RISCE Revista Internacional de Sistemas Computacionales y Electrónicos

Julio 2011
Número 4, Volumen 3, Año 3

ESCOM

75 Años
INSTITUTO POLITÉCNICO NACIONAL
1936-2011

IPN

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos; es una publicación bimestral del Instituto Politécnico Nacional, Av. Luis Enrique Erro S/N, unidad "Profesional Adolfo López Mateos", Del. Gustavo A. Madero, C.P. 07738, México D.F. a través de la Escuela Superior de Computo; Av. Juan de Dios Bátiz S/N esquina Miguel Othón de Mendizábal. "Unidad Profesional Adolfo López Mateos". Col. Lindavista C.P. 07738, México, D. F. tel. 57296000 ext. 52000. Certificado de reserva de Derechos al uso Exclusivo del título No. 04-2008-062613190500-203, ISSN en trámite. Los artículos son responsabilidad exclusiva del autor y no reflejan necesariamente el criterio de la institución, a menos que se especifique lo contrario. Se autoriza la reproducción total o parcial, siempre y cuando se cite explícitamente la fuente.
La revista se especializa en el área de los sistemas computacionales y electrónicos; tanto en el desarrollo, como en la investigación en:

Ciencias de la Computación
Cómputo educativo
Cómputo Móvil
Comunicaciones
Disciplinas Emergentes
Electrónica
Física Electrónica
Ingeniería de Cómputo
Ingeniería de Software
Innovación Tecnológica
Inteligencia artificial
Matemática computacional
Procesamiento de señales
Robótica y cibernética
Sistemas de Información
Tecnologías de la Información

Distribución
La revista cuenta con 300 ejemplares que se distribuyen en:
Europa, Asía y América Hispana; mediante CD ROM y correo electrónico

Directorio

INSTITUTO POLITÉCNICO NACIONAL

DRA. YOLOXÓCHITL BUSTAMANTE DÍEZ
DIRECTORA GENERAL

ING. JUAN MANUEL CANTÚ ALVAREZ
SECRETARIO GENERAL

DR. EFREN PARADA ARIAS
SECRETARIO ACADEMICO

DR. JAIME ALVAREZ GALLEGOS
SECRETARIO DE INVESTIGACIÓN Y POSGRADO

ING. ERNESTO MERCADO ESCUTIA
SECRETARIO DE SERVICIOS EDUCATIVOS

ING.OSCAR JORGE SÚCHIL VILLEGAS
SECRETARIO DE EXTENSIÓN E INTEGRACION SOCIAL

M. EN C. FERNANDO ARELLANO CALDERON
SECRETARIO DE GESTION ESTRATEGICA

C.P. ROBERTO ALVAREZ ARGUELLES
SECRETRARIO DE ADMINISTRACION

LIC. JUDITH CLAUDIA RODRIGUEZ ZUÑIGA
DEFENSORA DE DERECHOS POLITECNICOS

ESCUELA SUPERIOR DE CÓMPUTO

ING. APOLINAR FRANCISCO CRUZ LÁZARO
DIRECTOR

DR. FLAVIO ARTURO SÁNCHEZ GARFIAS
SUBDIRECTOR ACADÉMICO

DR. JESÚS YALJÁ MONTIEL PÉREZ
JEFE DE LA SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

LIC. ARACELI LOYOLA ESPINOSA
SUBDIRECTORA DE SERVICIOS EDUCATIVOS E INTEGRACIÓN SOCIAL

M. EN C. JUAN VERA ROMERO
SUBDIRECTOR ADMINISTRATIVO

DR. EDUARDO BUSTOS FARÍAS
EDITOR DE RISCE

Miembros del comité Revisor

(Todo el comité técnico está formado por doctores en ciencias o su equivalente)

Francisca Losavio de Ordaz (Venezuela) (Universidad Central de Venezuela)
Alfredo Matteo (Venezuela) (Universidad Central de Venezuela)
Emmanuel F. Moya Anica (México)
Edgardo Manuel Felipe Riverón (Cuba) (México) (CIC)
Luis Enrique Palafox Maestre (México)
Eduardo F. Caicedo Bravo (Colombia)
Hilda Ángela Larrondo (Argentina)
Guillermo Leopoldo Kemper Vásquez (Perú)
Elizabeth León Guzmán (Colombia)
María Cecilia Rivera (Chile)
Satu Elisa Schaeffer (Finlandia) (UANL)
Rafael Canetti (Uruguay)
Javier Echaiz (Argentina)
Pablo Belzarena (Uruguay)
Carlos Beltrán González (Italia) (Universitá di Genova)
Elena Fabiola Ruiz Ledesma (México)
Jonatan Gómez (Colombia)
Armando De Giusti (Argentina)
Juan José Torres Manríquez (México)
Jesús Yaljá Montiel Pérez (México)
Luis Alfonso Villa Vargas (México)
Marco Antonio Ramírez Salinas (México)
Félix Moreno González (España) (UPM)
Salvador Godoy Calderón (México) (CIC)
José Luis López-Bonilla (México) (IPN ESIME ZAC)
Lorena Chavarría Báez (México)
Miguel Santiago Suárez Castañón (México)

INDICE

INTEGRACION DE UN SISTEMA DE VISIÓN PARA LA DETECCIÓN DE OBJETOS DEL ROBOT PARALLIX LKF-2040

Tópico: Robótica y Cibernética

Trejo Becerra Ana Gabriela
(Responsable de comunicación)
Instituto Tecnológico de Querétaro
Av.Tecnológico s/n Esq. M. Escobedo Col.Centro
76000 Querétaro, Qro. México.
+52 (442)2 27 44 00
e-mail: gab_ross@hotmail.com

Castillo Castañeda Eduardo
Instituto Politécnico Nacional, CICATA
+52 (442) 2282904 Ext. 81013
Cerro Blanco #141 Colinas del Cimatario
76090- Queretaro, Mexico
e-mail: ecastilloca@ipn.mx

Resumen:

El robot de tipo paralelo PARALLIX LKF-2040 fue desarrollado en el CICATA-IPN con fines didácticos y ha sido transferido a instituciones educativas nacionales y extranjeras desde 2008. El robot puede realizar desplazamiento articular o cartesiano, guardar puntos y seguir secuencias de desplazamientos predeterminadas por el usuario. Actualmente el CICATA busca incursionar en el mercado industrial ofreciendo tecnología de calidad fabricada en México a las industrias manufactureras del país. Este trabajo presenta el desarrollo de un sistema de visión por computadora para convertir este robot en una versión más robusta e integrarle capacidad sensorial que le permita la detección automática de objetos. Las imágenes de este sistema de visión son adquiridas mediante una cámara web y procesadas por una PC con ayuda del software propiamente diseñado en este proyecto. Así se obtiene una coordenada que indica al robot paralelo dónde posicionarse para tomar el objeto identificado.

Palabras clave- Robot paralelo, Detección de contornos, Sistema de Visión .

