

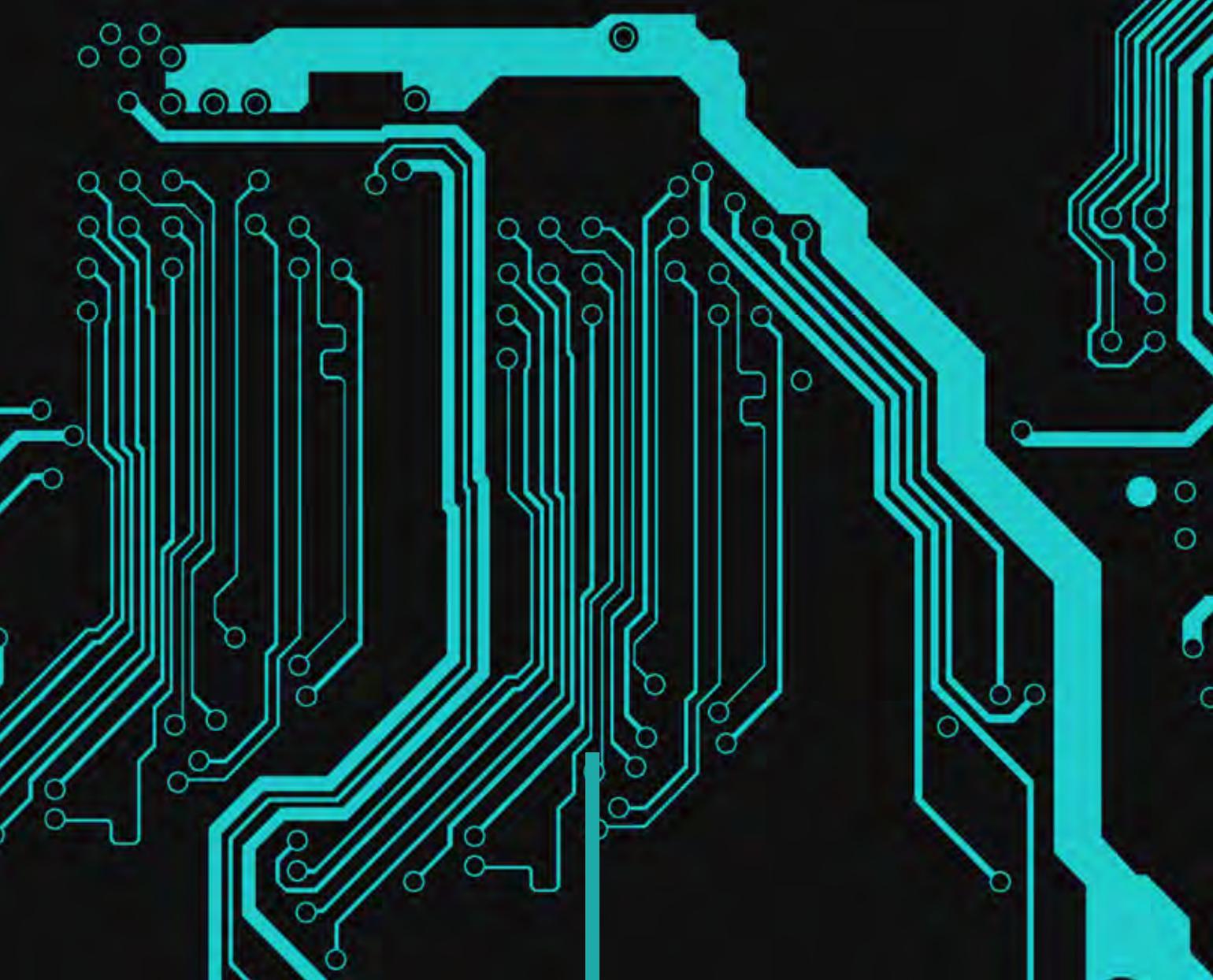


Año 7, núm. 30,
agosto-septiembre de 2016

spinor

Dos facetas, información y divulgación
un sólo objetivo, comunicar

Computación





XXIII

Semana Nacional de Ciencia y Tecnología

2 0 1 6

Anualmente la Benemérita Universidad Autónoma de Puebla en colaboración con el Consejo Nacional de Ciencia y Tecnología y el Consejo de Ciencia y Tecnología del Estado de Puebla llevan a cabo la "Semana Nacional de Ciencia y Tecnología en Puebla", siendo en 2016 la vigésimo tercera edición. Año con año este evento se ha convertido en un espacio idóneo donde el público proveniente de las diversas instituciones de nuestro Estado y de todos los niveles educativos tiene la oportunidad de conocer más y estar en contacto con la ciencia, la tecnología y la innovación. Este año realizaremos este evento durante la semana del 24 al 28 de octubre.

Podrás invitar a un investigador de la BUAP a impartir una conferencia en tu Institución o Unidad Académica, así como participar en alguno de los talleres que se ofrecen.

Informes en:

www.viep.buap.mx

**o al tel. (222) 229.55.00 ext. 5729 con
Lupita Merino o Lourdes Hernández.**





spinor

Dos facetas, información y divulgación
un sólo objetivo, comunicar

Revista de la Vicerrectoría de Investigación
y Estudios de Posgrado

Dr. José Alfonso Esparza Ortiz
Rector

Dr. René Valdiviezo Sandoval
Secretario General

D. C. Ygnacio Martínez Laguna
Vicerrector de Investigación y Estudios de Posgrado

**Dra. Ma. Verónica del Rosario
Hernández Huesca**
Directora General de Estudios de Posgrado

Dr. José Ramón Eguibar Cuenca
Director General de Investigación

Dr. José Eduardo Espinosa Rosales
Director General de Divulgación Científica

Investigación y revisión:

David Chávez Huerta
Heccari Bello Martínez
Laura I. Álvarez González
Jessica López
Laura Elisa Leyva M.
Erick Munive

Dirección de la revista:

Dr. José Eduardo Espinosa Rosales

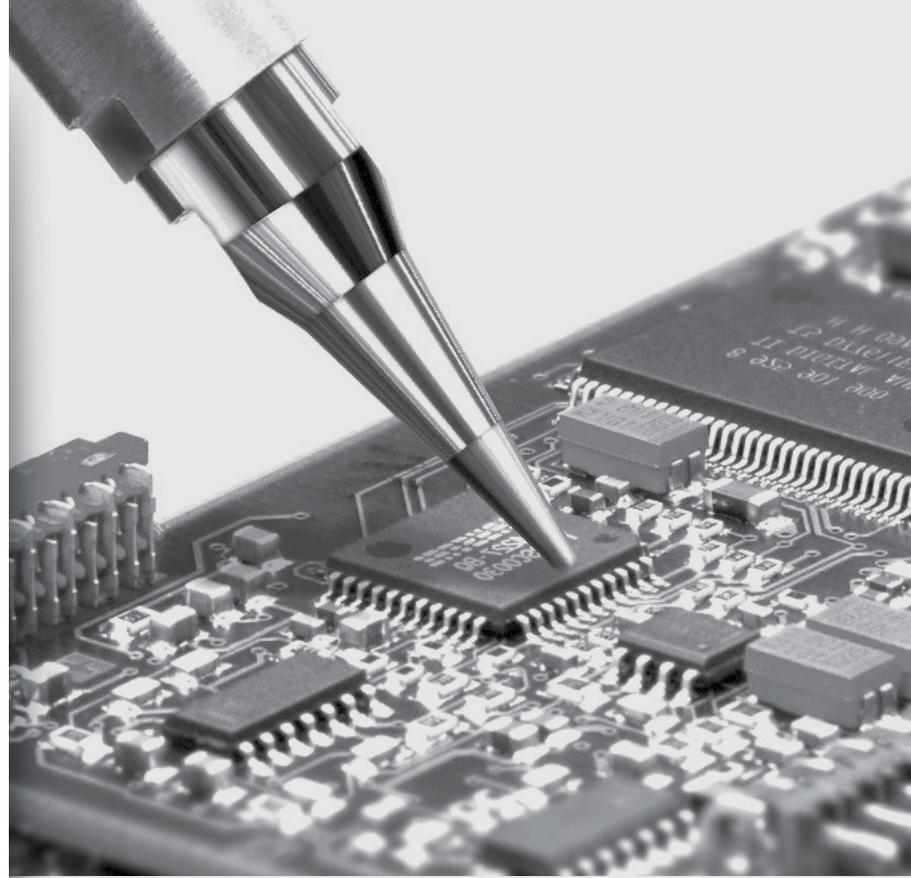
Consejo Editorial:

Dr. Jaime Cid Monjaraz, Dr. Miguel Ángel León Chávez,
Dra. Ma. de Lourdes Herrera Fera, Dr. Guillermo
Muñoz Zurita, Dr. Efraín Rubio Rosas, Dr. Óscar
Martínez Bravo, Dra. Olga Félix Beltrán

SPINOR, Año 7, No. 30, agosto-septiembre de 2016, es una publicación bimestral editada por la Benemérita Universidad Autónoma de Puebla, con domicilio en 4 sur 104, Col. Centro, C.P. 72000, Puebla Pue., y distribuida a través de la Dirección de Divulgación Científica de la VIEP, con domicilio en 4 sur 303, Col. Centro, C.P. 72000, Puebla Pue., Tel. (52) (222) 2295500 ext. 5729, www.viep.buap.mx, revistaspinor@gmail.com, Editor Responsable Dr. José Eduardo Espinosa Rosales, espinosa@fcm.buap.mx. Reserva de Derechos al uso exclusivo 04-2012-082209441800-102. ISSN: (en trámite), ambos otorgados por el Instituto Nacional del Derecho de Autor. Con Número de Certificado de Licitud de Título y Contenido: (16523), otorgado por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Impresa en EL ERRANTE EDITOR S.A. DE C.V., Privada Emiliano Zapata No. 5947, Col. San Baltasar Campeche, Puebla, Pue. C.P. 72590, Tel. (222) 4047360, este número se terminó de imprimir en Agosto de 2016 con un tiraje de 5000 ejemplares. Costo del Ejemplar Gratuito.

Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación.

