENTO ACUMULADO				CRECIMIENTO PROMEDIO ANUAL	
	2016	2018	2024	2030	2003-2016	2016-2018	2016-2024	2016-2030	2003-2016	2016-2030
Producción Potencial (millones de toneladas)	1.89	2.05	2.61	3.16	1.0876	0.0874	0.2692	0.6728	5.82	3.49
Exportaciones (millones de toneladas)	1.02	1.17	1.65	2.14	7.2278	0.1415	0.4177	1.0904	0.176	0.0504
Valor de exportaciones (millones de dólares a precios del 2016)	2227.25	2542.44	3604.4	4655.78						

Fig. 2. Tabla de crecimiento anual.
Fuente: Planeación agrícola nacional 2017-2030 SAGARPA

De las estadísticas de la FAO (Organización de las Naciones Unidas para la Alimentación y la Agricultura) en el 2017, una de cada 10 personas enferma por consumir alimentos contaminados y muchas de las nuevas enfermedades son originados por estos cultivos contaminados. A nivel nacional México pierde el 30% de sus cultivos por plagas o por inundaciones. Si los cultivos no cumplen con ciertas normas no pueden ser comercializados lo que provoca pérdidas monetarias.

Para el aguacate las plagas reglamentadas que limitan la comercialización son: el barrenador de ramas del aguacate (*Copturus aguacatae*), cuyos daños provocan que las ramas se rompan con facilidad; el barrenador pequeño del hueso del aguacate (*Conotrachelus perseae* Barber), el barrenador grande del hueso del aguacate (*Heilipus lauri*); y la palomilla barrenadora del hueso (*Stenoma catenifer*), las cuales ocasionan daños en el fruto cuando las larvas se alimentan de la pulpa y del hueso, situación que afecta su rendimiento y puede provocar hasta un 90% de pérdidas si no se realizan acciones de control.

A pesar de que ya hay zonas libres de estas plagas en México, todavía hay estados donde el porcentaje es menor como Chiapas, Colima, Guanajuato, Guerrero, Jalisco, Michoacán, Morelos, Nayarit, Oaxaca, Puebla, Querétaro, Nuevo León, Estado de México, Hidalgo y Veracruz, por lo que, es importante el correcto manejo de cultivos, pero, sobre todo, identificar y dar alertas oportunas para realizar control de plagas correspondientes.

Durante la investigación realizada, se encontró que las principales plagas que afectan el cultivo del aguacate son las siguientes:

- Los Trips (*Heliethrips haemorrhoidalis*) son de particular importancia, debido a que en el pericarpio de la fruta atacada pueden provocar el desarrollo de protuberancias que reducen su calidad estética. El daño que provoca en el caso más extremo es la caída del fruto o heridas que permiten la entrada de enfermedades. Los daños se hacen más visibles conforme el fruto se desarrolla, ocasionando pérdida de calidad en su presentación.
- Barrenador Pequeño del Hueso (*Conotrachelus perseae* y *C. aguacatae*). Es una de las plagas más perjudiciales para el fruto. Provoca la caída de los frutos.
- Barrenador de Ramas (*Copturus aguacatae*). La larva se alimenta de madera de las ramas más jóvenes, de ahí parten las galerías en un desplazamiento paralelo a los tejidos y barrenando hasta el inicio de la pupación.
- Agallador del Aguacatero (*Trioza anceps* Tuthill). La ninfa es de color amarillo pálido. Para alimentarse se fijan en el haz de las hojas tiernas. Esto trae como consecuencia una debilidad general de la hoja, ya que en cada una de ellas suelen fijarse cientos de ninfas.
- Palomilla Barrenadora del Hueso (*Stenoma catenifer*). Recien reportada en México, por primera vez en el estado de Querétaro en el 2011, lo que abre nuevas consecuencias en el país.

1.2 Árboles de decisión

En inteligencia artificial hay varias maneras de solventar problemas de predicción, una que es muy útil a la hora de manejar aprendizaje automático es el uso de algoritmos de árboles de decisión, principalmente si se hace uso de valores nominales.

Un árbol de decisión es una forma gráfica o analítica de descripción de sucesos de forma escalonada que permite hacer un seguimiento paso a paso de éstos para obtener predicciones. Además, debido a su carácter gráfico son de fácil comprensión aun así con gran número de datos, ya que la naturaleza del algoritmo es “podar” las hojas que no representen información significativa.[4].

2 Antecedentes

En 1989, Julio Vecino Berbel escribió “La inteligencia artificial en la agricultura: Perspectivas de los sistemas expertos” [5], dio pie a que a partir de la década de los 80, se aplicara la inteligencia artificial y en específico una de sus ramas, sistemas expertos, el cual tiene lugar en una gran variedad de actividades humanas. Los sistemas expertos se han convertido en un instrumento poderoso y que posee un gran potencial diferentes áreas.

Una de estas áreas es la agricultura, y el futuro es nuestro presente, como lo demuestra Javier Montoya, que en 2015, con su libro “Intelligent System for plague control in crops”, confirma lo que Julio Vecino Berbel escribió. Así, en la actualidad el desarrollo de las tecnologías para aliviar problemas que facilitan la producción agrícola representa una herramienta de gran impacto en la agricultura [6].

Aún más recientemente Juan Carlos Galindo manifiesta que la “agricultura e inteligencia artificial serán inseparables”, pero el hecho del “serán” demuestra que hay lugar de exploración y un gran potencial de investigación [7].

El principal objetivo de este trabajo es que a través de una aplicación y con la ayuda de árboles de decisión se logren identificar, cualquiera de las plagas y enfermedades que pueden atacar los cultivos del aguacate.

Para iniciar el desarrollo del sistema se tuvieron que definir las variables y para esto se usó un artículo publicado por la Universidad Pedagógica y Tecnológica de Colombia, escrito por Jimenes Andrés en 2009, donde se tiene un sistema de análisis de información para la clasificación y manejo de plagas de un duraznero [8].

En consecuencia, se decidió crear una aplicación capaz de reconocer el tipo de plaga con solo ingresar los valores necesarios, para definir la plaga mediante las reglas de derivación que se obtuvieron por medio del método antes mencionado. Así se dará instrucciones para el manejo dependiendo del tipo de plaga y, por último, se lanzará una alerta para que instituciones como SENASICA o SAGARPA puedan tener en cuenta y tomen acciones para el control de plagas.

3 Método

Se analizaron las características de las plagas que afectan los cultivos de aguacate; cómo se ven los insectos o bacterias; y qué efectos visuales tienen sobre los árboles de aguacate, como color de hojas, color en ramas o tronco, cáscara del aguacate, entre otros. Con los datos obtenidos se seleccionaron variables características de estas plagas, obteniendo así 15 variables para 12 tipos de enfermedad o plaga.