***Resumen*— El robot de tipo paralelo PARALLIX LKF-2040 fue desarrollado en el CICATA-IPN con fines didácticos y ha sido transferido a instituciones educativas nacionales y extranjeras desde 2008. El robot puede realizar desplazamiento articular o cartesiano, guardar puntos y seguir secuencias de desplazamientos predeterminadas por el usuario. Actualmente el CICATA busca incursionar en el mercado industrial ofreciendo tecnología de calidad fabricada en México a las industrias manufactureras del país. Este trabajo presenta el desarrollo de un sistema de visión por computadora para convertir este robot en una versión más robusta e integrarle capacidad sensorial que le permita la detección automática de objetos. Las imágenes de este sistema de visión son adquiridas mediante una cámara web y procesadas por una PC con ayuda del software propiamente diseñado en este proyecto. Así se obtiene una coordenada que indica al robot paralelo dónde posicionarse para tomar el objeto identificado.**

Palabras clave- Robot paralelo, Detección de contornos, Sistema de Visión .

I. Introducción

El uso de la visión por computadora está motivado por la constante necesidad de aumentar la flexibilidad y los campos de aplicación de los sistemas de robótica. La visión es considerada la capacidad sensorial más potente del robot.

Empleando una cámara como sensor visual, es posible obtener la información del entorno en forma de imágenes y así controlar el efector final de un robot durante la realización de una tarea de manera no intrusiva en el proceso. Las aplicaciones robóticas en entornos estructurados con presencia de objetos cuya posición y orientación no es perfectamente conocida, son áreas de oportunidad para la integración de los sistemas de visión.

El robot PARALLIX LKF-2040 es un robot de tipo paralelo construido con fines didácticos en el centro de investigación de tecnología avanzada y ciencia aplicada, CICATA. En su versión actual, el robot no reconoce objetos, únicamente ejecuta secuencias de puntos previamente establecidas por el usuario. Este trabajo presenta el desarrollo de un sistema de visión por computadora para convertir este robot en una versión más robusta e integrarle capacidad sensorial que le permita la detección automática de objetos.

Con este trabajo se pretende dar un valor agregado al robot y posteriormente promoverlo en la industria nacional. Por lo tanto se busca diseñar un sistema de visión que sea compatible con la programación del robot paralelo PARALLIX LKF-2040 y brinde las coordenadas de los centros de los objetos detectados para posicionarlo correctamente.

En su versión actual, el robot se programa a través del la Interface Gráfica Usuario ROBWIN Versión 4.0, desarrollada en CICATA-IPN.

II. El robot Parallix lkf-2040

A. Descripción

El PARALLIX LKF-2040 es un manipulador con estructura de Mecanismo Paralelo [1] con tres grados de libertad manufacturado en el IPN-CICATA unidad Querétaro, ver figura 1, actualmente se encuentra en vías de desarrollo para ser introducido al mercado industrial.

Figura 1. Robot PARALLIX LKF-2040

Este mecanismo posee una plataforma fija y otra móvil. Los actuadores están orientados en la plataforma fija, reduciendo el cableado y manteniéndolo fuera del espacio de trabajo. La plataforma móvil es el elemento efector y puede ser

posicionada en un amplio espacio de trabajo. La estructura del manipulador es ligera, simplificando la dinámica y minimizando el peso a desplazar. Lo anterior, permite utilizar el par generado por los motores sólo para el desplazamiento de la carga. El robot PARALLIX LKF-2040 tiene sus orígenes en la configuración delta [2]. Las ventajas que presenta el PARALLIX LKF-2040 con respecto al robot delta es el tipo de articulaciones que en este caso son rotacionales para permitirle un espacio de trabajo más amplio.

Los componentes esenciales del controlador del robot son cinco tarjetas, tres tarjetas tipo PIC-SERVO SC [3], una tarjeta SSA-485, y una tarjeta tipo PIC-IO, ver figura 2. La SSA-485 es una tarjeta convertidora de USB/RS232 a RS485 que le permite comunicarse con los módulos en general y en particular con el NMC y las tarjetas PIC-SERVO SC y PIC-IO, a través del puerto USB de la PC.

Figura 2. Gabinete del controlador del robot

La tarjeta PIC-SERVO SC proporciona un control de lazo cerrado PID para los motores marca MAXON de CD de 24 volts, 3.36A a través de los encoders incrementales que posee.

Como efector final posee una ventosa plana (VAS-40-1/4 NBR) de 40 mm marca FESTO que tiene 32mm de succión efectiva.

B. Interfaz Gráfica Usuario, ROBWIN Versión 4.0

Esta interface gráfica, denominada ROBWIN, permite a un usuario la comunicación con el controlador del robot para operar el control de movimiento. ROBWIN Versión 4.0 cuenta con 5 grupos de comandos organizados en el mismo número de ventanas.

Las opciones principales indican al usuario la secuencia que debe seguirse para efectuar movimientos en el robot. El primer paso de la secuencia es la opción INICIAR CONEXIÓN USB, el último paso es la opción SALIR.

Puede seleccionar la velocidad y aceleración con las que el robot PARALLIX LKF-2040 ejecutará los desplazamientos, así como el tipo de desplazamiento que se desea utilizar, ya sea articular o cartesiano. El tipo articular es para posicionar cada motor según el número de cuentas que se desee, donde cada cuenta equivale a 0.064° del motor. En el tipo cartesiano, se especifica una o varias coordenadas (x, y, z) en mm a las que se desea llegar y es posible guardar y ejecutar una rutina de movimiento.

En el último bloque se pueden modificar los parámetros del control PID; es decir, las ganancias Kp, Kd y Ki para cada uno de los tres motores.

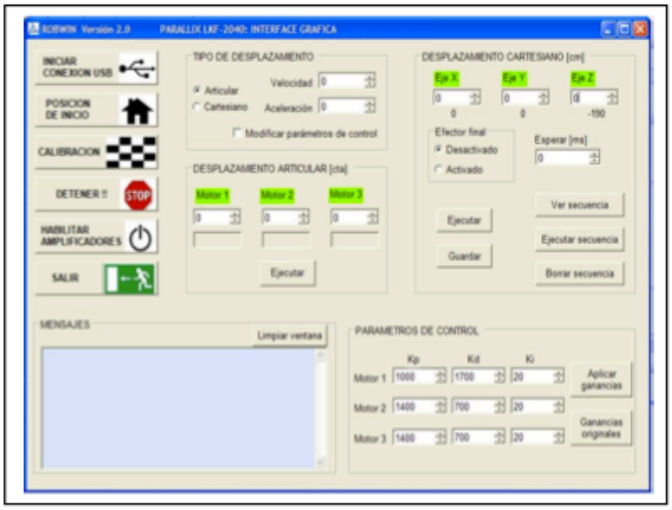


Figura 3. Interface gráfica original del PARALLIX

III. PROGRAMA DEL SISTEMA DE VISION

Es el responsable de procesar las imágenes capturadas por una cámara. Durante el análisis, el programa utiliza diversas herramientas para lograr otorgar una coordenada (x, y) correspondiente al centro de gravedad del objeto detectado.