Queda estrictamente prohibida la reproducción total o parcial de los contenidos e imágenes de la publicación sin previa autorización de la Benemérita Universidad Autónoma de Puebla.



Editorial

En este número se presentan en forma ágil proyectos realizados por investigadores de la facultad de Ciencias de la Computación de nuestra universidad, apoyados por estudiantes de la misma.

Una característica de la computación es su versatilidad, lo que le permite relacionarse con otras disciplinas como la medicina, genoma humano, finanzas, comercio, ingeniería y seguridad, entre muchas otras. Las áreas computacionales que se usan en la mayoría de los problemas son: la inteligencia artificial, la seguridad en cómputo, cómputo móvil, procesamiento de lenguaje natural, robótica y web.

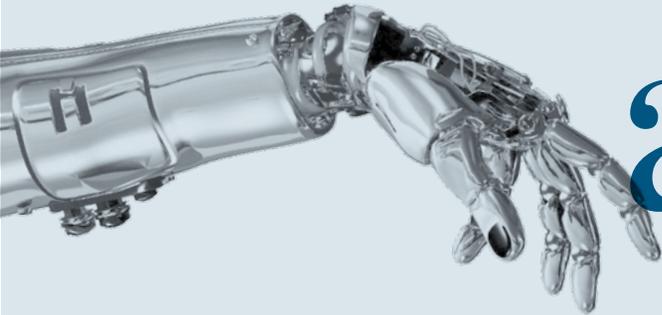
Con especial fervor invitamos a leer las contribuciones que hizo el Dr. Harold V. McIntosh a la ciencia computacional, así como el papel que desempeñó motivando a varias generaciones de estudiantes para que fueran exitosos profesionistas del área, todo contado por el Dr. Gerardo Cisneros.

También se presenta la novena edición de la Feria de proyectos (FePro), un evento académico que en estos últimos años ha permitido proyectar a los alumnos a nivel regional, nacional e internacional.

Deseamos que para nuestro joven lector sea motivante este número.



Un viaje rápido por la inteligencia artificial



Marcela Rivera Martínez¹ y Luis René Marcial Castillo²
Profesores-investigadores de la Facultad de Ciencias de la Computación, BUAP.

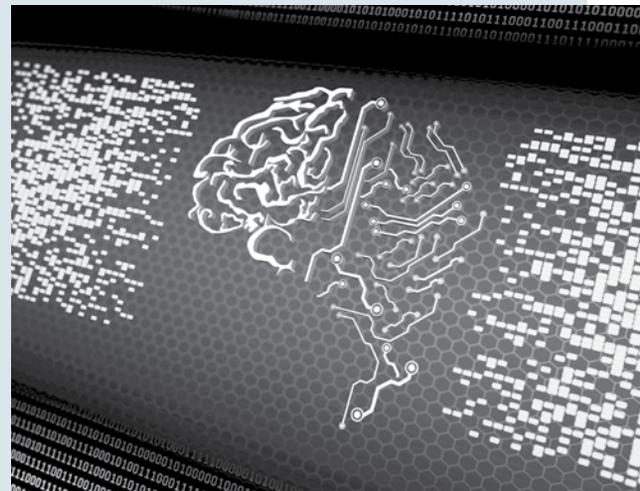
La inteligencia artificial es la rama de las Ciencias de la Computación que exhibe comprensión inteligente por medio de artefactos tales como teléfonos, autos, robots, entre otros, creados por humanos.

Para determinar la inteligencia de un artefacto, se realiza la prueba de Turing que concluye si una máquina se puede considerar inteligente o no; la dinámica es simple: cuando un humano es incapaz de distinguir si está hablando con una máquina o con otra persona (al comunicarse sin ver físicamente a su interlocutor), la conclusión es sí. Una forma invertida de la prueba de Turing, que se usa ampliamente en internet, es el test Captcha que está diseñado para determinar si un usuario es un humano o una computadora.

En el mundo cotidiano existen problemas que requieren una gran cantidad de tiempo de cómputo para encontrarles una solución, los artefactos que simulan inteligencia, en general, requieren analizar o buscar sobre millones de datos para dar una solución correcta, es por ello que la inteligencia artificial en lo correspondiente al *software* debe innovar algoritmos para ayudar a procesar una gran cantidad de datos y dar una respuesta oportuna.

Hemos realizado diversos trabajos en el área de inteligencia artificial. Mencionaremos brevemente algunos a continuación:

Sistema experto para detectar diversos tipos de cáncer, como son los de colon, mama y cérvico uterino. La codificación del conocimiento se realizó mediante reglas, el sistema es el resultado de la cooperación de expertos humanos que laboran en diversos hospitales de México y de las guías de prácticas clínicas de la Secretaría de Salud que ayudan en el fortalecimiento de la toma de decisiones clínicas. Los resultados se han validado con la ayuda de expertos humanos aplicándolo a pacientes reales.



» En junio de 2014, 33% de los jueces de la Real Sociedad de Londres se convencieron de que conversaban con un chico de 13 años, sin embargo, era una computadora creada por el programador ruso Vladimir Veselov

¹ Áreas de interés: inteligencia artificial, heurísticas.

² Áreas de interés: heurísticas, procesamiento de imágenes digitales.



» De igual manera los robots no cuentan con sentido común, el sentido común de los seres humanos ha sido adquirido por experiencia acumulada desde que el hombre está en la Tierra

También se ha utilizado una red neuronal multicapa para decidir si un paciente tiene cáncer de mama o no. La red neuronal hace uso, para su entrenamiento, de las técnicas colonia de abejas y búsqueda armónica; los resultados obtenidos se compararon usando la base de datos de la Universidad de Wisconsin, obteniendo un porcentaje de clasificación correcta de hasta 99% para el caso de colonia de abejas y 94% para el caso de búsqueda armónica.

Se programó un algoritmo híbrido de colonia de hormigas, asistido por un recocido simulado para resolver el problema de *job shop scheduling*. En la manufactura de un producto se requiere de una serie de procesos, cada uno de estos se efectúa en una máquina determinada. Esto origina diferentes problemas, entre los que se encuentra secuenciar trabajos en máquinas. El problema de *job shop scheduling* tiene como objetivo encontrar el orden de ejecución de trabajos que requieren una serie de procesos en máquinas, de manera que se optimice el tiempo. Se han podido resolver de manera satisfactoria problemas de hasta 20 trabajos con 10 máquinas.

El inconveniente de transformar un *job shop* en un *flow shop* es una configuración común en la elaboración de un producto. En dicha transformación, uno de

los objetivos que se persigue es minimizar la longitud de la línea de flujo de producción resultante. El problema se modela utilizando la supersecuencia común más corta y se le aplica la heurística *majority merge*, combinada con métodos de reducción. Los experimentos demostraron la eficiencia del método híbrido resolviendo problemas de 30 trabajos con 10 máquinas.

Se han aplicado las técnicas: colonia de abejas y luciérnagas, para el problema de restauración de imágenes digitales cuando se usa regularización no suave y no convexa la cual tiene la ventaja sobre la regularización convexa de producir bordes más limpios pero hace que sea más difícil de resolver. Los resultados experimentales prueban la eficiencia de estas técnicas cuando se adaptan a este tipo de circunstancias.

Los algoritmos genéticos se han utilizado para resolver el problema de ensamblado de fragmentos, el cual es útil en la parte final de la lectura de ADN que a su vez es una parte importante en la investigación sobre el genoma humano.

Las técnicas ya mencionadas junto con otras permiten a la inteligencia artificial, tener diferentes aplicaciones en la vida cotidiana, como por ejemplo: vehículos autónomos; aparatos electrodomésticos como refrigeradores, lavadoras con sistema difuso; vi-

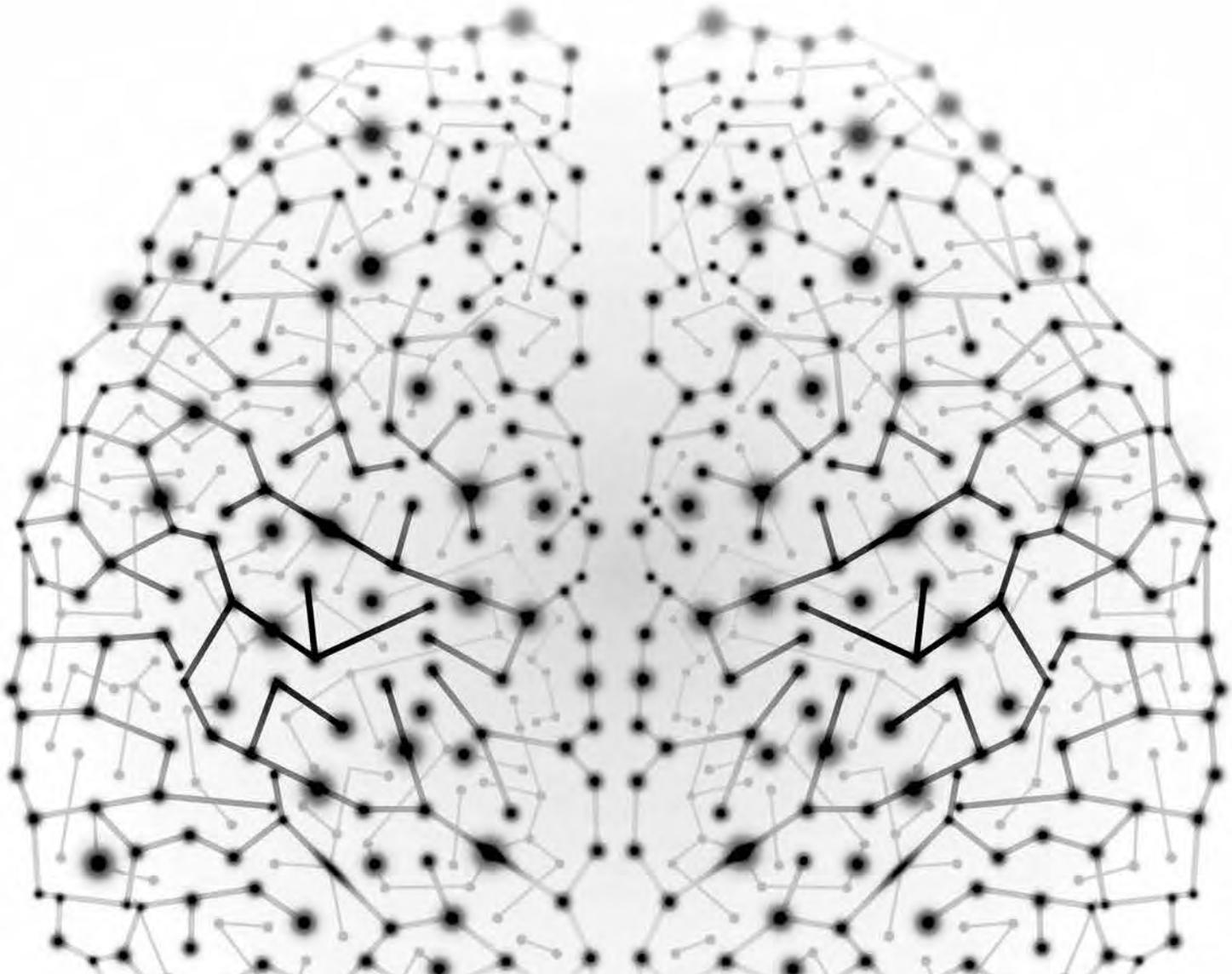
de juegos que incluyen estrategias inteligentes; casas inteligentes (domótica), toma de decisiones bancarias, económicas y comerciales entre otras.