Como resultado de la investigación, se obtuvo una base de datos, los cuales se obtuvieron mediante la recopilación de imágenes y artículos sobre plagas en aguacate. Las Tablas 1 y 2 muestran extractos de la base de datos obtenida. En dichas tablas, la primera columna corresponde a las 12 enfermedades o plagas y en la primera fila comprende las 15 variables que se manejaron para la obtención de datos.

Tabla 1. Extracto de la base de datos, primeros 8 atributos.

Nombre	color fruto	protuverancia	hueso	hoja	Fruto forma	Larva	color rama	color hoja
Trips	Cafe	Cascara	Normal	Seca	Deformado	Si	Normal	Blanco
Barrenador de rama	Negro	Nula	Dañado	Seca	Normal	Si	Normal	Blanco
Barrenador de hueso	Negro	Nula	Dañado	Normal	Normal	Si	Normal	Blanco
Palomilla barrenadora	Blanco	Nula	Dañado	Seca	Necrosado	Si	Normal	Blanco
Agallador aguacatero	Amarillo	Hojas	Normal	Marchita	Normal	Si	Normal	Amarilla
Tristeza del aguacate	Blanco	Nula	Normal	Seca	Normal	No	Normal	Amarilla
Anillamineto de pendulo	Purpura	Nula	Negro	Normal	Redondo	No	Negro	Verde
Marchitamiento	Cafe	Hojas	Normal	Amarilla	Normal	Si	Negro	Verde
Cancer de tronco y de rama	Cafe	Ramas	Normal	Normal	Normal	No	Negro	Verde
Antracnosis	Cafe	Cascara	Normal	Manchas	Necrosado	No	Normal	Verde
Sarna o roña	Cafe	Cascara	Normal	Normal	Deformado	No	Cafe	Blanco
No es plaga	Verde	Nula	Normal	Normal	Normal	No	Normal	Verde

Tabla 2. Extracto de la base de datos, últimos 7 atributos.

Nombre	rama seca	rama anillosa	ramanecrosada	color hueso	Manchas en hoja	Desarrollo fruto	ColorLarva
Trips	Si	No	No	Normal	No	Pequeño	Cafe
Barrenador de rama	Si	No	Si	Normal	No	Pequeño	Cafe
Barrenador de hueso	No	No	No	Cafe	No	Pequeño	Cafe
Palomilla barrenadora	Si	No	No	Cafe	Si	Pequeño	Cafe
Agallador aguacatero	Si	No	No	Normal	Si	Normal	Amarilla
Tristeza del aguacate	Si	No	Si	Normal	No	Pequeño	NA
Anillamineto de pendulo	Si	Si	Si	Normal	No	Podrido	NA
Marchitamiento	Si	No	Si	Normal	Si	Normal	Blanca
Cancer de tronco y de rama	Si	No	Si	Normal	No	Normal	NA
Antracnosis	Si	No	No	Normal	Si	Normal	NA
Sarna o roña	No	No	Si	Normal	Si	Mediano	NA
No es plaga	No	No	No	Normal	No	Normal	NA

Se utilizó como herramienta R-Project, para así, con la tabla generada aplicar el algoritmo de árboles de decisión ID3 y obtener las reglas de derivación y, por tanto, el árbol en forma gráfica. R-Project, es un software de computación estadística y de gráficos.

Dentro de los paquetes que proporciona este software se encuentra el de árboles de decisión.

Un árbol de decisión es un grafo parecido a un diagrama de flujo, para llegar a puntos específicos dentro del árbol se necesitan tomar decisiones con base en ciertas reglas. El árbol con el que se trabaja funciona con base en el algoritmo ID3, que significa Inducción a través de árboles de decisión, desarrollada por John Quinlan (1983).

El árbol proporciona como salida una decisión que puede ser sí o no (booleano), aunque también es posible representar funciones con un mayor rango de salidas. Lo que busca el árbol es estimar las probabilidades de las respuestas.

La entropía es un término que se refiere a una medida de incertidumbre. En este caso será usada para decidir qué atributo o atributos deben seleccionarse [9].

$$Entropía(S) = \sum_{i=1}^n x_i - ip_i \log_2 p_i$$

donde:

S: Es una colección de elementos.

pi: Es la probabilidad de los posibles valores.

i: Son las posibles respuestas de los elementos.

Por otra parte, mediante el lenguaje de programación C# se implementaron las reglas de derivación que proporcionó el software para llevar a cabo una aplicación, donde solo se debe introducir las características del fruto, hoja o rama y la aplicación devuelve si éste está enfermo, posee una plaga o si es un fruto sano.

4 Resultados

Se investigó el flujo de plagas de tipo depredadora para el aguacate, encontrando en total once plagas y enfermedades, obteniendo así, un total de quince atributos que ayudaron a describirlas. El problema es que no hay una base de datos existente, por lo que, se realizó una tabla con los quince atributos y las once plagas.

Entre cada plaga se puede presentar ligeras variaciones, por ejemplo, en el caso de la Antracosis, la hoja puede presentar manchas o no y parecer que no tiene nada, aprovechando estas ligeras diferencias se realizó una tabla con más identificadores variando los atributos.

En el método se muestra una porción significativa de la tabla utilizada, pero hay que tomar en cuenta que la tabla completa contempla un total de 384 datos, a los cuales se decidió particionarlos en un rango de entrenamiento del 70%, que da un total de 268 datos, y un rango de 30% para la validación, que representa 116 datos.

Una vez obtenida la tabla, con ayuda del software R se procedió a obtener las reglas de derivación por medio del algoritmo ID3. Se utilizó la parte gráfica, obteniendo así veinte reglas y el árbol mostrado en la Figura 3. Mientras que en la Figura 4 se presenta, como una muestra, la segunda instancia del nodo principal del árbol de decisión y la ruta que se toma para lograr tres reglas de derivación.

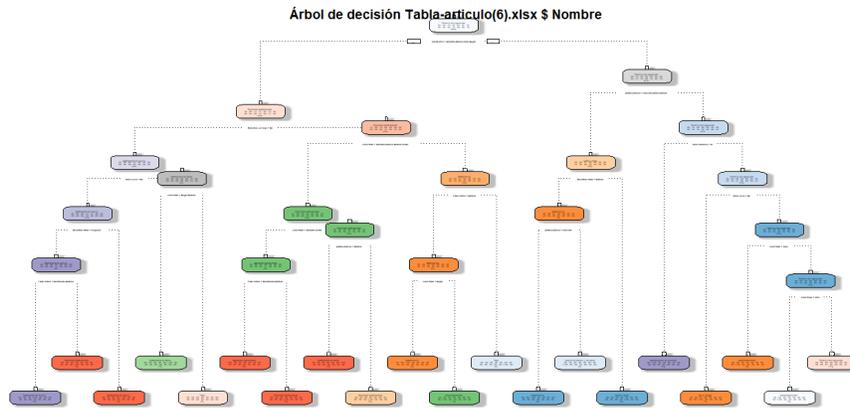


Fig. 3. Árbol de decisión generado en R-Project.