El programa del Sistema de Visión se realizó en el lenguaje de programación de Visual C++ 2005 [4], ya que es el lenguaje de programación del robot PARALLIX LKF-2040 y se complementó con diversas librerías de OpenCV [5], [6] y [7]. Los pasos que se consideraron para la elaboración del mismo fueron:

- Adquirir imagen: Se busca obtener imágenes en tiempo real del entorno.
- Binarizar la imagen: Una vez obtenidas las imágenes es necesario convertirlas en matrices binarias para posteriormente aplicar técnicas de detección de contornos [8].
- Detectar objetos y sus contornos: El método utilizado es el de los Vectores de Freeman [9].
- Desplegar contornos: Una vez identificados, muestra visualmente sobre una pantalla en Visual C++ los contornos encontrados.
- Calcular el centro de gravedad del objeto a partir de su contorno trazando una cruz en el centro del objeto.
- Aplicar una transformación homogénea a la coordenada de la imagen para hacerla compatible con el sistema de referencia del robot. Además, dado que la coordenada obtenida tiene como unidad el pixel, debe ser

transformada a la unidad de milímetros para hacerla compatible con las unidades manejadas para describir los desplazamientos del robot.

Este último punto se detalla a continuación.

A. *Transformación de coordenadas de la cámara*

Un punto P' (coordenada del robot) está relacionado con un punto P (coordenada de la cámara) de esta manera:

$$P' = \begin{bmatrix} R_{3x3} & T_{3x1} \\ 0 & 1 \end{bmatrix} * P \qquad (1)$$

La matriz homogénea requerida para relacionar estos puntos, está compuesta por una submatriz de 3x3 de rotación y una de 3x1 de traslación, así como de un vector fila de 1x3 de perspectiva y un componente unitario que indica el escalamiento.

Esta ecuación también puede ser expresada como:

$$\begin{bmatrix} X' \\ Y' \\ Z' \\ 1 \end{bmatrix} = \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} X \\ Y \\ Z \\ 1 \end{bmatrix} \qquad (2)$$

Si se considera que las coordenadas de los puntos P' y P son datos conocidos, se puede obtener el siguiente conjunto de ecuaciones:

$$X' = aX + bY + cZ + d \qquad (3)$$

$$Y' = eX + fY + gZ + h \qquad (4)$$

$$Z' = iX + jY + kZ + l \qquad (5)$$

Cuatro pares de puntos correlacionados son suficientes para obtener un sistema de 12 ecuaciones con 12 incógnitas. Dichos puntos correlacionados se obtuvieron experimentalmente comparando la coordenada otorgada por el sistema de visión y la coordenada correspondiente a la ubicación del robot PARALLIX LKF-2040.

El determinante de una matriz homogénea es 1, por lo que al sistema se le debe añadir otra ecuación:

$$afk + bgi + cej - bek - agj - cfi = 1 \qquad (6)$$

Con ayuda de MATLAB, se resolvió el sistema no lineal obteniendo la matriz:

H=

$$\begin{bmatrix} -1.6670 & -0.0056 & -0.5724 & -0.1765 \\ 0.0126 & 1.4917 & -0.4525 & 0.9977 \\ 0 & 0 & -0.4022 & 420.6466 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Así las ecuaciones resultantes para obtener la coordenada de los objetos son:

$$X' = -1.6670x - 0.0056y - 0.5724z - 0.1765$$

$$Y' = 0.0126x + 1.4917y - 0.4525z + 0.9977$$

$$Z' = -0.4022z + 420.6466$$

El método empleado para detectar el centro de los objetos puede ser considerado como una aproximación muy cercana al centro real del objeto y en este caso resulta suficiente dado que el efector final es una ventosa de 32 mm de diámetro de succión.

IV. CÁMARA USB

La cámara que se instaló en el área de trabajo del PARALLIX LKF-2040 fue una cámara web Microsoft LifeCam Show de 33 x 62 mm, con una resolución de 2.0 megapixeles y una captura de video de 800 x 600 pixeles. Su frecuencia de cuadro es arriba de 30 cuadros por segundo y transfiere las imágenes a través de un puerto USB 2.0 de alta velocidad. La adquisición de las imágenes de la cámara se realizó utilizando librerías de OpenCV programadas en lenguaje Visual C++. La resolución final de la cámara para esta aplicación fue de 0.6 pixeles por milímetro.

V. SISTEMA DE ILUMINACIÓN

Los componentes ópticos como las fuentes iluminadas son utilizados para enfatizar las características de los objetos a procesar. Esto da como resultado la obtención de imágenes bien definidas, homogéneas e inmunes a las variaciones luminosas del medio ambiente [10].

Se elaboró una base iluminada, como se observa en la Figura 4, utilizando una matriz de LEDS de 5 volts, para favorecer el reconocimiento de contornos de los objetos, ver Figura 5. Así se producen imágenes sin matices en blanco y negro al iluminar la parte posterior del objeto.

Figura 4. Fuente de iluminación construida

La base iluminada se ubicó en la parte inferior derecha del robot. De esta manera, los objetos quedan a una altura Z=300, según el sistema de referencia del robot. Este valor fue elegido de acuerdo al espacio de trabajo del robot PARALLIX LKF-2040, ver Figura 9. Cabe recalcar que Z se considera conocida dado que el sistema de detección de objetos brinda los valores de la coordenada (x, y) de los objetos pero no de Z.

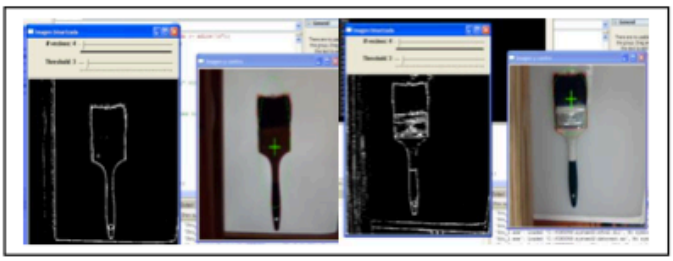


Figura 5. Objeto iluminado(izquierda) y objeto no iluminado(derecha)

VI. INTEGRACIÓN DE LA INTERFACE VISUAL

Se modificó la interface ROBWIN Versión 4.0 añadiéndole los botones necesarios para extraer y usar las coordenadas del centro de los objetos detectados con el sistema de visión, ver Figuras 6 y 8. Al oprimir el botón de ABRIR IMAGEN se abre la ventana que muestra la imagen binarizada, ver Figura 7-a. En ella es posible modificar los dos valores (# vecinos y constante de Threshold) que afectan el valor del Threshold adaptable. Así se obtienen contornos más nítidos y se pueden eliminar algunos brillos que prevalezcan a pesar del uso de la fuente iluminada.

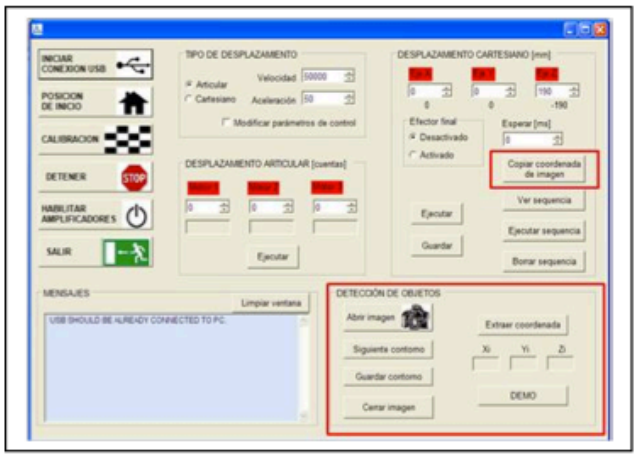


Figura 6. Modificaciones en la interface resaltadas

Con el botón EXTRAER COORDENADA se abre la ventana que muestra a colores y en tiempo real los objetos detectados, ver Figura 7-b. En la parte inferior derecha se muestra la coordenada (x, y, z) del objeto seleccionado. Con esta ventana abierta, puede seleccionarse el objeto de nuestro interés oprimiendo el botón de "Siguiente contorno" hasta que el contorno y cruz dibujados se encuentren sobre el objeto deseado.