Las computadoras actualmente son muy eficaces resolviendo ciertos problemas como la toma de decisiones en asuntos comerciales, venciendo a los humanos en juegos como el ajedrez. Las dos tareas que realizan los seres humanos sin esfuerzo alguno son: reconocer patrones y usar el sentido común. En el caso de reconocimiento de patrones, un robot puede ver mucho mejor que un ser humano, pero no comprende lo que ve, para lograr tal comprensión necesita asociar los puntos y líneas que conforman una imagen y buscar en su memoria algo semejante, esto requiere de muchas horas de cálculo, por el contrario, el cerebro humano es una máquina de reconocimiento de patrones. De igual manera, los robots no cuentan con

sentido común, el de los seres humanos ha sido adquirido por experiencia acumulada desde que el hombre está en la Tierra.

Para seguir avanzando en el área de inteligencia artificial, se necesita conocer de manera exacta cómo funciona el cerebro humano para posteriormente hacer dicha simulación en algún artefacto. Se espera que en poco tiempo, imitando el funcionamiento del cerebro humano, los artefactos ya no tengan un procesador de alta potencia, sino miles de pequeños procesadores interconectados entre sí, de tal forma que puedan aprender a través de experiencias recogidas por medio de cámaras de video, micrófonos, sensores, etc., que son equivalentes a algunos de los sentidos humanos.

Siguiendo esta misma línea, se trabaja actualmente en paralelizar las heurísticas que se han mencionado en párrafos anteriores.





Harold V. McIntosh

y la computación en México

Extracto del artículo del Dr. Gerardo Cisneros "La computación en México y la influencia de H. V. McIntosh en su desarrollo" del Departamento de Aplicación de Microcomputadoras del Instituto de Ciencias de la BUAP

EL DR. HAROLD V. MCINTOSH FUE UNO DE LOS PIONEROS del área de la computación en la Universidad Autónoma de Puebla y en nuestro país, así como uno de sus más destacados investigadores. Nació en Denver, Colorado, EUA, el 11 de marzo de 1929. Cursó la Licenciatura en Ciencias con especialidad en Física en el Colorado A&M College, donde se tituló en 1949; la Maestría en Ciencias (Matemáticas) de la Universidad de Cornell en 1952 y terminó créditos doctorales en Cornell y Brandeis University. Más tarde, obtuvo el Doctorado en Química Cuántica en la Universidad de Uppsala en 1972.

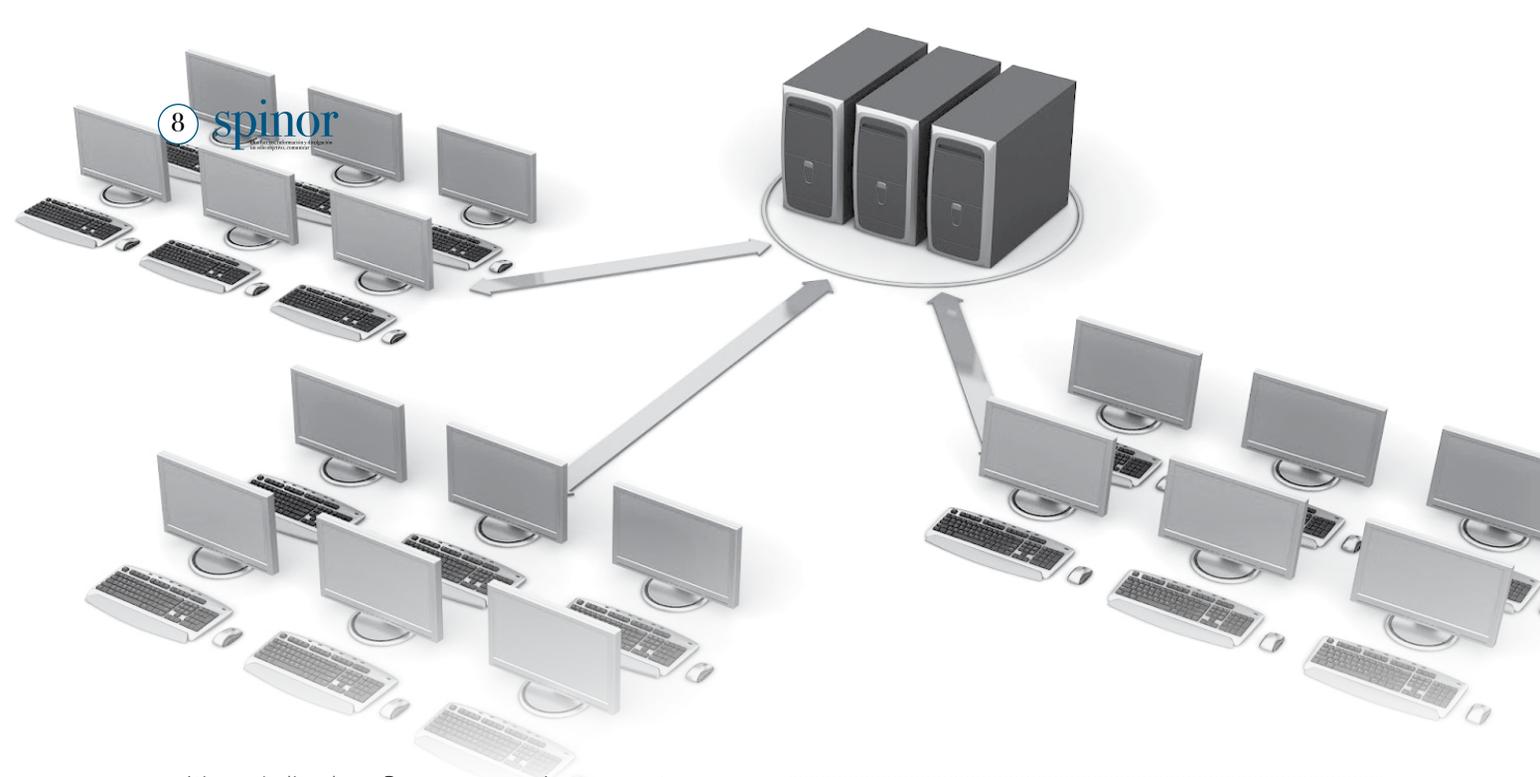
En México comenzó su trabajo en el Departamento de Física del Centro de Investigación y Estudios Avanzados del IPN de 1964 a 1965; en este periodo trabajó en el área de compiladores para el lenguaje de programación Convert, ideado por McIntosh para realizar manipulaciones simbólicas útiles en la solución de problemas de mecánica clásica y cuántica. Como una continuación de la experiencia adquirida con el compilador MBLISP que creó McIntosh, Lowell Hawkinson y Robert Yates construyeron un excelente compilador de LISP para la computadora IBM 709.

Entre 1965 y 1966, McIntosh fue director del Departamento de Programación del Centro de Cálculo Electrónico de la UNAM (actualmente llamado IIMAS). Durante este periodo construyó el primer compilador del lenguaje REC (Regular Expression Compiler) como parte de las pruebas de aceptación para la computadora PDP-8, la cual fue una de las primeras minicomputadoras comercialmente exitosas.

De 1966 a 1975, fue Profesor en la Escuela Superior de Física y Matemáticas del IPN y Coordinador de la Academia de Mate-

» Los últimos lugares en los que trabajó antes de emigrar a México fueron el Departamento de Física y Astronomía de la Universidad de Florida y el Instituto de Investigación de Estudios Avanzados (RIAS) en Baltimore





máticas Aplicadas. Con su asesoría se construyeron compiladores de REC para las computadoras IBM 1130 y CDC 3150 en el Centro Nacional de Cálculo del IPN; él mismo se hizo cargo de la construcción de paquetes para cálculos matriciales, integración numérica de ecuaciones diferenciales de segundo orden, y cálculo de trayectorias de una partícula cargada en el campo de dos centros con cargas magnéticas y eléctricas.

Entre 1970 y 1975, McIntosh fue consultor del Instituto Nacional de Energía Nuclear. Con la ayuda de alumnos y egresados de la ESFM del IPN continuó el desarrollo del paquete de solución numérica de ecuaciones diferenciales de segundo orden y otros programas de interés para la comunidad científica del Instituto. También fue en este Instituto donde McIntosh desarrolló <PLOT75>, un paquete de graficación que por su utilidad logró difusión en todo el mundo.

En 1971, McIntosh publicó un artículo sobre simetría y degeneración que en 1980 fue citado tres veces de manera extraordinariamente entusiasta por Herbert Goldstein en la segunda edición de su mundialmente famoso libro de mecánica clásica.