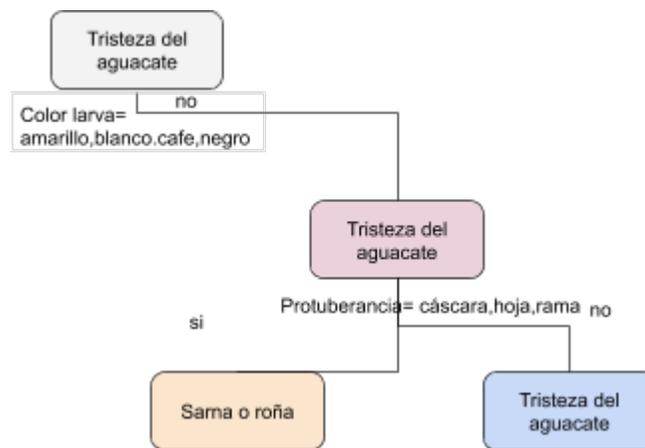


Fig.4. Nodo raíz y segunda instancia.

La lectura del árbol se empieza con el nodo raíz, donde se cumple la condición de tener o no una larva visible, para tomar como siguiente instancia las protuberancias en las ramas y cáscara del fruto, para luego continuar con la condición de no tener ramas anilladas.

La Figura 5 muestra la continuación de la segunda instancia. Se puede observar a detalle, las reglas obtenidas para las condiciones especificadas.

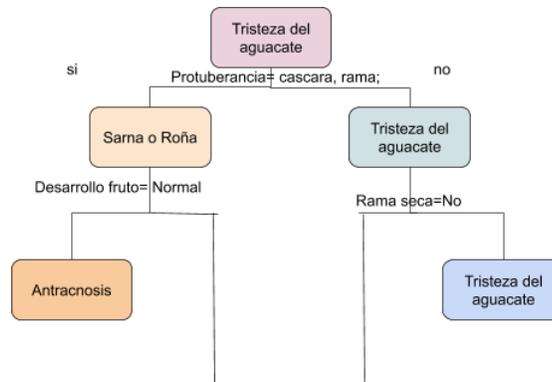


Fig. 5. Niveles intermedios del árbol de decisión.

Por último, la Figura 6 muestra la parte más baja del árbol de decisión, donde se puede observar el tipo de plaga que puede ser. Con base a la imagen corresponde: tristeza de aguacate y marchitamiento, donde se puede observar que marchitamiento puede darse mediante dos reglas de derivación, donde llegando a esta condición el fruto se presenta de color café o no, pero que sí presenta hoja seca, también se acompaña de la probabilidad de cada decisión.

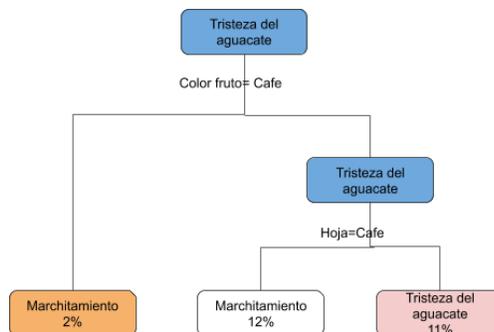


Fig. 6. Niveles finales y hojas de derivación.

Las reglas que se generaron son las que indican la forma en la que se formó el árbol. Estas reglas corresponden a los resultados obtenidos en el último nivel del árbol, este nivel da como resultado el tipo de plaga que se presenta en el fruto, hoja o rama, después de seguir diferentes decisiones que caracterizan a cada una de estas.

El formato de cada regla es el siguiente: aparece primero el número de regla seguido del nombre de plaga a la que corresponde, después el porcentaje que corresponde a cada plaga con base en sus características, pero como se mencionó anteriormente hay casos en los que se repite, esto se debe a que hay más de un camino con diferentes atributos que llevan a una misma plaga. Por último, se presentan las características que se utilizaron para llegar a este último nodo del último nivel de cada plaga.

En este caso la plaga que más posibilidad tiene de aparecer es la Palomilla Barrenadora, a pesar de que también otras plagas tienen más de una regla, ésta es la de mayor porcentaje. A continuación, se muestran las reglas que se obtuvieron para esta plaga.

- Rule number: 43 [Nombre=Palomilla barrenadora cover=21 (8%) prob=0.00 ColorLarva=Amarilla,Blanca,Cafe,Negro, Manchas en hoja=Si, color fruto=Amarillo, Blanco,Normal,Verde, protuberancia=Cascara,Nula
- Rule number: 41 [Nombre=Palomilla barrenadora cover=3 (1%) prob=0.00], ColorLarva=Amarilla, Blanca,Cafe,Negro
- Rule number: 33 [Nombre=Palomilla barrenadora cover=3 (1%) prob=0.00], ColorLarva=Amarilla,Blanca,Cafe,Negro Manchas en hoja=No, rama seca=No, Desarrollo fruto=Pequeño

Se puede observar en las tres reglas características como: color de larva, manchas en hoja, color de fruto. Estas son características constantes, así también hay características que son variables como: protuberancias, forma del fruto o desarrollo del fruto, esto se debe a las variaciones que puede haber en esta plaga y que se logran cubrir gracias a estas reglas.

Por último, se realizó una aplicación de fácil entendimiento para el usuario final, donde el productor o persona interesada, sepa el estado de su producto al consultarla para saber si tiene o no un caso de plaga o enfermedad. En caso de ser afirmativo, saber con precisión y exactitud de cual se trata.

En la Figura 7 se muestra la interfaz de la aplicación, donde el usuario puede seleccionar la opción que mejor describa su aguacate o árbol, al final se informa qué plaga es la que tiene. Se decidió meter la regla número 33, donde: color de larva es amarillo, hay manchas en hoja, su rama está seca, y el tamaño del fruto es pequeño y de forma redonda; como resultado se obtuvo que la plaga que se tiene es Palomilla Barrenadora.

Selecciona alguna de las siguientes opciones dependiendo de tu aguacate

Amarilla	Color fruto	Protuberancia
Manchas	Redondo	Limpiar
Seca	Pequeño	Calcular



¡Palomilla barrenadora!

Fig.7 Interfaz de la aplicación para la inferencia con base en las reglas de derivación.