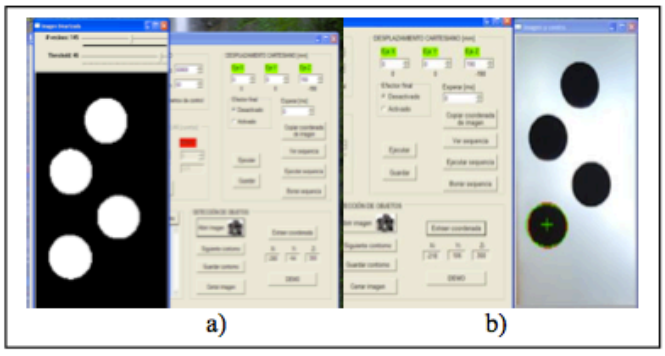


Figura 7. Ventanas de la detección de objetos.

Con el botón GUARDAR CONTORNO se genera un archivo de texto en la carpeta donde se ejecuta el programa de la interfaz. En dicho archivo se guardan todas las coordenadas que conforman el contorno seleccionado.

Seleccionando el modo CARTESIANO del robot, se activa la parte superior derecha de la interfaz. Al oprimir el botón "Copiar coordenada", la coordenada (x, y, z) obtenida con el sistema de visión se coloca en las casillas de los ejes x, y, z del Robot ubicados en la parte superior. De esta manera es posible incluir la coordenada de la detección de objetos en una secuencia determinada por el usuario.

Figura 8. Bloque de Detección de objetos de la interfaz

La opción DEMO, contiene una subrutina predeterminada en la que toma los 4 primeros objetos que detecta el sistema de visión y los coloca en las coordenadas: (200,-50), (200,20), (200,90), (200,160).

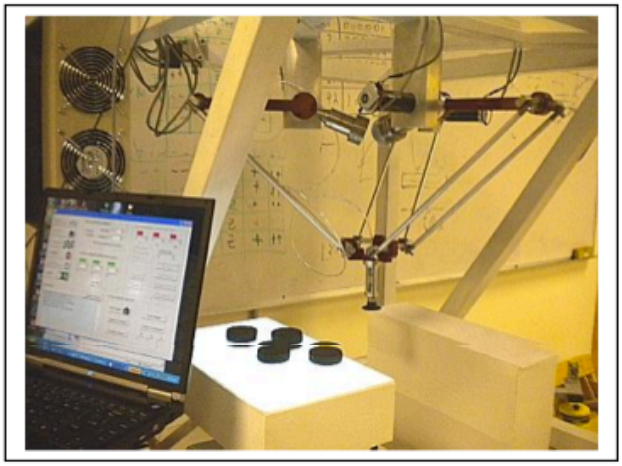


Figura 9. Sistema completo

CONCLUSIONES

Fue posible elaborar un sistema de visión que es compatible con la programación del robot paralelo PARALLIX LKF-2040, detecta objetos y brinda las coordenadas de los centros para tomarlos. El centro detectado es una aproximación al centro de los objetos que es suficiente para cubrir el objetivo de posicionar al robot correctamente y sujetar el objeto con su efector final (la ventosa).

Las pruebas muestran que el sistema de visión es exacto para objetos regulares y localiza un buen punto de sujeción para objetos irregulares. La resolución de la cámara web, 800 x 600 pixeles, brinda una coordenada del centro de los objetos detectados que resulta adecuada para la sujeción de los mismos. La base iluminada elaborada mejora la detección de los contornos de los objetos y por lo tanto, la localización del centro de los mismos. Al controlar las condiciones de

iluminación del sitio donde se implementa el sistema de visión, se favorece la detección de contornos y se elimina la detección de elementos despreciables como reflejos de otras lámparas.

Este sistema de visión será transferido a los actuales usuarios del robot PARALLIX LKF-2040 ya que su costo es únicamente una el de una cámara convencional del tipo USB. La continuación de esta investigación consiste en identificar y tomar objetos en movimiento en tiempo real. Esto se logrará al sincronizar la velocidad del robot con el sistema de visión generado e integrar también una banda transportadora.

AGRADECIMIENTOS

Los autores de este trabajo agradecen al Instituto de Ciencia y Tecnología del Distrito Federal por el financiamiento otorgado para la realización de este trabajo, mediante el proyecto con número de registro PIFUTP08-159, del Fondo de Fomento al Uso de Tecnologías de Punta en la Investigación Científica y Tecnológica del Gobierno del Distrito Federal.

REFERENCIAS

[1] Tsai, L.-W. (1999). Robot Analysis, The Mechanics of Serial and Parallel Manipulators, Ed.Wiley-Interscience.

[2] Clavel, R. (1990). Patent No. 4,976,582. EUA.

[3] PIC-SERVO Motion Control http://www.jrkerr.com/boards.html. Fecha de consulta: 4 de mayo de 2010.

[4] Visual C++® developing center http://msdn.microsoft.com/en-us/visualc/bb530677.aspx. Fecha de consulta: 23 de abril de 2010.

[5] Gary Bradski, Adrian Kaehler. " *Learning OpenCV*". Edit. O' REILLY. E.U. 2008.

[6] Introducción al uso de OpenCV. Dr. J.B Hayet. http://www.cimat.mx/~jbhayet/CLASES/VISIONROB/opencv1.pdf . Fecha de consulta: 23 de abril de 2010.

[7] Image Processing and Analysis Reference http://www710.univ-lyon1.fr/~bouakaz/OpenCV-0.9.5/docs/ref/OpenCVRef_ImageProcessing.htm. Fecha de consulta: 6 de mayo de 2010.

[8] Tresholding (image processing) http://www.worldlingo.com/ma/enwiki/es/Thresholding_(image_processing). Fecha de consulta: 4 de mayo de 2010.