En 1973, se fundó en la Universidad Autónoma de Puebla la Licenciatura en Computación dentro de la Escuela de Ciencias Físico-Matemáticas, promovida principalmente por Isidro Romero Medina, quien solicitó la asesoría de McIntosh y el resultado fue una de las carreras de computación mejor equilibradas y con mayor orientación a los fundamentos matemáticos que existen actualmente en México. En 1975, McIntosh y todo el grupo que colaboraba con él en el Instituto Nacional de Energía Nuclear fueron invitados a trabajar plena-

» En 1971 McIntosh publicó un artículo sobre simetría y degeneración que en 1980 fue citado tres veces de manera extraordinariamente entusiasta por Herbert Goldstein en la segunda edición de su mundialmente famoso libro de mecánica clásica.

mente en la Universidad Autónoma de Puebla, de este modo, quedó establecido el Departamento de Aplicación de Microcomputadoras en el Instituto de Ciencias de la UAP, donde se desarrollaron aplicaciones y avances en múltiples áreas de la computación, tales como los Sistemas de Múltiples Usuarios (SMU), el desarrollo de equipo de computación, la construcción del paquete de graficación <PLOT84>, heredero del trabajo previo de McIntosh, teoría de autómatas, así como el estudio de autómatas celulares. Inclusive, parte de los deberes del Departamento fueron los de asesorar y auxiliar a la administración de la Universidad en la selección y uso de computadoras. El Departamento participó en proyectos de automatización de la nómina de la Universidad, el Control Escolar y las bibliotecas.

El 30 de noviembre de 2015 el Dr. Harold V. McIntosh falleció a los 86 años de edad. Durante toda su trayectoria fue su prioridad la formación de investigadores y el avance científico, por lo que la comunidad universitaria siempre le estará agradecida.

Desarrollo de Aplicaciones Móviles

en la Facultad de Ciencias de la Computación

Rosa G. Paredes Juárez
Profesora-investigadora de la FCC, BUAP

El desarrollo de aplicaciones móviles se refiere a la programación de aplicaciones de software que van a ser consumidas por los usuarios a través de dispositivos móviles, tales como Personal Digital Assistant, tabletas, teléfonos inteligentes y más recientemente relojes inteligentes (Ogata & Yano, 2004; Paredes et al., 2005). El auge de estos dispositivos es tal, que ha llegado a ser una de las plataformas de mayor uso en la actualidad y su difusión sigue en constante ascenso, a la par de la disponibilidad de nuevas capacidades que nos permiten mantener los desarrollos que llevamos a cabo en constante evolución (Ogata et al., 2006; Paredes & Ayala, 2012). Si bien es cierto que en computación tanto los equipos como las aplicaciones se encuentran evolucionando continuamente, en el caso de los móviles el cambio es aún más visible, rápido y dramático.

Las posibilidades también son infinitas. ¿Tienes una idea para un juego o una aplicación? Excelente; mañana vas a poder ponerle aún más y mejores características: gráficas más complejas, sonidos más realistas, movimiento preciso por sensores, reconocimiento de voz.

Pero como ya sabemos para muestra basta un botón, y en esta ocasión me gustaría platicarles un poco más sobre los proyectos que llevamos a cabo y que son los mismos estudiantes quienes los proponen e implementan. Espero que a muchos les llamen la atención, y no solo eso, sino que próximamente los estén descargando de su tienda de aplicaciones preferida.

El semestre pasado, por ejemplo, contamos con el desarrollo de una aplicación para mantener y consultar recetas en el celular. La idea era que pudieras indicarle a la aplicación los ingredientes que tenías a la mano en casa y que ésta desplegará una lista con las posibles recetas que podías cocinar. Sin embargo, las utilidades de la aplicación no paraban ahí; además, te permitía indicar tus recetas favoritas y revisar la popularidad de las mismas antes de seleccionar. Asimismo, incluía las instrucciones en texto, la foto del platillo terminado y un video con las indicaciones para la preparación. Finalmente, te dejaba compartir las recetas por correo o presumir en redes sociales lo que acababas de preparar y lo que ibas a comer durante el día.





Este semestre, un equipo de estudiantes está trabajando en una aplicación para ayudarte a mover de un lugar a otro en la ciudad de Puebla. El sistema presenta un mapa que te muestra la posición en la que te encuentras actualmente y te permite indicar a dónde quieres llegar. Mediante un algoritmo de resolución bastante complejo, te indica la(s) ruta(s) que debes tomar y en dónde debes transbordar, así como un tiempo y costo aproximado del viaje. Suena bien, ¿verdad? Bueno, pues además la aplicación te muestra zonas de peligro y sitios de interés por los que vas pasando a lo largo del viaje, para que decidas si te da tiempo de bajar a dar un paseo o para que no se te vaya a ocurrir caminar de noche por una zona en donde se han reportado robos o asaltos. En caso de que te estés preguntando de dónde sale toda esta información, aprovecho para comentar que los estudiantes hacen uso del poder de las redes sociales. Es decir, es la misma comunidad la que va a utilizar la aplicación que se encarga de decir dónde es peligroso, o dónde hay un lugar interesante que podrías visitar.

Otra aplicación que podríamos poner como ejemplo es una que fue desarrollada para ayudar a las personas con dificultades auditivas o de habla para comunicarse con los demás. La aplicación presentaba una lista de las acciones, personas y lugares más utilizados por el usuario y le permitía formar oraciones completas de forma fácil y gráfica, para que después un sintetizador de voz pudiera pronunciar la oración por él/ella. La aplicación era muy útil para los usuarios para los que estaba pensada y cumplía con el propósito de su creación. Sin

embargo, una vez terminada nos dimos cuenta que no era el único caso de uso. La aplicación podía ser fácilmente modificada para utilizarla como un traductor. El usuario podía formar sus oraciones de forma rápida y fácil en español, elegir un idioma destino y dejar que el sintetizador hablara por él/ella.

Como se puede ver, las posibilidades son muchas y lo que tratamos de hacer es buscar proyectos que consideren la conjunción de tres factores importantes: los deseos de la gente (usuarios finales del sistema), la viabilidad comercial (el plan de negocio) y la capacidad tecnológica (las características que se requieren en los dispositivos). Con base en estos tres factores, podemos asegurar que las aplicaciones desarrolladas tienen un excelente futuro y que no complacen únicamente al equipo que las desarrolla, sino también al mercado para el que fueron diseñadas e implementadas.

Referencias

- Ogata, H. & Yano, Y. (2004). Context Awareness Support for Computer-Supported Ubiquitous Learning. Proceedings of the Second IEEE International Workshop on Wireless and Mobile Technologies in Education, WMTE-2004, pp. 27-34.
- Ogata, H., Yin, Ch., Paredes, R., Saito, N., Yano, Y., Oishi, Y. & Ueda, T. (2006). Supporting Mobile Language Learning outside Classrooms, Proceedings of Sixth International Conference on Advanced Learning Technologies ICALT2006, Kerkrade, Netherlands, Jul. 2006, pp. 928-932.
- Paredes, R., Ogata, H., Saito, N., Yin, Ch., Yano, Y., Oishi, Y. & Ueda, T. (2005) Loch: Supporting Informal Language Learning Outside the Classroom with Handhelds, Proceedings of the Third IEEE International Workshop in Ogata, H., Sharples, Yano, K. & Yano Y., (eds.) Wireless and Mobile Technologies in Education 2005. IEEE Computer Society Tokushima, Japan, Nov. 28-30, pp. 182 – 186.
- Paredes, R. & Ayala, G. (2012). User and Context Modelling for Adaptive Mobile Learning Interfaces. International Journal on Mobile Learning Organization (IJMLO), Special issue on: Technology Transformed Learning: Going Beyond the One-to-One Model.

Vulnerabilidad de seguridad

de los Comprobantes Fiscales Digitales por Internet en México

Miguel Ángel León Chávez

Facultad de Ciencias de la Computación, BUAP
 Correo-e: miguel.leon@correo.buap.mx



Una aplicación de la criptografía asimétrica, i.e., en la que el usuario posee dos llaves, una privada o secreta y otra pública, es la firma digital o electrónica, la cual es el análogo de la firma manuscrita donde el firmante acepta respetar un contrato y su firma es válida para propósitos legales.

Esta firma provee los siguientes servicios de seguridad: autenticación, integridad y no rechazo. El servicio de autenticación permite verificar la identidad del firmante puesto que él o ella es el único poseedor de la llave secreta con la que se firma el contrato; el servicio de integridad permite verificar que el contrato no fue modificado; el servicio de no rechazo permite resolver posibles disputas entre el firmante y el receptor del contrato por una tercera instancia confiable.

La figura 1 muestra la estructura básica de la firma digital y consta de las siguientes fases: generación, transferencia, verificación y almacenamiento. Durante la fase de generación el firmante cifra (E), usando su llave secreta (SK), el resumen (h) de longitud fija producido por una función Hash (H) que tuvo como entrada un mensaje de longitud arbitraria (M). En la fase de transferencia, la firma (s) se concatena (||) al mensaje y se envía al receptor o verificador. Durante la fase de verificación, el receptor calcula nuevamente el resumen del mensaje y lo compara con el descifrado (D) de la firma usando la llave pública (PK) del firmante. Si ambos resúmenes coinciden la firma se acepta, en caso contrario se rechaza. En cualquier momento, durante la fase de almacenamiento, una tercera parte confiable puede verificar la firma por tanto el firmante debe almacenar el mensaje y la firma.

Se puede notar que la seguridad de la firma digital depende de todas las fases y que cualquier vulnerabilidad en una fase afectará todos los servicios de seguridad.

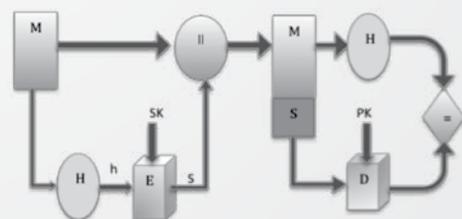


Fig. 1 Firma electrónica



Se puede notar que la seguridad de la firma digital depende de todas las fases y que cualquier vulnerabilidad en una fase afectará todos los servicios de seguridad. Además, la fortaleza o nivel de seguridad de la firma digital depende tanto del nivel de seguridad del algoritmo asimétrico de cifrado/descifrado como del nivel de seguridad de la función Hash y ambos niveles de seguridad deben ser iguales. El nivel de seguridad se define como el número de operaciones necesarias para romper el algoritmo criptográfico.