5 Conclusiones

Lo expuesto a lo largo de este trabajo permite arribar a la siguiente conclusión. México tiene un gran potencial agrícola, y un campo de oportunidad donde se puede empezar a atacar problemas es en el sector aguacatero, por la calidad del producto nacional que se exporta y por el capital que se maneja. Aunque hay diversas fuentes de conflicto en el manejo de producción agrícola, como el uso de suelo o el riego tecnificado, es importante el saneamiento de los cultivos.

La FAO establece que aproximadamente un tercio de la producción se pierde por plagas y enfermedades. Es en donde se deben diseñar técnicas para prevenir y solventar este problema. Para esto se puede hacer uso de la inteligencia artificial.

Hay muchas áreas donde la inteligencia artificial y la agricultura se pueden relacionar, pero desgraciadamente en nuestro país no se aplican nuevas tecnologías en este sector. Por lo que, es conveniente empezar la aplicación de técnicas de inteligencia artificial, como el uso de árboles de decisión, que pueden ayudar a los productores y comerciantes en la validación del producto mediante estándares de calidad, de una manera rápida y sin complicación alguna.

Además, es notorio que el uso de la técnica presentada en este trabajo tiene una amplia aplicación, no solo en el aguacate, sino se puede ampliar la implementación para otros tipos de productos, ya sean frutas o verduras, de consumo u ornamental, y para hacer una reducción de pérdidas de cultivo.

Sin embargo, es imprescindible no quedarse en el pronto despliegue de acciones para combatir la plaga o enfermedad, sino en la prevención que además reduciría costos de operación y haría cultivos más sanos y así tener un mejor aprovechamiento de recursos.

6 Trabajos futuros

Como trabajo futuro a corto plazo se necesita hacer investigaciones de campo en zonas aguacateras, lugares de cultivo y comparar los resultados que se tiene hasta ahora, con datos reales, para así afinar el porcentaje de error y sea un sistema con una alta precisión y comprobada fiabilidad.

A mediano plazo se debe crear una base de datos dinámica con la información recolectada, esto con la finalidad de servir de apoyo a las organizaciones que deseen

aportar información para lograr hacer un sistema computacional más robusto, e incluso con participación de la SADER.

A largo plazo se pretende ampliar la gama de productos agrícolas que sean susceptibles a plagas y enfermedades, para que el sistema no sólo sea utilizado en aguacate, sino en otros tipos de cosechables que sean producidos en el país.

Así mismo, integrar una base de datos de las fichas técnicas que ya existen sobre cada tipo de plaga y enfermedad, para que la aplicación de usuario final emita recomendaciones, y en caso deseado se redirija con alguna dependencia de la elección del interesado para la oportuna solución de problemas de este tipo.

Referencias

1. Martínez, Maria del Pilar. (2018). México principal productor de aguacate. *El economista*. Recuperado de <https://www.eleconomista.com.mx/empresas/Mexico-principal-productor-de-aguacate-20180131-0111.html>.
2. Juárez, Axel. (2019). Cuánto guacamole se come en el super bowl. Nota periodística, El Universal.
3. L. V. Enrique, H. O. Marco, et. al, "Planeación Agrícola Nacional 2017-2030, Aguacate Mexicano", 2017, SAGARPA, pp. 2-9.
4. Vecino, Berbel, Julio. (1989). La inteligencia artificial en la agricultura: Perspectivas de los sistemas expertos. Dialnet
5. Jiménez, Adrés. Ravelo, Dianeth. Gómez, Johana. (2010), Sistema de adquisición, almacenamiento y análisis de información fenológica para el manejo de plagas y enfermedades de un duraznero mediante tecnologías de agricultura de precisión. Artículo, Universidad Distrital Francisco José de Caldas.
6. Montoya Urtega, Javier. (2015). Intelligent System for plague control in crops. REFI UPN.
7. Galindo, F, Juan Carlos. (2017). Agricultura e inteligencia artificial serán inseparables. Muy interesante.
8. Berlanga, V., Rubio Hurtado, M. J., & Vilà Baños, R. (2013). Cómo aplicar árboles de decisión en SPSS. REIRE. Revista d'Innovació i Recerca en Educació, 2013, vol. 6, num. 1, p. 65-79.
9. Martínez, G. R. S., & Mejía, J. A. S. (2011). Árboles de decisiones en el diagnóstico de enfermedades cardiovasculares. *Scientia et Technica*, 16(49), 104-109.

Bases matemáticas y curvas elípticas en la criptografía

Héctor David Ramírez Hernández¹, Roberto Contreras Juárez², Nelva Betzablel Espinoza Hernández³, Eduardo Mendoza Sánchez⁴
^{1,2,3,4}Facultad de Ciencias de la Computación-BUAP, Edif. CC02,
Ciudad Universitaria Av. San Claudio y 14 sur, Colonia San Manuel, C.P. 72570, Puebla, Pue.
¹hector.ramirezhe@correo.buap.mx, ²rcmarvin0828@gmail.com, ³nespinoza@cs.buap.mx,
⁴kamuipain58@gmail.com.

Resumen. La criptografía actual se basa en dos tipos de protocolos, uno el de la criptografía simétrica y el otro que corresponde a la criptografía asimétrica. En este trabajo se revisan las bases matemáticas de las curvas elípticas que dan soporte a la implementación de un protocolo del tipo asimétrico basado en las curvas elípticas sobre el campo finito $GF(p)$, en la que se propone una librería desarrollada en PHP que permite cifrar y descifrar información, con el fin de brindar los servicios de seguridad, autenticación, integridad y confidencialidad de la información.

Palabras Clave: Criptografía, Criptografía Asimétrica, Curvas Elípticas.

1 Introducción

La criptografía se puede definir como el arte o la ciencia de cifrar y descifrar información, utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas a quienes van dirigidos o que si se resguarda información esta no pueda ser extraída. Los criptosistemas utilizados son los denominados simétricos y los asimétricos. Los criptosistemas simétricos son aquellos que utilizan únicamente una llave para realizar el proceso, así el mensaje únicamente se descifra con la única llave existente. Este tipo de criptografía garantiza confidencialidad, pero al querer compartir el mensaje con otro usuario deberá crearse una nueva llave y el número de llaves aumenta conforme aumenten los usuarios con quienes se comparte el mensaje [1]. En 1976, Whitfield Diffie y Martin Hellman [2] introducen el concepto de criptosistema asimétrico, que surge como una solución al problema de intercambiar claves privadas por canales inseguros. Los sistemas asimétricos son aquellos en los cuales tanto el emisor como el receptor poseen un par de claves: una de tipo pública y la otra de tipo privada y para enviar mensajes el emisor tiene que cifrar el mensaje con la clave pública del receptor para que así este sea el único que pueda descifrar el mensaje usando su clave privada. Este sistema de encriptación fundamenta su seguridad en problemas matemáticos cuya solución computacional resulta difícil de resolver, ya que, aun conociendo los algoritmos para resolverlos, no es factible su ejecución en un tiempo razonable. Ejemplos de este tipo de criptografía son RSA y criptografía basado en curvas elípticas (ECC) [1]. La criptografía de curva elíptica (ECC), planteada por Koblitz y Miller [5], es una variante de la criptografía asimétrica la cual se basa en las propiedades de las curvas elípticas que resulta ser más eficiente que los métodos como el Rivest, Shamir y Adleman (RSA), además de proporcionar un nivel de seguridad equivalente [4].