[9] H. Freeman (1974). Computer processing of line-drawing images. Comput. Surveys 6:57-97

[10] Adrian Low. "Introductory Computer Vision and Image Processing". Edit Mc Graw Hill. Pp 51-99

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 4, Volumen 3, Año 3. Julio 2011
Artículos con arbitraje

Modelado y predicción de la resistencia coronaria del sistema nervioso central con las Metodologías de Razonamiento Inductivo Difuso (CARFIR)

Pilar Gómez Miranda
Instituto Politécnico Nacional
UPIICSA – Depto. Computación
Distrito Federal, México
pgomez84@hotmail.com

Fernando Vázquez Torres
Instituto Politécnico Nacional
UPIICSA – SEPI – Informática
Distrito Federal, México
fvazquez_t@hotmail.com

Resumen— Metodología de Razonamiento Inductivo Difuso (FIR) surge de la Teoría General de Sistemas (GSPS) desarrollada por G. Klir [5], y es una herramienta que permite estudiar los modos de comportamiento de los sistemas dinámicos. Esta metodología de modelado y simulación cualitativa se basa en la observación del comportamiento del sistema más que en el conocimiento de su estructura interna. La metodología CARFIR une la metodología FIR con los sistemas difusos clásicos. El propósito esencial es extender la metodología FIR mediante la adición de un sistema de inferencia difuso para obtener un conjunto de reglas más compacto y robusto. Se trata de explorar cuanto del conocimiento capturado en las reglas patrón que genera FIR se puede conservarse en un esquema de reglas difusas clásicas. Por otro lado, desde el punto de vista de los sistemas difusos clásicos, ésta aproximación proyecta estudiar hasta que punto la metodología CARFIR puede ayudar a resolver el complejo problema de la identificación de sistemas difusos.

Palabras clave: Reglas difusas, reglas patron, sistema de inferencia difuso.

I. INTRODUCCIÓN

La metodología de razonamiento inductivo difuso (FIR) ha sido probada en diferentes campos de aplicación obteniendo buenos resultados en muchos de ellos [2, 3, 4 y 6]. La metodología FIR tiene un inconveniente importante, la base de reglas patrón generada por el proceso de modelado cualitativo es muy grande si el número de datos registrados del sistema es elevado ya que el número de reglas patrón generadas es prácticamente igual, de grande que el número de observaciones registradas del sistema. Por lo tanto, cuando el número de reglas patrón es elevado, el proceso de predicción de un nuevo valor resulta demasiado lento. La metodología CARFIR pretende abordar este inconveniente de FIR intentando capturar el conocimiento inherente en las reglas patrón en un conjunto de reglas difusas clásicas mucho más compacto.

II. ESTADO DEL ARTE.

La Metodología de Razonamiento Inductivo Difuso FIR realiza dos tareas principales [1]. La primera es identificar las relaciones causales y temporales entre las variables del sistema para construir el modelo cualitativo del sistema observado. La segunda es predecir el comportamiento futuro del sistema a partir de las observaciones pasadas y del modelo previamente identificado. Para cumplir con estas tareas, la metodología FIR cuenta con cuatro funciones básicas: fusificación, modelado cualitativo, simulación cualitativa y defusificación, como se muestra en el esquema de la figura 1. El resultado del modelado cualitativo es la base de reglas patrón que representa el conocimiento adquirido del sistema. El número de reglas patrón de FIR está directamente relacionado con la cantidad de datos de entrenamiento utilizados, por lo que, si este es extenso las reglas lo son en igual proporción, lo que ocasiona que FIR reduzca su poder en el tratamiento de problemas que cuentan con gran cantidad de datos.

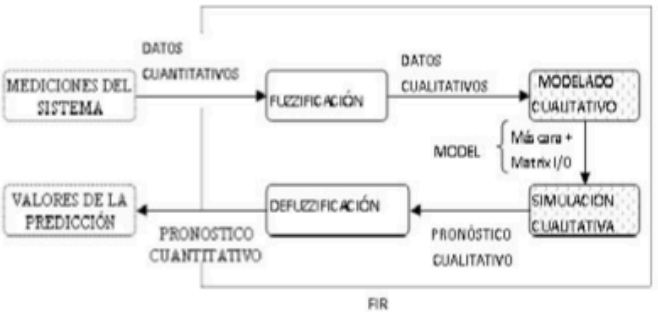


Figura 1. Representación esquemática de la metodología FIR.

III. METODOLOGÍA CARFIR.

La metodología CARFIR une la metodología FIR con los sistemas difusos clásicos. El propósito esencial es extender la metodología FIR mediante la adición de un sistema de inferencia difuso para obtener un conjunto de reglas más

compacto y robusto. Se trata de explorar cuanto del conocimiento capturado en las reglas patrón que genera FIR puede conservarse en un esquema de reglas difusas clásicas.

Como se muestra en la figura 2, la metodología CARFIR está compuesta por dos partes principales, la estructura de la metodología FIR y la estructura del sistema de inferencia difuso (FIS). CARFIR hace uso de los dos primeros procesos de FIR, la fusificación y la identificación del modelo cualitativo y ofrece una alternativa para los dos últimos (predicción difusa y defusificación) que consiste en un sistema de inferencia difuso (FIS) que permite por un lado, compactar las reglas patrón en una base de reglas difusas clásicas y, por otro lado, realizar la predicción mediante un sistema de inferencia difuso tipo Sugeno que utiliza la nueva base de reglas identificadas.

Los sistemas de inferencia difusos en la actualidad son muy utilizados, por ser sistemas que tienen la capacidad inherente de tratar con datos inexactos y producir generalizaciones válidas. La estructura básica de un sistema de inferencia difuso está compuesta de tres componentes: fusificación, inferencia y defusificación. La base de conocimiento de los sistemas difusos la componen los parámetros externos, los cuales vienen dados por las funciones de pertenencia, la base de reglas difusas, los operadores difusos, los pesos de las reglas difusas y el método de defusificación.

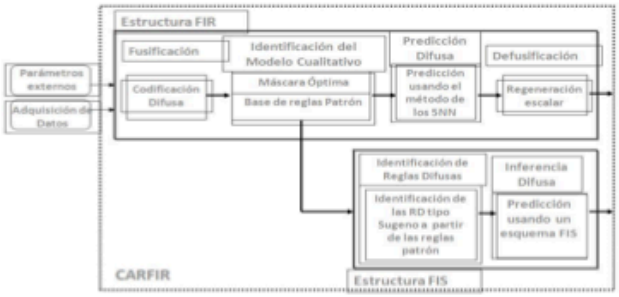


Figura 2. Representación esquemática de la metodología CARFIR.

Modelo Difuso de Sugeno en CARFIR, para generar estas reglas, CARFIR parte de la representación del comportamiento del sistema capturado en las reglas patrón que genera FIR. La base de reglas patrón está representada por una matriz donde cada renglón constituye un estado cualitativo pseudo-estático o regla cualitativa basada en patrones. El siguiente paso es la generación de las reglas difusas partiendo de la base de reglas patrón, de tal forma que se puedan ajustar automáticamente los paramentos del sistema difuso. La idea que subyace en este proceso de obtención de reglas difusas a partir de las reglas patrón se basa en la representación espacial de ambas reglas. Las reglas basadas en patrones pueden ser representadas gráficamente en el espacio de entrada/salida. Si el modelo obtenido por FIR presenta una calidad alta, las reglas patrón forman una superficie plana y uniforme en el espacio de entrada/salida. Contrariamente, si el modelo obtenido contiene mucha incertidumbre la representación espacial mostrará un plano donde el grosor en algunas zonas es más significativo que en otras. La densidad de la superficie indica que para un determinado patrón de entrada, la variable de salida puede tomar diferentes valores de clase. Esto es, las reglas basadas en patrones no son deterministas. Como se ha mencionado anteriormente, la calidad del modelo se calcula utilizando una medida de entropía que refleja el nivel de determinismo de la matriz de transición de estados asociada a la máscara y a la base de reglas patrón.