Para implementar la firma digital debe existir una infraestructura de llave pública compuesta por una autoridad certificadora responsable de generar, firmar digitalmente y distribuir los certificados digitales de los usuarios; los certificados contienen información del usuario, su llave pública, periodo de validez y parámetros del algoritmo usado para generarla. De esta forma cualquier usuario puede verificar el certificado de otro usuario usando la llave pública de la autoridad certificadora. Note que es responsabilidad del usuario resguardar su llave secreta.

En México el Sistema de Administración Tributaria (SAT) es una autoridad certificadora responsable de generar dos certificados digitales de todos los contribuyentes en el país: un certificado denominado firma electrónica avanzada (Fiel) para fines de administración fiscal, y otro certificado llamado de sello digital con el objetivo de firmar digitalmente todas las facturas

electrónicas (Comprobantes Fiscales Digitales a través de Internet, CFDI) expedidas por el contribuyente.

Los requerimientos de seguridad de los CFDI son los siguientes: infalsificable, único, protección contra la modificación, protección contra el no rechazo y perdurable en su almacenamiento. Estos requerimientos se satisfacen incorporando dos firmas digitales al CFDI: una por el contribuyente emisor y la segunda por el SAT o un proveedor autorizado de certificación (PAC).

El estándar informático que especifica la estructura, forma, sintaxis, formato y criptografía de los datos que deberán contener los Comprobantes Fiscales que se expidan por medios electrónicos está definido en el Anexo 20 de la Resolución Miscelánea Fiscal para los años 2006, 2010, 2012 y 2014 [1] publicados por la Secretaría de Hacienda y Crédito Público (SHCP) del gobierno mexicano en el *Diario Oficial de la Federación*.

Los elementos utilizados en la generación de sellos digitales son los siguientes:

- **Cadena original, el elemento a sellar, en este caso de un CFDI.**
- **Certificado de sello digital y su correspondiente llave privada.**
- **Algoritmos de criptografía de llave pública para Fiel.**
- **Especificación de conversión de la firma electrónica avanzada a base 64.**



Los algoritmos criptográficos definidos en el Anexo 20 para la generación de los sellos digitales son los siguientes:

- **SHA-1 que es una función Hash (digestión, picadillo o resumen) de un solo sentido tal, que para cualquier entrada produce una salida compuesta de 160 bits (20 bytes) denominada "digestión".**
- **RSAPrivateEncrypt (módulo 1024 bits), que utiliza la llave privada del emisor para "encriptar" la digestión del mensaje.**
- **RSAPublicDecrypt (módulo 1024 bits), que utiliza la llave pública del emisor para "desencriptar" la digestión del mensaje.**

Note que usando estas funciones el nivel de seguridad teórico del CFDI es de 80 bits, un medio la longitud del resumen. Sin embargo, el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio del gobierno de los Estados Unidos de Norteamérica ha recomendado a todas las dependencias

de gobierno norteamericano no usar la función SHA-1 desde el año 2010 [2] debido a que el nivel de seguridad de la función es actualmente de 2^{53} bits.

Además desde al año 2013 [2], el NIST recomienda usar la firma digital RSA módulo ≥ 2048 la cual provee un nivel de seguridad de 112 bits por lo que la función SHA recomendada es SHA-224 o SHA3-224 dado que proveen el mismo nivel de seguridad.

Si el SAT desea proteger los CFDI con un nivel de seguridad de 112 bits deberá recomendar el uso de RSA módulo 2048 y SHA-224 o SHA3-224. Se puede notar que entre más grande es el módulo más grande es la longitud de la llave y tanto el tiempo de procesamiento como el espacio de almacenamiento serán más grandes. Una alternativa es usar criptografía de curvas elípticas como lo hacen otras aplicaciones seguras donde el tamaño de las llaves es más pequeño.

Referencias

1. *Diario Oficial de la Federación* (30/12/2013). *Anexo 20 de la Resolución de la Miscelánea Fiscal para 2014*, publicado el 30 de diciembre de 2013 en el *Diario Oficial de la Federación* por el Poder Ejecutivo a través de la Secretaría de Hacienda y Crédito Público (2014).
2. NIST SP 800-131A Rev. 1. *Transitions: Recommendations for Transitioning the Use of Cryptographic Algorithms and Key Lengths* (2013, 2015).

¿Dónde está el Internet?

David Chávez Huerta

Actualmente un enorme número de personas están familiarizadas con la idea abstracta del Internet: una *red* que conecta a las personas alrededor del mundo y permite comunicarse y compartir información. No hay nada de malo en esta noción, sin embargo, son muy pocos quienes saben con seguridad qué es, físicamente, esa red. ¿A dónde va a parar — por poner un ejemplo — una imagen que he compartido, luego de que sale de mi teléfono hacia la red *Wi-Fi* de mi casa? ¿Por dónde tiene que viajar hasta estar globalmente disponible?

Más o menos desde el comienzo de su expansión, términos como *ciberspacio*, *carretera de la información* o más recientemente *aldea global*, han alimentado esa sensación de que Internet es algo etéreo, casi mágico e incomprensible, que escapa a cualquier descripción física. En este artículo, vamos a hacer lo posible por desmitificar la naturaleza y la estructura básica de una de las máquinas más complejas, extensas y valiosas creadas por la humanidad.

Su arquitectura básica, una idea del siglo XIX

Ciertamente, a algunas personas les resultará familiar la historia que comienza con Arpanet (red de uso militar, precursora de la red moderna), pero para explicar lo que ahora nos interesa se puede partir del antecesor estructural de Internet: las redes intercontinentales de telégrafo.

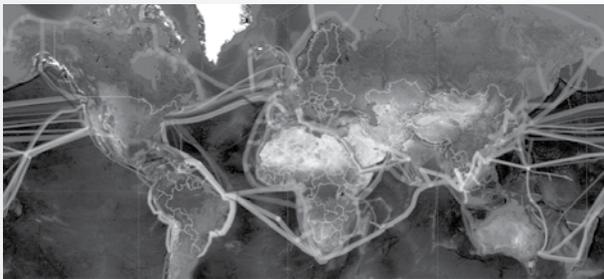
Desde mediados del siglo XIX se comenzó el tendido de cables submarinos de telégrafo y para 1901 esta tecnología permitía el envío de mensajes a todo lo ancho del planeta. Basta mirar el mapa de las líneas pertenecientes a la *Eastern Telegraph Co.*, para convencerse de que el concepto detrás de Internet (entendido como una forma de transmitir información de manera confiable



» Probablemente el lector esté enterado de la existencia de internet satelital, sin embargo el tráfico que esta tecnología es capaz de transportar es aún mínimo en comparación con el total.

veloz de un extremo a otro de la Tierra) antecede por muchas décadas al nacimiento de la computadora.

Una buena parte de las características que hacen de internet la gran herramienta que es, tiene que ver con dos ideas detrás de su diseño básico: la primera es la cualidad de mover información de usuario a usuario (a diferencia de sistemas como la televisión, enfocados en transmitir mensajes de manera unilateral); la segunda idea fundamental es que debe ser redundante, muchos caminos diferentes para llegar de un punto a otro. Ambos conceptos ya están presentes en la red de telégrafo (vea el mapa y sus muchas maneras de transmitir desde Nueva York hasta Londres) y serán heredados a las redes telefónicas. No es ninguna casualidad que sean estas compañías telefónicas quienes bien entrado el siglo xx implementen dentro de sus propias estructuras al naciente Internet.



La anatomía de la máquina

Contrario a la experiencia diaria, realmente aún no hay tal cosa como un Internet inalámbrico. La mínima parte del recorrido (digamos, de la computadora al *Wi-Fi*) que hace la información por medios inalámbricos no se compara con la totalidad del sistema. La globalidad de Internet depende de nuestra capacidad para hacer que la información atraviese físicamente los océanos. Esto se consigue con más de ochocientos mil kilómetros de cables de fibra óptica que, tal como se muestra en el segundo mapa, al atravesar los océanos siguen rutas trazadas sobre las de sus modestos antecesores. Estos cables, protegidos por múltiples capas de metal y plásticos, son enterrados en el lecho marino y en algunos casos se pueden ver sobre la playa. Cuando accidentes naturales o humanos dañan estas líneas, una alta redundancia del sistema es vital, tal como ocurría con las líneas de telégrafo.

Probablemente el lector esté enterado de la existencia de internet satelital, sin embargo el tráfico que esta tecnología es capaz de transportar es aún mínimo en comparación con el total.

Una vez establecida la comunicación intercontinental todavía hacen falta dos estructuras fundamentales de internet: los servidores raíz (Root Servers) y las redes Tier 1. Los servidores raíz son trece en total y cada uno tiene instalaciones alrededor del mundo. Son operados generalmente por gobiernos o empresas y hacen de traductores entre la *dirección*, que un humano puede entender (www.google.com.mx) y la dirección IP que para una computadora es más efectiva de usar (74.125.227.79). Sin ellos, haría falta tener a la mano la dirección IP de cada sitio al que se quiera acceder. En la Ciudad de México se ubica una *sucursal* del Root Server D, operado por la Universidad de Maryland.

Las redes Tier 1, operadas en su mayoría por empresas de comunicaciones (AT&T, Verizon, Deutsche Telekom...) son precisamente eso: redes capaces de mover ordenadamente cantidades inmensas de datos y que tienen como principal cualidad su alcance. Sin depender de terceros, las dieciséis redes Tier 1 que existen actualmente pueden acceder por sí mismas al resto de la red global. Por esta razón cientos de empresas más pequeñas compran el *acceso a internet* directamente aquí, para luego vender dicho acceso a los consumidores. Es notable que unos cinco billones de computadoras, teléfonos y demás dispositivos dependan de un número relativamente pequeño de estructuras base y esto es posible por el diseño cuidadoso del sistema.