2 Estado del arte.

Como se mencionó anteriormente, la criptografía de curvas elípticas (ECC) pertenece a la criptografía asimétrica, debido a que se utilizan dos tipos de llaves distintas, una pública y una privada, en la que el conocimiento de la llave pública no permite determinar el conocimiento de la llave privada. La criptografía de curvas elípticas fue propuesta en

1985 por Neal Koblitz [5] y Víctor Miller [6] y desde entonces ha permitido explorar nuevos criptosistemas, tal como la técnica de emparejamientos bilineales [7].

2.1 Curva Elíptica

Definimos de manera general a las curvas elípticas de la siguiente manera.

Sea K un campo. Una curva elíptica sobre K , es la curva plana sobre K definida por la ecuación de Weierstrass:

$$y^2 = x^3 + ax + b, \tag{I}$$

donde $x, y, a, b \in K$.

Para poder definir una estructura algebraica de grupo abeliano es necesario incluir un punto llamado punto en el infinito, denotado por ∞ , que no se encuentra en la curva.

Si $x^3 + ax + b$ no tiene raíces múltiples, entonces la curva correspondiente, aunado con el punto ∞ , más la operación suma definida más adelante, es lo que se denomina grupo de la curva elíptica sobre K , denotado por $E(K)$. Esto es, el conjunto:

$$E(K) = \{(x, y) : x, y \in K, y^2 = x^3 + ax + b\} \cup \{\infty\}$$

forma un grupo abeliano, en donde, ∞ es la identidad del grupo de curva elíptica. La siguiente gráfica representa un ejemplo de curva elíptica definida sobre \mathbb{R} .

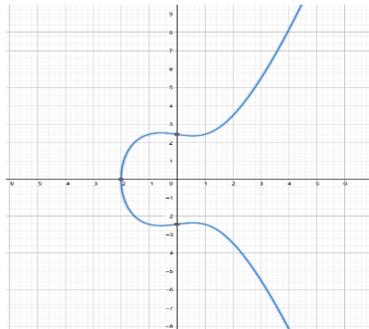


Fig. 1. Curva Elíptica $y^2 = x^3 - x + 6$

A la expresión $\Delta = 4a^3 + 27b^2$ se le conoce como el discriminante de la curva elíptica. Se verifica que para que la curva elíptica no tenga raíces múltiples es necesario que $\Delta \neq 0$. Esta condición permite excluir las curvas elípticas que tengan un punto doble o un pico como lo muestra la figura 2.

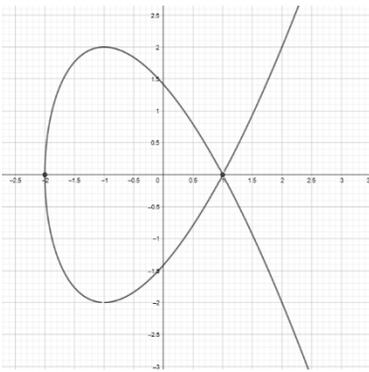


Fig. 2. Curva Elíptica $y^2 = x^3 - 3x + 2$ sobre \mathbb{R}

Trabajar criptografía con curvas elípticas sobre los números reales se puede volver lento e inexacto, debido a los errores de redondeo que puedan existir. En la práctica, el trabajo de criptografía se lleva a cabo con curvas elípticas sobre el campo finito $GF(p)$ pertenecientes a los campos primos y $GF(2^m)$ pertenecientes a los campos de binarios.

En este trabajo nos centraremos en las curvas elípticas sobre el campo finito $GF(p)$, con p un número primo, recordando que el campo de $GF(p)$ usa los números del 0 al $p-1$ y en cómputo final se obtiene el módulo de p .

Una curva elíptica definida sobre el campo de $GF(p)$, denotada por $E(GF(p))$, está formada por las variables a y b dentro del campo de $GF(p)$. Las curvas elípticas incluyen todos los puntos de (x, y) que satisface la ecuación de una curva elíptica módulo p . Esto es, una curva elíptica sobre $GF(p)$ tiene por ecuación:

$$y^2 \text{ mod } p = (x^3 + ax + b) \text{ mod } p, \quad (2)$$

donde $a, b, x, y \in GF(p)$.

De manera análoga, si $x^3 + ax + b$ contiene factores no repetidos, o equivalentemente si

$$4a^3 + 27b^2 \neq 0 \text{ mod } p \quad (3)$$

entonces la curva elíptica se puede utilizar para la criptografía. Una curva elíptica sobre el campo de $GF(p)$ tiene los puntos correspondientes en la curva elíptica, junto con un punto especial ∞ , el cual se le llama punto en infinito o punto cero. Son limitados los muchos puntos en las curvas elípticas. La cardinalidad de puntos de una curva elíptica se denota por $\#E(GF(p))$. El número de puntos de una curva elíptica es llamado el orden de la curva.

Ejemplo: Consideremos la curva elíptica sobre $GF(11)$. Con $a = 6$ y $b = 10$, la ecuación de la curva elíptica es $y^2 = x^3 + 6x + 10$. Los puntos que pertenecen a esta curva son: $(0,3), (0,5), (6,3), (6,8), (8,3), (8,8), (9,1), (9,10), (10,5), (10,6)$ incluyendo a ∞ . Esto es, $\#E(GF(p)) = 11$.

Desde el punto de vista algebraico la ley de grupo para una Curva Elíptica representada por la ecuación de *Weierstrass* (1), se define de acuerdo con las siguientes propiedades:

1. $P_1 + \infty = P_1$
2. Si $P_1 = (x_1, y_1)$, entonces $-P_1 = (x_1, -y_1)$.
3. Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos de la curva elíptica con $P_1, P_2 \neq \infty$. Entonces si $x_1 = x_2$ pero $y_1 \neq y_2$ o $P_1 = P_2$ y $y_1 = 0$ entonces $P_1 + P_2 = \infty$. En otro caso, $P_1 + P_2 = P_3 = (x_3, y_3)$ con $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$

$$m = \begin{cases} \frac{3x_1^2 + a}{2y_1} & x_1 = x_2 \\ \frac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \end{cases}$$

La curva elíptica $E(GF(p))$ dotada de la operación suma definida anteriormente forma un grupo abeliano.