Nótese que la superficie formada por las reglas patrón (círculos) no tiene demasiado grosor y por lo tanto, la base de reglas puede considerarse bastante determinista. Vemos también, que la malla formada por las reglas difusas clásicas tipo Sugeno (cuadros) se ajusta adecuadamente a la superficie formada por la base de reglas patrón, figura 3.

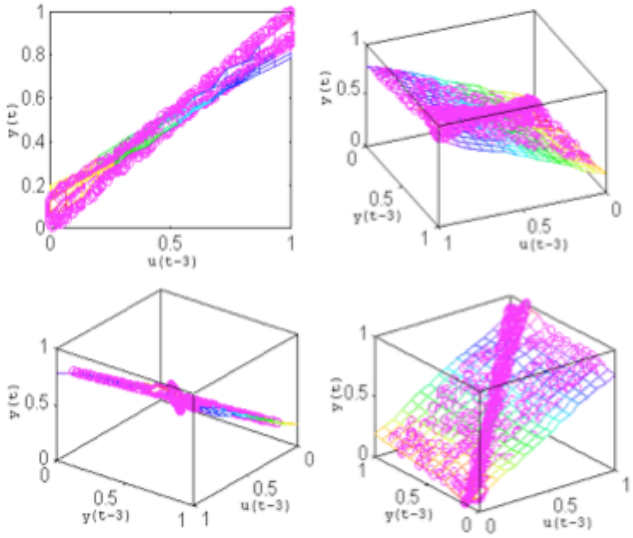


Figura 3. Sistema de reglas patrón y reglas difusas.

Proceso de Sintonización de Sugeno.

En la sintonización de Sugeno el proceso de defusificación es el encargado de asociar los pesos asociados los cuales están implícitas en el consecuente. Esto es, el consecuente de una regla difusa tipo Sugeno se obtiene al aplicar el operador difuso producto a los valores de membresia de los antecedentes de las reglas patrón; el consecuente de estas reglas es el peso asociado a la regla. Para este procedimiento se utiliza la ecuación *1*.

$$u^* = \sum_{i=1}^{n} (\mu_i \cdot w_i) / \sum_{i=1}^{n} \mu_i \qquad (1)$$

En la ecuación *1*, μ_i es el disparo de la i-ésima regla, w_i es el peso de la i-ésima regla y n es el número total de reglas del sistema. El operador difuso utilizado es el producto, que obtiene los disparos de cada regla.

Este proceso consiste en ajustar los pesos, w_i, iterando a través del conjunto de datos usando el método de gradiente descendiente. La sintonización del peso de la i-esima regla se obtiene calculando la derivada de la función de costo "E" con respecto a w_i. La función de costo está definida por la ecuación *2*, (la suma del error cuadrático), donde *ND* es el número de datos, y es el valor dado por el sistema y' es el valor real.

$$E = \frac{1}{2}\sum_{k=1}^{ND}(y - y^r)^2 \qquad (2)$$

Los parámetros externos permiten ajustar el Sistema de Inferencia difuso para relacionar, de la mejor manera posible, los valores de entrada con los valores de salida del sistema. La principal meta del proceso de sintonización es determinar el consecuente asociado a un conjunto de antecedentes. Recordemos que la estructura de una regla difusa consiste en un conjunto de antecedentes y un solo consecuente. Para la matriz de comportamiento generada por *FIR* esta condición no se cumple, ya que para un mismo conjunto de entradas existen diferentes salidas. Por lo tanto, el sistema de inferencia *Sugeno* generará para cada conjunto de antecedentes un sólo consecuente, lo cual repercute en una reducción del número de reglas patrón y un la generalización de estas.

Para este propósito el sistema de inferencia primeramente determina el espacio de entrada[1], que esta definido tomando en cuenta todos los antecedentes. Para un sistema con dos antecedentes y un consecuente se deben obtener 9 reglas difusas. Con el espacio de entrada del sistema obtenido y con las reglas patrón disponibles, las reglas son buscadas y extraídas de la matriz de comportamiento que previamente se les asocio el valor crisp de salida. El valor de salida de todas las reglas con un mismo patrón de entrada es promediado sumando el valor de salida de las reglas iguales y dividido entre el número de estas. Si alguna de las reglas del espacio de salida no se encuentra en la matriz de comportamiento, la salida de esa regla es el promedio general de los valores de salida; la figura *12, P1, P2* y *P3* son los promedios para las reglas con los mismos antecedentes y *PG* es el promedio general. Lo que genera las reglas difusas aproximadas; estas reglas trazan una malla a través de los puntos de las reglas numéricas que le permite aprender de ellas y construir el sistema difuso. Estas reglas son utilizadas para obtener el grado de disparo de la regla definitiva. Una vez obtenidas la base de reglas difusas definitivas, cada una de ellas es utilizada para predecir la región de salida asociada a los datos registrados y con ello verificar su precisión. Si la suma de los errores absolutos obtenidos es positiva el peso de las reglas se incrementa. De lo contrario, si la suma de los errores absolutos obtenidos es negativa el peso de las reglas se disminuye, esto significa estar ajustando al mayor grado de exactitud al sistema de inferencia difuso.

Los métodos de defusificación de Sugeno son*: centro de área, centro de sumas y altura*. El *centro de área* (centroide o centro de gravedad) consiste en encontrar el centro del área bajo la curva generada por el proceso de agregación. Para el caso discreto, el valor de salida defusificado u^* está dado por la ecuación *3*, donde u_i es el i-ésimo punto discreto en el eje x, l es el total de valores discretos del eje x y μ_k es el valor máximo de disparo del k-ésimo conjunto de la variable de salida

$$u^* = \sum_{i=1}^{I} max_k(\mu_k(u_i))u_i \;/\; \sum_{i=1}^{I} max_k(\mu_k(u_i)) \qquad (3)$$

El Centro de Suma. Consiste en encontrar el centro del área bajo la curva generando la contribución de cada conjunto individualmente, de tal manera que el área de intersección de los conjuntos se considera más de una vez. El valor de salida defusificado u^* está dado por la ecuación *4* para el caso discreto, donde u_i es el i-ésimo punto discreto en el eje x, l es el total de valores discretos del eje x, μ_k es el valor máximo de disparo del k-ésimo conjunto y n es el total de conjuntos de la variable de salida.

$$u^* = \sum_{i=1}^{I} max_k(\mu_k(u_i))u_i \;/\; \sum_{i=1}^{I}\sum_{k=1}^{n} max_k(\mu_k(u_i)) \qquad (4)$$

Altura. Este método de defusificación consiste en tomar las alturas de los conjuntos y construir la suma ponderada con respecto a los centros de las funciones. El valor de salida defusificado u^* está dado por la ecuación *5* para el caso discreto, donde c_k es el valor de la media (centro) del k-ésimo conjunto dado sobre el eje x y μ_k es el valor máximo de disparo de ése conjunto.

$$u^* = \sum_{k=1}^{n}\mu_k \cdot c_k \;/\; \sum_{k=1}^{n}\mu_k \qquad (5)$$

En el proceso de defusificación en CARFIR estada dado el centro de área.

Esquema de Predicción en CARFIR.