Y ahora sí, el usuario puede desde su teléfono acceder a su proveedor de internet, se conectará a redes cada vez más grandes hasta llegar al Tier 1 más cercano. Éste eventualmente alcanzará al destinatario, por ejemplo alguno de los inmensos Data Centers de cierta red social. Desde aquí, tocando varias veces las instalaciones de los servidores raíz y atravesando océanos conectados por fibra óptica, se hace finalmente disponible toda clase de información a escala global.



El procesamiento de lenguaje natural
como medio de detección de

actividades criminales

Maya Carrillo Ruiz y Luis Enrique Colmenares Guillén
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN, BUAP

Durante siglos el ser humano se ha ocupado, en la ficción y en la realidad, de crear máquinas inteligentes capaces de comportarse como seres humanos. Aunque la tecnología ha logrado reproducir cierto comportamiento humano, como toma de decisiones, planeación, solución de problemas, entre otros, no ha logrado semejar la inteligencia. Mientras que en las

fábulas y cuentos, los animales hablan y pueden pensar como personas, los humanos no podemos hablar sin pensar, y parece que todo cambio se genera como una idea creada a partir de un dialogo interno. Entonces ¿la inteligencia es dependiente del lenguaje? Y si así lo es, ¿se podrá desarrollar una inteligencia artificial, si la computadora no entiende el lenguaje humano?



Ante este planteamiento, el procesamiento del lenguaje natural es una disciplina de la inteligencia artificial que se ocupa de la formulación e investigación de mecanismos computacionales para la comunicación entre personas y máquinas mediante el uso de lenguajes naturales. Los lenguajes naturales son los utilizados en la comunicación humana, ya sean escritos o hablados: español, inglés, francés, alemán, ruso, náhuatl, sánscrito, etcétera.

Ahora bien, ¿para qué sirve el procesamiento de lenguaje natural? En la práctica se emplea en diversas tareas, relativamente sencillas, como: corrección de textos, separación de palabras por sílabas, traducción de escritos; pero también se utiliza para buscar y utilizar información en los contenidos, así contribuye a la creación de motores de búsqueda como *Google*, responder a preguntas directas como ¿cuántos habitantes tiene la ciudad de México?; a descubrir, a partir de textos vastos, el conocimiento que no está explícitamente escrito en cualquiera de los documentos. Esto incluye buscar tendencias, promedios, desviaciones, dependencias, etc. Además puede apoyar en la solución de problemas más complejos que aquejan a la sociedad. Como la detección de posibles predadores sexuales en internet.

Sin lugar a dudas, las actividades de pedófilos se han incrementado, con la aparición de aplicaciones para hacer contactos en internet, pues permiten relacionarse tanto con menores de edad, como con otros pedófilos. Varios proyectos e iniciativas que investigan este fenómeno se han desarrollado en el mundo.¹ Esto como respuesta a los datos reportados por diferentes organizaciones. Por mencionar algunos, en abril del 2013 en la Ciudad de México, el Procurador General de Justicia del Distrito Federal, Rodolfo Ríos Garza, dio a conocer que la trata de personas genera al crimen organizado ganancias de 32 mil millones de dólares anuales (*Excélsior*, 2013).

Según Infancia Común, México tiene el segundo lugar en el mundo como productor de pornografía infantil. Tan sólo en cinco años detectaron en el país más de cuatro mil sitios electrónicos dedicados a la pornografía infantil. En Latinoamérica hay al menos cien foros virtuales donde intercambian este tipo de material; un tercio de ellos se ubican en el país.²

Para resolver la problemática planteada se han utilizado diferentes estrategias: crear páginas *web* ficticias como señuelo para usuarios pedófilos que permitan identificarlos; el ingreso de agentes de la policía y voluntarios a salas de *chat* haciéndose pasar por niños a fin de capturar a los delincuentes. Aunque estas estrategias han dado algunos resultados positivos, se necesitan recursos físicos considerables. Ante esta situación se ha planteado la posibilidad de automatizar el proceso de detección de actividades pedófilas en internet utilizando técnicas de *procesamiento de lenguaje natural*.³

Actualmente en la Facultad de Ciencias de la Computación estamos desarrollando métodos de *procesamiento de lenguaje natural*, que permitan detectar de manera automática texto con contenido pedófilo. Para ello, hemos conformado un grupo multidisciplinario en el que participamos el doctor Luis Enrique Colmenares Guillen, la doctora Maya Carrillo Ruiz y estudiantes de las licenciaturas de Computación, Psicología y Criminología de la BUAP, a fin de construir modelos cognitivos y perfiles psicológicos y criminalísticos de pedófilos.

Todo esto con el objetivo de analizar contenidos textuales de archivos, correos de internet, conversaciones en salas de chat, conversaciones en sistemas de mensajería instantáneos y grupos de noticias a fin de detectar temas pornográficos, temas pedófilos, formación de relaciones de comunicación (entre los pedófilos y los niños, así como entre pares pedófilos); temas de apoyo entre pederastas; e información pederasta relacionada (listado de sitios *web* seguros y otros datos). Los modelos y métodos definidos se están empleando para construir herramientas de *software* que permitan alertar a los padres y autoridades de las posibles víctimas de pedófilos, así como la identificación de dichos criminales.

Referencias

- 1 Breeden, B., & Mulholland, J. (2006). Investigating "Internet Crimes Against Children" (ICAC) cases in the state of Florida. Proceedings of the 2006 acm symposium on Applied computing, Dijon, France.
- 2 Monroy, Paulina (2010). México: pasividad ante explotación sexual infantil. Recuperado el 19 de junio de 2013, de <http://www.voltairenet.org/article167246.html>
- 3 Penna, L., Clark, A., & Mohay, G. (2005). Challenges of automating the detection of paedophile activity on the Internet. Proceedings First International Workshop on Systematic Approaches to Di Forensic Engineering.

La Agencia que no es, quiere ser el Aleph

Francisco Rodríguez Henríquez
Departamento de Computación, Cinvestav-IPN
Correo-e: francisco@cs.cinvestav.mx

Sí, [el Aleph].
el lugar donde están, sin confundirse,
todos los lugares del orbe,
visto desde todos los ángulos.
[...]
Lo que vieron mis ojos fue simultáneo:
lo que transcribiré, sucesivo,
porque el lenguaje lo es.

El aleph, Jorge Luis Borges.

A partir del 5 de junio de 2013, el expleado de la Agencia Nacional de Seguridad estadounidense (NSA, por sus siglas en inglés), Edward Snowden, ha ido revelando a través de los periódicos *The Guardian* y *The Washington Post*, documentos clasificados como de alto nivel de seguridad, los cuales describen una serie de programas de espionaje que la NSA aplica desde hace varios años con el objetivo de vulnerar la seguridad informática que deberían brindar diversas aplicaciones de software y hardware de uso comercial y cotidiano en internet, servidores, computadoras personales, teléfonos celulares y otros dispositivos digitales.

Por medio de tales programas de espionaje, la NSA ha almacenado una desahogada cantidad de información que le ha permitido establecer una incesante vigilancia de cientos y quizás miles de millones de personas a un nivel sin precedentes en la historia de la humanidad. En palabras de Snowden:

“En tanto el individuo objetivo tenga una cuenta de correo electrónico, es posible espionarlo sin importar si se trata de ti, de tu conocido, de un juez, o incluso, del presidente.”

Resulta significativo que incluso en los propios Estados Unidos se suela decir en broma que el verdadero significado de las siglas NSA es: No Such Agency, lo cual podría traducirse como: la agencia que no es.

Gracias a esas revelaciones, conocemos que la NSA tiene la capacidad de monitorear en tiempo cuasi real llamadas hechas desde teléfonos celulares ubicados en casi cualquier rincón del planeta, almacenar millones de correos electrónicos, mensajes de texto sms y datos confidenciales pertenecientes a cientos de millones de usuarios de compañías informáticas emblemáticas tales como Yahoo, Facebook, Twitter, Google, Apple y Microsoft, entre otras. Asimismo, se sabe ahora que en su insaciable apetito, la NSA ha espiado las actividades industriales de la más grande compañía brasileña de petróleo, Petrobras, así como las reuniones de instituciones humanitarias tales como la Unesco, además de haber interceptado los mensajes y correos electrónicos de al menos treinta y una figuras políticas mundiales, en una amplia lista que incluye a la canciller alemana Angela Merkel, a la presidenta brasileña Dilma Rousseff y, significativamente para nuestro país, al expresidente Felipe Calderón y a Enrique Peña Nieto (al menos) durante su etapa como candidato presidencial.

Con un presupuesto estimado de 10,8 mil millones de dólares y un número aproximado de cuarenta mil empleados, la NSA, que fuera fundada en 1952, es una de las agencias gubernamentales más grandes del mundo. Oficialmente, la NSA dirige, planea y diseña los esfuerzos criptográficos, cripto-analíticos y de seguridad informática de los Estados Unidos. En la práctica, ingentes recursos de la agencia son dedicados al es-

pionaje informático y a recabar material de inteligencia que de acuerdo a sus criterios, pudiesen llegar a afectar la seguridad nacional de ese país. Por ejemplo, la NSA se arroga el derecho de grabar y almacenar todas las llamadas telefónicas hechas en los Estados Unidos.

Se cree que la NSA es el máximo empleador de matemáticos en el mundo, muchos de ellos genios brillantes. Se sabe además que la NSA cuenta con la súper-computadora Bluffdale que consume 65 megawatts de potencia y que tiene una capacidad de almacenamiento que está al menos en el orden de exabytes (un billón de megabytes).

Está documentado que la NSA ha mantenido una política muy activa de sobornos e influencias en los comités que diseñan los estándares criptográficos internacionales, con el objetivo expreso de promover el uso de algoritmos criptográficos débiles y vulnerables. Se sabe además que la NSA se ha coludido con fabricantes de *hardware* y *software* para debilitar esquemas de cifrado y de autenticación de usuarios en esquemas conocidos como autenticación por dos factores. Probablemente el ejemplo más emblemático de estas políticas, es la implantación de una puerta-trampa en el generador de números aleatorios SecurID de la compañía RSA.