Sea P un punto de la curva elíptica $E(GF(p))$. Entonces, kP significa la suma del punto P consigo mismo k -veces, con la suma definida anteriormente.

Es conocido el hecho de que si $\#E(GF(p))$ es un número primo entonces el grupo $E(GF(p))$ es un grupo cíclico. Este proceso facilita el hecho de que, si una curva elíptica cumple con esta condición, entonces cualquiera de sus puntos diferente del ∞ será un punto generador del grupo.

3 Protocolo Criptográfico

Para llevar a cabo la encriptación y desencriptación usando curvas elípticas, es necesario realizar múltiples operaciones que nos permiten establecer los mecanismos de seguridad que se necesitan en el resguardo de la información. Para ello detallaremos las operaciones utilizadas para llevar a cabo el objetivo de este trabajo. El desarrollo de este sistema fue utilizando PHP.

El primer paso consiste en proporcionar un número primo p y los coeficientes a y b , para formar la curva elíptica de la forma (2) cumpliendo la condición (3). Para mostrar este paso, consideremos los coeficientes $a = 9, b = 13$ y el número primo $p = 19$. Con estos parámetros se obtiene la curva $y^2 = (x^3 + 9x + 13) \bmod 19$, cumpliendo con la condición (3).

Para el siguiente paso se necesita determinar el número de puntos con los que cuenta la curva elíptica, $\#E(GF(p))$. Para poderlo calcular se puede implementar el algoritmo de Schoff que es de un tiempo polinómico. Sin embargo, su teoría e implementación queda fuera del alcance de este artículo, para obtener detalles de este algoritmo se puede consultar [8]. Para nuestro propósito, el cálculo del número de puntos es a través del método conocido por Baby Step-Giant Step (BSGS). Este método se apoya en el teorema de Hasse, el cual nos permite situar la cardinalidad de puntos de una curva elíptica dentro del intervalo $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$. La estructura del algoritmo es la siguiente:

1. $m = \lceil \sqrt[4]{q} \rceil$
2. $Q = (q + 1)P$
3. Calcular todos los puntos jP con $j = 0$ hasta hasta $j = m$. Además, se considera a los inversos de jP .
4. Calcular $Q + k(2mP)$ desde $k = -m, (m - 1), \dots, m$, hasta verificar si algún punto coincide con otro punto del paso anterior.
5. Verificar que $(q + 1 + 2mk \mp j)P = \infty$ y se toma a $M = q + 1 + 2mk \mp j$.
6. Sean p_1, p_2, \dots, p_r donde cada elemento es un factor primo de M .

Calculemos $(M/p_i)P$ para $i = 1, \dots, r$. Si $(M/p_i)P = \infty$ para algún i , entonces se reemplaza M con M/p_i y regresar al paso anterior, si $(M/p_i)P \neq \infty$ para todos p_i entonces M es el orden del punto.

3.1 Cifrado de datos

Para realizar el cifrado de los datos, debemos de contar con los siguientes parámetros: el número primo p , los coeficientes a y b , la cardinalidad de puntos de la curva elíptica $\#E(GF(p))$, un punto generador G de la curva, valores M y h con $Mh < p$, $llaveSA$ (llave secreta del usuario A), $llaveSB$ (llave secreta del usuario B) en donde $\text{mcd}(llaveSA, llaveSB) = 1$. Estos parámetros son utilizados por el cifrado de El Gamal. Mostraremos con un ejemplo el uso de la librería desarrollada en PHP. Consideremos: $p = 500009$, $y^2 = (x^3 + 15567x + 7896) \bmod 500009$, $M = 456$, $h = 123$, $\#E(GF(p)) = 49987$ (calculado con BSGS), $llaveSA = 24528$, $llaveSB = 11923$ y el punto generador $G = (241479, 71146)$

Supongamos que tenemos un usuario que se va a registrar en una plataforma y lo que interesa cifrar es la contraseña. Para nuestro caso la contraseña es carlos123 e ingresa sus datos en un formulario, figura 3.

Fig. 3 Formulario de contacto.

Procedemos a cifrar la contraseña del usuario de la siguiente manera:

Paso 1. Codificar el mensaje, para ello usaremos el código ascii que comprende del 0 al 255. Inicializamos con $j = 1$. Sabiendo que el ascii de la letra c es 99 se realizan los siguientes pasos:

Paso 1.1 Se calcula $x = \text{ascii}(c) (h) + j = 99 (123) + 1 = 12178$, y se sustituye este resultado en la ecuación de la curva elíptica, esto es,

$$y^2 = (x^3 + 15567x + 7896) = 12178^3 + 15567(12178) + 7896 = 334992,$$

dado que no existe valor de y que cumpla con esta ecuación, se aumenta a $j = 2$ y se reinicia el proceso.

Paso 1.2 $x = \text{ascii}(c) h + j = 99 (123) + 2 = 12179$, y se sustituye este resultado en la ecuación de la curva elíptica, esto es,

$$y^2 = (x^3 + 15567x + 7896) = 12179^3 + 15567(12179) + 7896 = 290136$$

este número si tiene raíz cuadrada que es igual a 161435.

Por tanto, la codificación de la letra c es (12179, 161435). Repetimos este proceso para cada una de las letras obtenemos:

$c = (12179, 161435)$	$s = (14147, 176240)$
$a = (11936, 218659)$	$1 = (6031, 183341)$
$r = (14023, 101746)$	$2 = (6152, 153375)$
$l = (13285, 115296)$	$3 = (6277, 52620)$
$o = (13656, 29398)$	

Paso 2. Se calcula la llave pública de A:
 $llavePA = LlaveSA * G = 24528 (241479, 71146) = (253513, 78497)$,
 entonces la pareja es igual $A = (24528, (253513, 78497))$.

Paso 3. Se calcula la llave pública de B:
 $llavePB = LlaveSB * G = 11923 (241479, 71146) = (339894, 358573)$,
 entonces la pareja es igual $B = (4562, (339894, 358573))$.

Paso 4. Cifraremos la letra c eligiendo un entero aleatorio $k = 205887$ y multiplicaremos ese número por el punto G, esto es,
 $kG = 205887(241479, 71146) = (45235, 155942)$.

Paso 5. Sumando la codificación de la letra c + $k(llavePB)$ se obtiene:
 $(12179, 161435) + 205887(339894, 358573)$
 $= (12179, 161435) + (237547, 189319) = (493092, 311065)$.

Paso 6. Se unen los resultados obtenidos en los pasos 4 y 5 para que la pareja de coordenadas quede como: $((45235, 155942), (493092, 311065))$.