Una vez que la base de reglas difusas tipo Sugeno esta disponible, tiene lugar en la predicción del comportamiento futuro del sistema bajo estudio. *CARFIR* contempla la opción de utilizar únicamente el proceso de pronóstico difuso de *FIR* que usa exclusivamente la base de regla de patrones. Esta opinión es recomendable cuando los recursos computacionales permiten conservar la base de reglas de patrones o cuando ninguno de los otros esquemas puede obtener una representación exacta del patrón de reglas. El sistema de inferencia difuso de *Sugeno* hace uso de las reglas difusas obtenidas a partir de la base de reglas patrón para realizar la predicción por medio del clásico sistema de inferencia de *Sugeno* que ha sido descrito.

Medida de Error en CARFIR.

La metodología CARFIR utiliza el error estándar (*RSM*) para conocer la precisión de las predicciones realizadas. El error *RSM*, obtiene la suma de los cuadrados de las diferencias entre los valores exactos y los valores calculados, como se muestra en la ecuación *5*, donde se denota con X_i al i-ésimo valor exacto y con C_i al i-ésimo valor calculado.

$$EC = \frac{\sum_{i=1}^{n}(X_i - C_i)^2}{2} \qquad (6)$$

[1] Se hace referencia a los antecedentes y se excluye el consecuente.

PREDICCIÓN Y MODELADO DE LA RESISTENCIA CORONARIA DEL SISTEMA NERVIOSO CENTRAL.

La investigación realizada se centra en la identificación de modelos para la predicción del controlador de la resistencia coronaria del SNC con la metodología FIR y CARFIR los resultados obtenidos por estas metodologías se comparan y por ende permitirán medir la eficiencia de CARFIR. En esta sección se desarrollan dos apartados los cuales se especifican a continuación.

A) Modelado y predicción del controlador resistencia coronaria del sistema nervioso central utilizando la metodología de Razonamiento Inductivo Difusos (FIR). El método de discretización utilizado es el Equal Frequency Partition (EFP), el número de clases para la variable de entrada y de salida es de tres.

B) Modelado y predicción del controlador resistencia coronaria del sistema nervioso central utilizando la metodología Construcción de Reglas en Razonamiento Inductivo Difuso (CARFIR). Como el número de reglas que se obtendrán es reducido, se planteo realizar la identificación de tres modelos en los cuales se varia el número de clases. 3, 5 y 9 clases respectivamente, esto es con la finalidad de ver el comportamiento del sistema con diferente cantidad de reglas (9, 25 y 81). En los dos primeros casos el método de discretización es el EFP. El tercer caso se discretiza de acuerdo a la opinión del experto.
Los resultados obtenidos en este apartado se comparan con los resultados del apartado *A,*

La variable de entrada es la presión seno carótica (CSP) y la variable de salida el controlador de la resistencia coronaria (CRC) los cuales cuentan con un total de 3640 datos, la validación del modelo se realiza con seis conjuntos de datos. La máscara candidata utilizada para generar el modelo tiene una profundidad de tres que cubre y cubre un período de tiempo de 0.48 segundos. La máscara candidata se define con el máximo de relaciones causales y temporales valores para estudiar todas las posibilidades de causalidad en la identificación del modelo cualitativo, ecuación *7*

t/x	CSP	CRC	
$t - 2\delta t$	-1	-1	
$t - \delta t$	-1	-1	*(7)*
t	-1	+1	

Para cuantificar la capacidad de predicción se utiliza el error estándar RMS, que se definió en la ecuación *6*.

Modelo y predicción con FIR del controlador resistencia coronaria

Una vez disponibles los valores de las variable de entrada presión seno carótida (CSP), la variable de salida controlador de la resistencia coronaria (CRC) y definidos los parámetros de entrada antes descritos, inicia el proceso de discretización de las variables y el proceso de fusificación. Concluido éste, el proceso de modelado cualitativo es, el encargado de identificar la máscara óptima y el conjunto de reglas patrón. La máscara subóptima utilizada para efectuar la simulación cualitativa de los seis conjuntos de datos disponibles está representada en la ecuación 8.

t/x	CSP	CRC	
$t - 2\delta t$	-1	-2	
$t - \delta t$	0	0	(8)
t	0	1	

La máscara y la base de reglas se utilizan para efectuar la simulación cualitativa, que permite la validación del modelo mediante el pronóstico de los seis conjuntos de datos de prueba.

Modelo y predicción con CARFIR del controlador resistencia coronaria.

Para realizar la identificación del modelo se conserva las máscaras candidata utilizada en la ecuación 7, la máscara subóbtima utilizada es la de la ecuación 8 el número de datos para identificar el modelo, las variables de entrada y salida, así como los conjuntos de datos de prueba son los mismos del caso anterior.

Recordemos que CARFIR compacta la base de reglas patrón de FIR en una base de reglas difusas clásicas mediante el sistema de inferencia difuso Sugeno. Una vez disponible la base de reglas patrón, es necesario crea los siguientes parámetros de entrada requeridos por el sistema de inferencia difuso Sugeno, el cual requiere un archivo que contenga la base de reglas patrón, división de cada variable, posición de las m-entras y la m-salida del sistema, posición de los datos reales, la complejidad de la máscara, la longitud de los datos y las marcas. Ya con esta información inicia el proceso de aprendizaje de Sugeno con el cual se obtienen las reglas difusas clásicas del sistema. Sugeno en un primer momento realiza la validación del modelo con los datos de entrenamiento. Y posteriormente se pueden hacer las predicciones con los datos de prueba obteniendo el error de predicción. El número de épocas con las que se entrenaron los casos desarrollados fue de 100 suficiente para lograr llegar al mínimo (estabilizar el sistema) obteniendo el error de entrenamiento.

El número de reglas patrón obtenidos por FIR en el apartado A es de 3638 y el número de reglas difusas clásicas que se obtuvieron en el apartado B son, 9, 25 y 81, para 3, 5 y 9 clases respectivamente, la reducción en las reglas es significativa lo que indudablemente genera perdida de información y por tanto la precisión en la predicción se ve afectada, de ahí que el porcentaje de error se vea reflejado en el seguimiento de las señales de salida. Los mejores resultados con CARFIR son los obtenidos con una discretización en las variables de 9 clases ya que son 81 reglas y obviamente le ayudan a seguir más el comportamiento del sistema.

Los resultados de FIR y CARFIR obtenidos en la identificación y predicción del controlador resistencia coronaria del Sistema Nervioso Central, se ilustran en la tabla 1. El primer renglón indica la metodología y la discretización de las variables. Los siguientes seis renglones son los conjuntos de prueba y el último renglón el error promedio de éstos. Las columnas contienen los errores de predicción para los casos desarrollados. La tabla 2 muestra los números de reglas utilizadas por la metodología FIR y CARFIR para realizar la predicción y el error general.