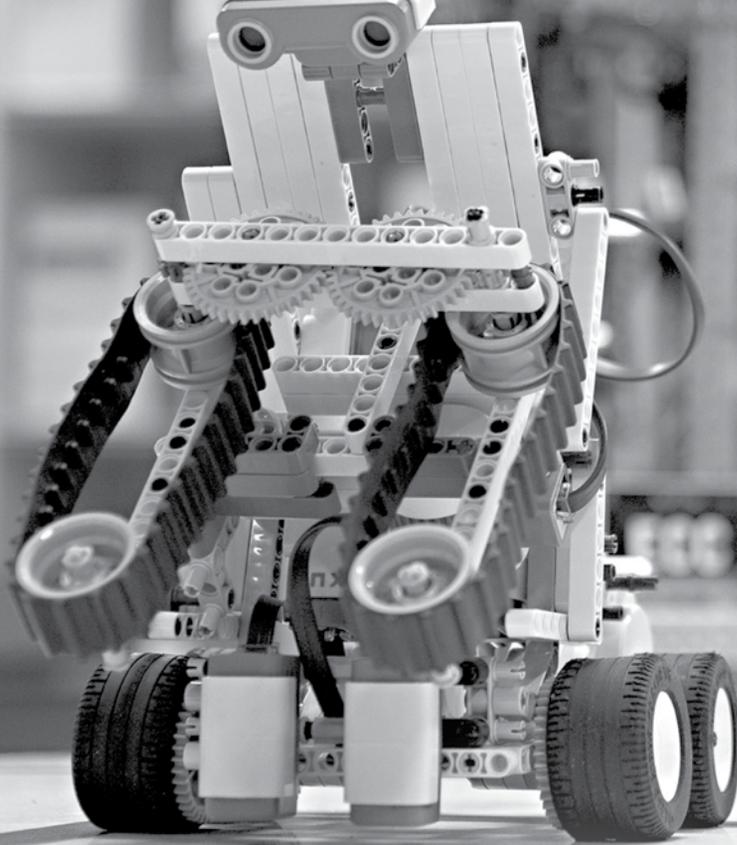
En diciembre del año 2013, el periodista Joseph Menn de Reuters publicó un artículo en el que se afirma que los directivos de RSA aceptaron un pago por diez millones de dólares para permitir que sus

bibliotecas criptográficas utilizaran de manera predeterminada, el esquema de generador de números aleatorios Dual_EC_DRBG que fuera promulgado como estándar de ISO y ANSI desde junio del 2004. Por extraño que parezca, el esquema Dual_EC_DRBG contiene una puerta-trampa introducida por la NSA, la cual permite predecir sin dificultades la secuencia generada por cualquier dispositivo de autenticación fabricado por la compañía.

Otros casos de éxito para la NSA, que son ejemplos sin duda interesantes pero que por motivos de espacio no discutiremos aquí, incluyen:

- **1. Ataques al esquema de cifrado utilizado por la última generación de teléfonos 4G**
- **2. Acceso a los datos en claro de uno de los proveedores mundiales más importantes (¿Skype?) de llamadas de voz a través de internet**
- **3. Colección de un millón de directorios personales por día de correos electrónicos de usuarios de Hotmail, Yahoo, Google y Facebook.**
- **4. Desciframiento de conexiones ssl (las cuales se utilizan en 90% de las transacciones de comercio electrónico a nivel mundial).**
- **5. Establecimiento de una división de inteligencia cuyo objetivo es infiltrar la industria mundial de telecomunicaciones**

A manera de conclusiones, en su archifamoso cuento fantástico *El Aleph*, el escritor argentino Jorge Luis Borges, planteó la existencia de un objeto esférico de unos dos o tres centímetros de diámetro en el cual están, sin confundirse, todos los lugares del orbe, vistos desde todos los ángulos y en el que el todo no es mayor que ninguna de las partes. Borges (el personaje) nos refiere que en el aleph se ven a un tiempo, una infinidad de actos deleitables o atroces, todos ocupando un mismo punto, sin superposición ni transparencia. Borges (el escritor) incluye una nota final en la que se afirma que en el inconcebible aleph se refleja el universo entero. En su intento por vigilar al planeta, la NSA, la agencia que no es, quiere ser el aleph.



Desarrollo de Sistemas Robóticos

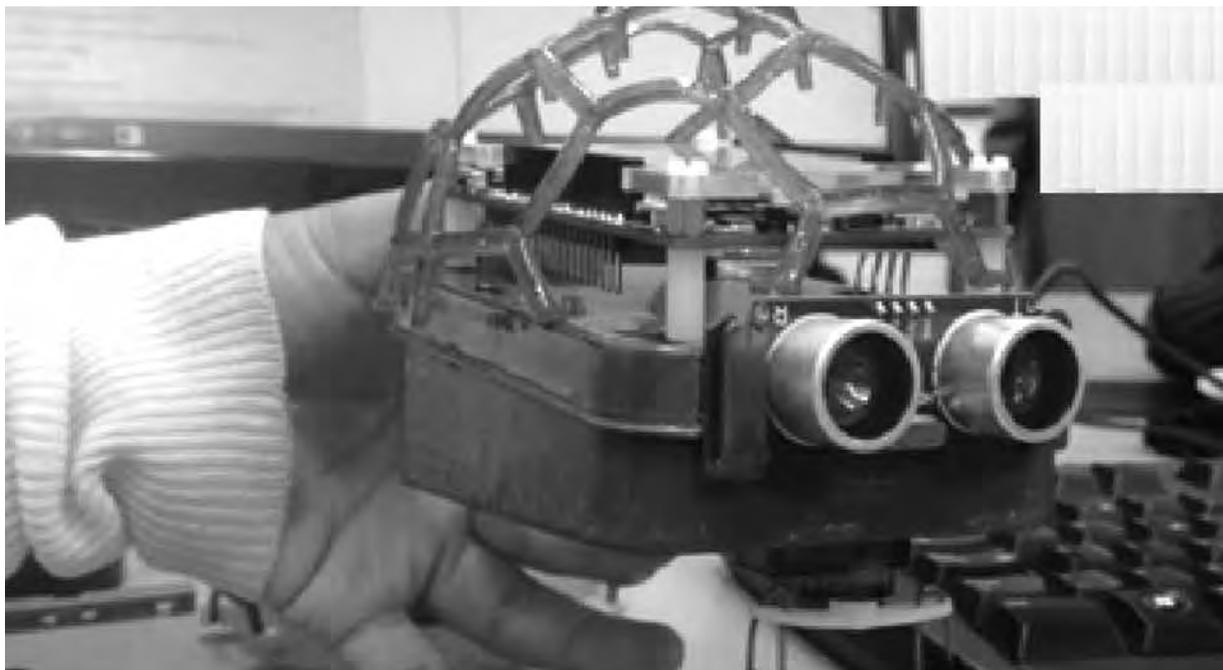
José Luis Hernández Ameca, Jessica Rocha Ruiz, Alan Joshep Fonseca Barrera,
Víctor Manuel Coatl Coyotl y Miguel Ángel Márquez Carrillo
Facultad de Ciencias de la Computación

El Laboratorio de Sistemas Robóticos, dirigido por el M. C. José Luis Hernández Ameca, de la Facultad de Ciencias de la Computación, se dedica al desarrollo de robots didácticos, de competencia y prototipos que pretenden resolver problemas de la vida real. Desde el punto de vista de la teoría de control, se puede considerar al robot como “un conjunto de elementos organizados que interactúan para lograr un fin común, que responde de manera ‘inteligente’ mediante acciones y algoritmos a las magnitudes que es capaz de detectar”. Por lo tanto se puede considerar como un sistema integrado por varios subsistemas, entre los que se pueden destacar los siguientes:

Sistema de captación de señales de entrada: principalmente compuesto por diversos tipos de dis-

positivos, diseñados para detectar magnitudes físicas (como posición, masa, longitud, movimiento, velocidad, aceleración, tiempo, temperatura, intensidad luminosa, etc.) y transformar estas magnitudes en señales eléctricas manipulables. Estos dispositivos, llamados sensores, son los encargados de recolectar la información que procesará el sistema de control.

Sistema de control: en esta etapa se mantiene la respuesta del sistema dentro de ciertos rangos de valores deseados, lo que se logra mediante algoritmos computacionales que miden, comparan, guardan y procesan la información recibida del sistema de captación. Los algoritmos computacionales se implementan en dispositivos de estado sólido como minicomputadoras, microcontroladores y una gran variedad de dispositivos lógicos pro-



gramables; los cuales hacen posible que el tratamiento de la información se realice en tiempos cada vez menores dependiendo de su arquitectura.

Sistema de accionamiento: Se compone de dispositivos que convierten una señal de un tipo de energía a otra, llamados transductores, y de elementos capaces de transformar energía hidráulica, neumática o eléctrica en energía mecánica, nombrados actuadores. Los transductores y actuadores fungen como elementos finales del control, permitiendo llevar a cabo las acciones del comportamiento final del robot. A continuación se describen algunos de los robots que el M. C. José Luis Hernández Ameza y su equipo de estudiantes pertenecientes a la ingeniería en ciencias de la computación han desarrollado dentro del laboratorio de Sistemas Robóticos.