Repetimos estos pasos para cada uno de los caracteres restantes, obteniendo como resultados:

Coordenadas Asignadas	k
(45235, 155942, 493092, 311065)	205887

(464947,454208,261541,436656)	425387
(1424,194779,211919,45374)	294652
(91384,133847,124363,495034)	258306
(22940,216821,391383,182458)	99447
(30055,298941,323275,69773)	340580
(220188,341581,147194,45165)	162281
(254288,121557,358833,451256)	470133
(310143,142529,222099,59930)	92723

Al tener todos los puntos cifrados solo bastará con mandarlos a una base de datos, como se muestra en la Figura 4.

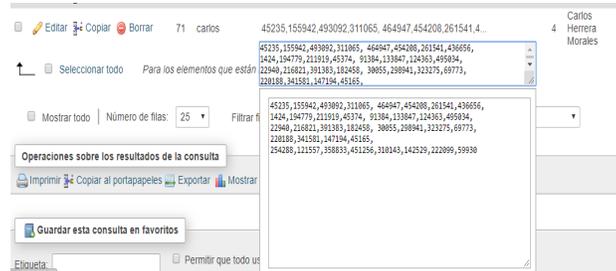


Fig.4. Puntos almacenados en una base de datos

El usuario al ser registrado puede ingresar a su información mediante su usuario y contraseña.

| carlos

|

Ingresar

Fig. 5 Datos del usuario.

Ahora debemos verificar que el usuario ingreso la contraseña correcta para ello debemos descifrar esa información.

Paso 1. Descifraremos el primer punto que son (45235,155942,493092,311065), tomando la primera pareja y multiplicándola por la llave secreta de B, esto es,

$$11923(45235,155942) = (237547,189319).$$

Paso 2. Se resta el resultado del paso 1 con la segunda pareja, recordando que $(x_1, y_1) - (x_2, y_2) = (x_1, y_1) + (x_2, -y_2)$. Por lo que se obtiene:

$$(493092,311065) + (237547, -189319) = (12179,161435).$$

Paso 3. Se realiza la decodificación usando la fórmula $\frac{x-1}{n}$. Sustituyendo los valores tenemos:

$$\frac{12179 - 1}{123} = 99.00813$$

Redondeando el resultado para que este quede solo en 99, y como sabemos el número 99 en el código ascii corresponde a la letra c, se obtiene el primer descifrado. Procedemos así para cada uno de los puntos.

4 Conclusiones

Se muestran los conceptos matemáticos para la realización de los algoritmos de cifrado y descifrado usando criptografía en curvas elípticas.

Actualmente las plataformas móviles o web recaban mucha información confidencial, por lo que se observó la necesidad de aportar un método de cifrado de esta información para que no pueda ser utilizada de manera incorrecta. Al hacer uso de una programación en PHP, se propone una librería que puede ser implementada para estos propósitos.

La dificultad que se presenta es la de calcular el número de puntos que contiene una curva elíptica, para ello será necesario establecer la programación adecuada para que logremos contar con este dato de una manera eficiente y poder trabajar con valores de números primos aún más grandes. Es por ello por lo que, como trabajo a futuro se pueda realizar la implementación del algoritmo de Schoff para este propósito.

Referencias

1. Amalraj, J.; Raybin, J.: *A survey paper on cryptography techniques*. IJCSMC, Vol. 5, Issue.8, pg.55 – 59. 2016.
2. Diffie, W.; Hellman, M.: *New directions in cryptography*. IEEE transactions on Information Theory, 22(6), pp. 644-654, 1976.
3. ElGamal, T.: *A public key cryptosystem and a signature scheme based on discrete logarithms*. IEEE transactions on information Theory, 31, pp. 469-472. 1985.
4. Gupta, V.; Stebila, D.; Sheueling, C.: *Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure*. Sun Microsystems, Inc.
5. Koblitz, N.: *Elliptic curve in cryptography*. American Mathematical Society J. Comput. Math., pp. 207-209. 1987.
6. Miller, V.: *Use of elliptic curves in cryptography*. In *Lecture notes in computer sciences; 218 on Advances in cryptology CRYPTO 85*, pp. 417-426, USA., Springer-Verlag New York, Inc. 1986
7. Kawahara, Y.; Takagi, T.; Okamoto, E.: *Efficient Implementation of Tate Pairing on a Mobile Phone Using Java*. In *Computational Intelligence and Security*, vol. 2, pp. 1247 - 1252, Berlin. 2006.
8. Schoff. N.: *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux 7, 219-254. 1985.

Análisis de la optimization de prótesis robótica

María del Carmen Santiago Díaz¹, Gustavo Trinidad Rubín Linares¹

Roberto Morales Aguilar¹, Ángel Peláez Ramírez²

¹Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla

²Facultad de Ciencias de la Electrónica, Benemérita Universidad Autónoma de Puebla
14 sur y Av. San Claudio, C.U. San Manuel, Puebla, México

{marycarmen.santiago, gustavo.rubin }@correo.buap.mx, {robertoma46,
angel.turquens.21}@gmail.com

Resumen. En el presente trabajo se muestra el diseño, construcción y funcionamiento de una prótesis de mano robótica capaz de emular los movimientos básicos de una mano humana, además se proponen las estrategias de optimización de cada módulo. Para ello, la mano robótica se diseñó con el programa SolidWorks y posteriormente se imprimió con una impresora 3D. La parte electromecánica consta de servomotores y un módulo Bluetooth donde las señales de entrada y salida son controladas con un microcontrolador basado en Arduino (Atmega328p).

Palabras Clave: Las palabras clave que identifican el artículo deben ir separadas por comas y escribirse con la inicial en mayúscula (excepto los artículos, las preposiciones y las conjunciones). Ejemplos: Interacción Persona Ordenador, Sistemas Empotrados, Ingeniería Web.

1 Introducción

El estudio de la anatomía de la mano de un ser humano es amplio y complejo debido a la cantidad de huesos que contiene y a los grados de libertad de movimiento. En ese sentido, la construcción de un dispositivo artificial es complejo, sin embargo, en este trabajo, nos enfocaremos en el desarrollo de un dispositivo más simple y al alcance de un estudiante del nivel medio superior. El tipo de movimiento que emularemos con nuestra mano robótica será con un grado de libertad dando lugar al movimiento de flexión, el cual es más amplio que el de abducción y adducción (movimientos laterales para abrir los dedos). La flexión de los dedos nos brinda la habilidad de atrapar objetos y mantenerlos con seguridad (agarre)[1].

El término robótica se le atribuye a Isaac Asimov, el cual procede de la palabra “robot” cuya definición es: “Manipulador multifuncional y reprogramable concebido para transportar materiales, piezas, herramientas o dispositivos especiales a través de movimientos programados variables para llevar a cabo tareas diversas” [2].

En la actualidad, los avances tecnológicos y científicos nos han permitido construir robots capaces de sustituir actividades humanas así como aplicaciones industriales complejas y hasta peligrosas. Sin embargo, en el área de la medicina, la robótica nos ha permitido reemplazar miembros perdidos, realizar procedimientos quirúrgicos delicados, dar terapia de neurorehabilitación en pacientes golpeados, diseñar aparatos didácticos para ayudar a los niños con discapacidad en el aprendizaje etc.

En este trabajo nos enfocaremos en un robot de rehabilitación, específicamente en una prótesis de una mano capaz de emular las destrezas de una mano humana.

Nuestro objetivo es diseñar y construir una prótesis de una mano robótica, capaz de emular los movimientos básicos de una mano humana. Para lograrlo, hacemos uso de servomotores SG90 encargados de la movilidad de los dedos de la mano, un módulo

Bluetooth que establece la comunicación entre la placa Arduino y un teléfono celular y un microcontrolador Atmega380 encargado de controlar dichas funciones.

Como bien sabemos, la tecnología nos permite facilitar el trabajo y desarrollo de ciertas actividades humanas con un toque de comodidad y confort en los diferentes sectores de la sociedad. Sin embargo, en nuestro país existen algunos sectores en los que no se ha avanzado. Más específicamente en el sector salud, las personas con diferentes discapacidades tiene que lidiar con la escases de dispositivos electrónicos que les puedan ayudar o facilitar sus actividades, a parte de los elevados costos.

En este proyecto nos enfocaremos en un sector específico de la sociedad, en aquellas personas con discapacidad motriz de una extremidad superior, más específicamente en una mano. Es importante aclarar que no pretendemos sustituir la discapacidad porque no está a nuestro alcance, pero si pretendemos ser de gran ayuda.

2 Desarrollo del Proyecto

Iniciaremos mostrando el diseño de la mano robótica, el cual fue realizado con el software llamado SolidWork, cabe mencionar que recibimos un curso previo del manejo de este programa [3].

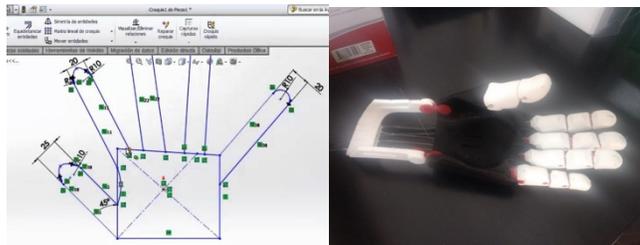


Fig. 1. Diseño de la prótesis en SolidWork.

Los elementos que integran el proyecto, son

- 1 placa Arduino UNO
- 5 servomotores SG90
- 1 módulo Bluetooth HC-06
- Hilo de nylon
- 1 Power Bank
- Jumper varios

La placa Arduino es la encargada de controlar la movilidad de la mano y establecer las señales de entrada y salida para la comunicación entre un teléfono celular y la placa.

Los servomotores constituyen la parte esencial de la parte mecánica de la mano.

El modulo Bluetooth establece una comunicación inalámbrica fiable y sencilla entre la placa Arduino y un teléfono celular.

El hilo naylor conecta los servomotores con las articulaciones de los dedos, que se tensiona cuando los motores están en funcionamiento, permitiendo la movilidad de la mano.

Cabe mencionar que en el comando “*if (letra == '2')*” el número “2” solo es un carácter que puede ser remplazado por una letra del alfabeto, el cual debe ser incluido en la aplicación dentro del teléfono celular para especificar el movimiento de un servomotor, en este ejemplo la letra “2” controla el servomotor asignado al dedo 3 de la mano.

En seguida se muestra la prótesis de la mano armada,

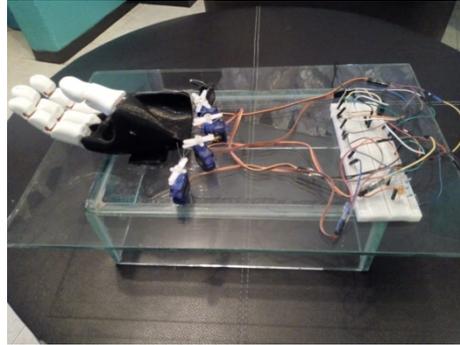


Fig. 3. Prótesis de la mano robótica terminada y funcionando

3 Resultados

Nuestro dispositivo está funcionando como esperamos. Las primeras pruebas que hicimos nos permitieron calibrar los servomotores para una mejor movilidad de la mano.

Cabe mencionar que al principio de las pruebas, nos encontramos con algunas dificultades técnicas, por ejemplo, las articulaciones de los dedos estaban muy tensas, de tal forma que la fuerza otorgada por los servomotores no era suficiente para facilitar la movilidad, se optó por desgastar parte del material de las articulaciones con la ayuda de una lija. Después de los ajustes, logramos que la prótesis de la mano funcionara correctamente y sin dificultades en su movilidad.

Para una siguiente etapa se deben considerar un conjunto de sensores a fin de medir los movimientos de los dedos y ajustar tanto fuerza como rapidez a fin de lograr una prótesis que ajuste el agarre dependiendo tanto del objeto o material a sujetar, como de las tareas asignadas con éste, por lo cual se requieren sensores de presión, de deslizamiento y de proximidad.

4 Conclusiones

En este trabajo diseñamos y construimos un dispositivo electromecánico capaz de simular el movimiento de una mano humana con la ayuda de algunos servomotores, un módulo de comunicación Bluetooth y un microcontrolador basado en la plataforma Arduino. Cabe mencionar que las aplicaciones de este tipo de proyectos son diversas, tales como: ayudar a una persona discapacitada en su movilidad de sus extremidades (mano), puede usarse como un aparato didáctico en el proceso de enseñanza aprendizaje en el manejo de la tecnología entre otros.

Referencias

1. Clavijo, F. F. (2011). Mano Robótica Inalámbrica. *Revista Universitaria Salesiana Guayaquil*, 90-180.
2. Dassault, S. (2002-2019). *Dassault Systemes SolidWorks Corporation*. Recuperado el Abril de 2019, de https://www.solidworks.es/sw/support/805_ESN_HTML.htm
3. Schlusser. (1985). Robotique, Control, Programation and Interaction. *Robot Institute of America*, 85-92.
4. Torrente, O. (2003). *Arduino: Curso práctico de formación*. México: Alfaomega.

*Aportes y Aplicaciones en las
Ciencias Computacionales*
se terminó de editar en Diciembre de 2019
en la Facultad de Ciencias de la Computación Av. San Claudio y 14 Sur
Jardines de San Manuel
Ciudad Universitaria
C.P. 72570

Aportes y Aplicaciones en las
Ciencias Computacionales
Coordinado por Gustavo Trinidad Rubín Linares