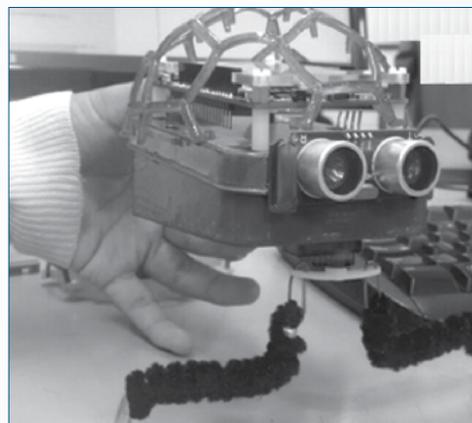
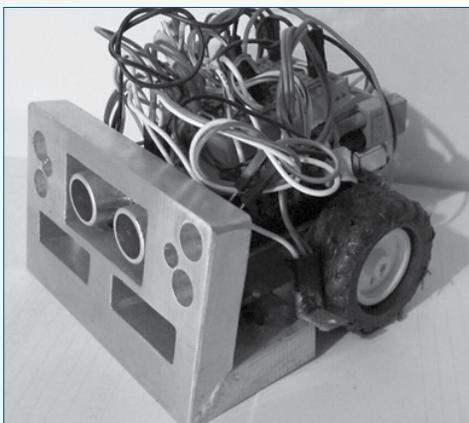
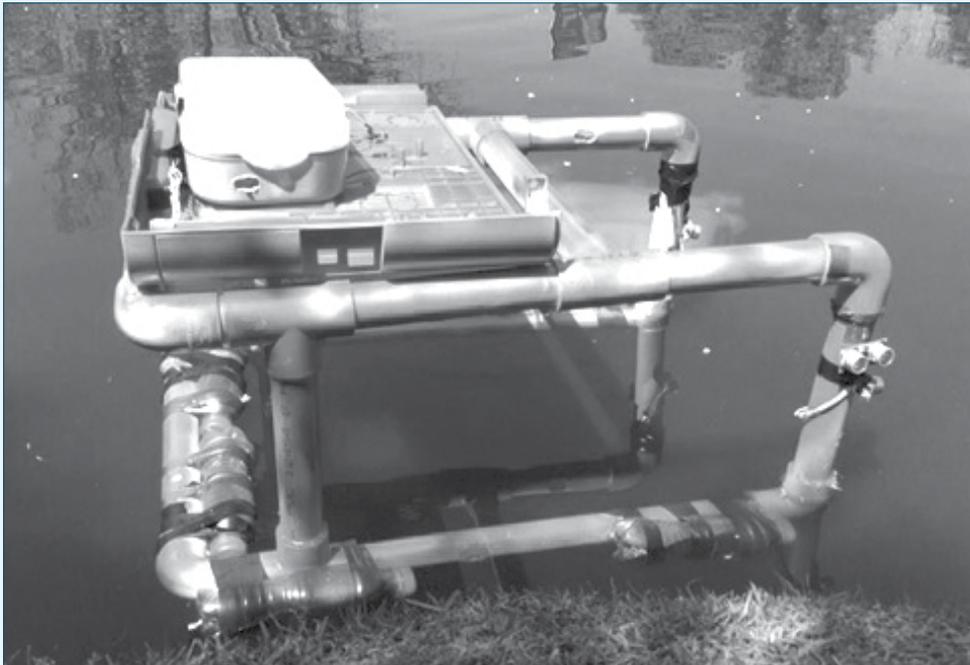
Robot didáctico cuadrúpedo

Es un prototipo diseñado para realizar exploración de terrenos y reconocimiento de objetos en ambientes inhóspitos u hostiles para el ser humano. Cuenta con dos sensores para el reconocimiento de objetos, un sistema de control implementado en un circuito integrado de última generación llamado FPGA, acrónimo de Field Programmable Gate Array, y cuatro servomotores acoplados cada uno a las patas del robot para su locomoción

Robots de competencia

Sumobots: Son robots basados en el sumo japonés, donde dos contrincantes se enfrentan con el objetivo de empujar a su oponente hasta sacarlo del área circular donde se lleva a cabo el combate, llamada *dohyo*. De igual forma los robots de sumo o *sumobots* deben localizar, seguir, y sacar de esta área a su adversario. Esta competencia se ha diversificado según el tamaño, peso y tipo de control que poseen los robots, ya sea autónomo o por radio frecuencia, dando como resultado las categorías de competición a nivel internacional conocidas como, megasumos, sumos medianos, minisumos y microsumos.

El minisumo que se ha desarrollado cuenta con características propias de su categoría como, masa total de 500 gramos, longitud y ancho de diez centímetros; detecta oponentes mediante sensores ultrasónicos montados en la parte frontal y límites del área de combate con sensores ópticos colocados bajo su base. La autonomía del móvil se programa en un micro controlador, la programación puede realizarse en lenguajes de alto, medio y bajo nivel, dependiendo de la arquitectura del micro controlador, en este caso se implementaron estrategias de ataque, búsqueda y defensa. La movilidad del robot depende de factores como la fricción de las llantas contra la superficie del área de combate, el engranaje de los minimoto reductores que las impulsan y el consumo de corriente y



voltaje que dan velocidad y fuerza. La alimentación de voltaje y corriente para todo el sistema proviene de una batería de polímero de litio debido a su potencia, densidad de energía, tasa de descarga, masa y longitud.

Prototipos que buscan resolver problemas de la vida real

Robot recolector de basura acuático:

En esta primera versión el robot realiza un recorrido autónomo por una superficie acuática; en particular, las pruebas se han realizado en la laguna ubicada en ciudad universitaria, a su paso el robot recolecta

todo objeto que flota sobre la superficie. La estructura robótica está hecha de tubos de policloruro de vinilo, comúnmente conocidos como PVC, ocho sensores de distancia, tres motores acuáticos y una minicomputadora como sistema de control. Ya que en un futuro se pretende que el robot pueda comunicarse con otros robots, identificar objetos, enviar su localización e información sobre su entorno.

Agradecemos el apoyo a nuestra dirección y a la Vicerrectoría de Extensión y Difusión de la Cultura por invitarnos a exponer estos y otros proyectos en las Caravanas Universitarias.



Estudiantes e investigadores

Por este medio, los invitamos a participar en la revista de divulgación científica *Spinor*, editada por la Dirección de Divulgación Científica de la Vicerrectoría de Investigación y Estudios de Posgrado de nuestra universidad.

El principal objetivo de la revista es abrir un espacio para la difusión del quehacer científico en las diversas unidades académicas, así como reseñar el panorama científico histórico actual. Es por esto que los invitamos a escribir un artículo con carácter de divulgación

sobre sus actividades de investigación y someterlo para publicación.

A los interesados les pedimos envíen su artículo al correo electrónico de divulgación: **viep@correo.buap.mx**.

Esperamos su respuesta a esta invitación, para cualquier aclaración al respecto puede comunicarse con nosotros a la misma dirección de correo o al tel. 229.55.00 ext. 5729.

Atentamente
Dirección de Divulgación
Científica, VIEP.

Feria de proyectos, impulsor de estudiantes innovadores

M. C. Yalú Galicia Hernández.
 Profesor-investigador
 Facultad de Ciencias de la Computación BUAP

El propósito de la Feria de Proyectos (FePro) es empoderar a nuestra comunidad estudiantil a través de impulsarlos a desarrollar proyectos tecnológicos con impacto social, económico o científico.

Inicialmente, FePro se visualizó como un espacio donde los alumnos pudieran presentar, por iniciativa propia y sin calificación de por medio, sus proyectos finales de curso. En lugar de guardarlos y olvidarlos una vez que obtenían una calificación, se les animaba a continuar trabajando con ellos, hacerlo crecer, innovarlos y enfocarlos a solucionar algún problema específico.

FePro cambió a una competencia en diferentes categorías que premia a los tres primeros lugares. Los premios son otorgados principalmente por amables patrocinadores quienes han confiado en nosotros y se han unido a este esfuerzo, principalmente empresas de tecnologías de la información, tanto pequeñas como de talla mundial, como: Microsoft, Linux, BigData, Hp, Intel, Ty Systems, VW, entre otras. Así también como las dependencias de la BUAP (VIEP, DAPI, DAE, VD, HUP, etc.), editoriales como: AlfaOmega, McGraw-Hill, Oxford, Fomento Editorial, BUAP, Prentice Hall, JhonWilly and Sons, John Wiley, entre otras. Los patrocinadores participan como parte del jurado evaluador, imparten conferencias o talleres, lo que permite el contacto directo

con los estudiantes, para lograr un ganar-ganar. Con el propósito de motivar y dotar de equipo de desarrollo tecnológico a la comunidad estudiantil, se han solicitado premios tales como: laptops, smartphones, tablets, tarjetas de desarrollo, iPads, Xboxs, Oculus Rift, libros especializados, becas estudiantiles para cursos, talleres y certificaciones en: Microsoft, Cisco, Oracle, Intel, etcétera.

Actualmente, FePro es plataforma de lanzamiento, ya que a través de convenios se otorgan "acreditaciones" y financiamientos totales o parciales a los estudiantes ganadores para participar en competencias nacionales e internacionales. Uno de los objetivos de impulsar esta actividad es brindar la oportunidad al estudiante para que cambie su vida, al abrir horizontes, su visión y perspectiva de futuro; ayudándolos a ser innovadores, competitivos, seguros de sí mismos. En este tipo de competencias y concursos, los ganadores de la FCC, han hecho un destacado papel y obtenido muchas veces primeros lugares, honrando el apoyo que se les otorga para poder viajar. Compartiendo a su vez estas experiencias a sus compañeros y motivándolos así a que nuevas generaciones participen también y se enfrenten a retos cada vez más difíciles y complejos.

La ciudad de Puebla es un referente a nivel nacional por albergar a diferentes universidades con prestigio nacional e internacional, y FePro 2016 ¡Levemos anclas!, en su novena edición (<http://Fepro.cs.buap.mx/2016/>), busca llevar y compartir experiencias de estos años, empoderando estudiantes de la comunidad universitaria BUAP y que impacte en la región. Adicionalmente, en este año, FePro ha tomado el reto de impulsar la generación de talentos en áreas tecnológicas a través de promover el gen emprendedor y la responsabilidad social, por medio de proyectos multidisciplinarios.

9^{NA} COMPETENCIA



LEVEMOS ANCLAS!

8.9.10
SEPTIEMBRE

COMPLEJO
CULTURAL
UNIVERSITARIO

fepro.cs.buap.mx



Twitter
@fePro...



Instagram
Feria de Proyectos



Facebook
Feria de Proyectos
FP: FePro



YouTube
FeriaBUAP



BUAP

Facultad de Ciencias
de la Computación



PROGRAMAS DE FOMENTO A LA INVESTIGACIÓN

PRESENTACIÓN DE CARTELES
19 DE SEPTIEMBRE 2016

JÓVENES INVESTIGADORES
OTOÑO VII (2015)

JÓVENES INVESTIGADORES
PRIMAVERA XI (2016)

LA CIENCIA EN TUS MANOS XVI
(2016)

VERANO DE TALENTOS XIV
(2016)