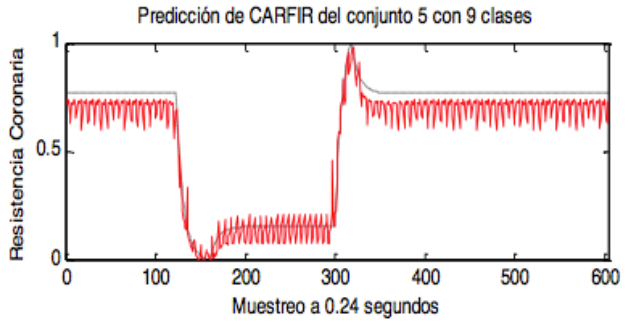
Conjunto de datos	FIR (3 3)	CARFIR (3 3)	CARFIR (5 5)	CARFIR (9 9)
1	0.4192	5.1557	3.5206	1.9851
2	0.8198	5.2374	3.5938	2.1431
3	0.8194	5.1389	3.4867	2.0801
4	0.0000	5.6728	3.9113	4.0475
5	0.3261	5.2157	3.4207	1.7641
6	0.8671	5.7980	4.1804	2.4099
Error promedio	0.5420	5.3697	3.6856	2.4050

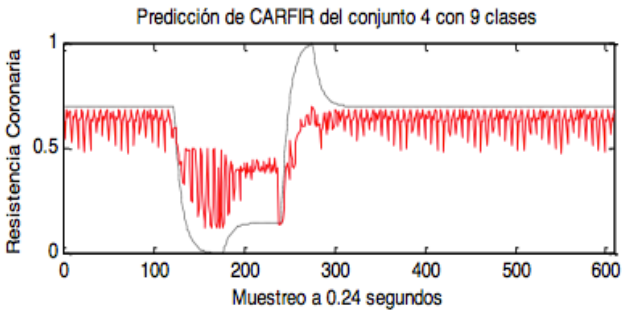
Tabla 1. Resultados de la metodología FIR y CARFIR.

Conjunto de datos	No. de reglas	Error de entrenamiento	Error promedio de prueba
FIR (3 3)	3682	---	0.5420
CARFIR (3 3)	9	3.7412	5.3697
CARFIR (5 5)	25	2.0633	3.6856
CARFIR (9 9)	81	2.2054	2.4050

Tabla 2. Resultados de FIR y CARFIR.

La figura 4 muestra las predicciones con el error más pequeño 1.7641 y con el más grande 4.0475 para el caso con 9 clases.





IV ANALISIS DE RESULTADOS

La metodología FIR mediante el procedimiento de modelado cualitativo, obtiene la base de reglas patrón cuya cantidad esta dada por la cantidad de datos que intervienen en el sistema, como se puede apreciar el número de datos utilizados para identificar el modelo de la resistencia coronaria del sistema nervioso central es de 3640 que se traducen en 3638 reglas patrón. CARFIR recibe como entrada este número de reglas obteniendo 9, 25 y 81 reglas difusas clásicas, con las cuales realiza el pronóstico y como lo muestran los resultados el error resulta ser más grande que el obtenido por FIR ya que CARFIR al generalizar pierde información, no obstante la señal es seguida con cierta precisión.

V CONLUSIONES Y TRABAJO FUTURO

La idea original de la metodología CARFIR resulta interesante, al permitir trabajar con un sistema de reglas difusas clásicas, las cuales son el producto de la integración de las reglas patrón que se obtienen con FIR y que permite obtener ventajas de ambas aproximaciones. La metodología FIR es una poderosa herramienta para identificar y predecir sistemas. Sin embargo, tiene una importante restricción cuando se trabaja con sistemas complejos que requieren de una gran cantidad de datos y variables para ser representados, pues la base de reglas patrón resulta extremadamente grande, por lo que el coste computacional asociado a la predicción se incrementa. CARFIR puede llegar a ser una herramienta igual o más poderosa que FIR, que se encuentra en la etapa inicial de su desarrollo, pues es la primera vez que se prueba con sistemas complejos (sistema nervioso central) y los resultados obtenidos son prometedores ya que con un número tan reducido de reglas permite identificar y seguir la señal del sistema, aunque no con la precisión deseada. Un aspecto interesante es la importancia que CARFIR da a los conjuntos de datos más densos.

Por otro lado, un aspecto importante que se detectó es que el coste computacional de CARFIR en el proceso de aprendizaje e identificación de las reglas difusas es elevado, punto que hay que tratar. Sin embargo, esta metodología abre un nuevo camino para tratar con el sistema de contaminación medioambiental.

Para que CARFIR logre la robustez necesaria para abordar el problema de los sistemas de contaminación medioambiental es necesario llevar a cabo la depuración del código, para minimizar el coste computación en la identificación de las reglas difusas. Así mismo, se debe crear un sistema mixto capaz de realizar predicciones con un porcentaje de reglas patrón (las que conlleven mayor incertidumbre) y las reglas difusas, esto permitirá incrementar la precisión en la predicción del sistema. Un tercer trabajo futuro es el estudio de la relevancia causal entre las variables, de tal manera que permita simular el comportamiento del sistema. Finalmente será interesante no perder de vista el método de discretización.

AGRADECIMIENTOS

Los autores agradecen el apoyo de las siguientes instituciones para la realización de este trabajo de investigación a: La Secretaría de Investigación y Posgrado del IPN, La Secretaría Académica del IPN, La Comisión de Fomento a las Actividades Académicas del IPN (COFAA).

Artículo derivado del proyecto de investigación titulado "Desarrollo de nuevas técnicas informáticas, para la creación de modelos para identificar sistemas complejos" Clave: 20040871.

REFERENCIAS

[1] Cellier F.E., A. Nebot, F. Mugica and A. de Albornoz, Combined qualitatitive/quantitative simulation models of continuous-time processes using FIR tecniques. International Journal of General Systems 24 (1-2). Pp. 95-116. 1996.

[2] Gómez P., A Nebot, F. Mugica, and F. Wotawa, Fuzzy Inductive Reasoning for the Prediction of Maximum Ozone Concentration. In Proceedings ESS'01: European Simulation Symposium, page 8pp., Marseille, France, 18-20 October 2001.

[3] Gómez & Vázquez 2007 "Modelado y predicción de la concentración de ozono con la Metodología de Razonamiento Inductivo Difuso

[4] Gómez & Vázquez 2007 "Modelado y predicción de la concentración de ozono con la Metodología de Razonamiento Inductivo Difuso", XX Congreso Nacional y VI Congreso Internacional de Informática y Computación de la ANIEI e incluidas en el libro electrónico del evento "Avances en Tecnologías de la Información" CNCIIC 2007.

[5] [Gómez & Vázquez 2010] "Metodología para la construcción autmática de reglas en razonamiento inductivo difuso (CARFIR)", XXIII Congreso Nacional y IX Congreso Internacional de Informática y Computación ANIEI 2010".

[6] Klir G., Architecture of Systems Problem Solving, Plenum Press, New York, 1985.

[7] Nebot A., F.E. Cellier and M. Vallverdú, Mixed quantitative/qualitative modeling and simulation of the cardiovascular system, Computer Methods and Programs in Biomedicine 55, pp. 127-155, 1998.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 4, Volumen 3, Año 3. Julio 2011
Artículos con arbitraje

Guías útiles para la construcción de Objetos de Aprendizaje para dispositivos Móviles (AOM)

Aldo Ramírez Arellano, José Antonio Rodríguez Mancera, Elizabeth Acosta Gonzaga
Instituto Politécnico Nacional (IPN)
Ciudad de México, México
aramirezar@ipn.mx, jrodriguezm0909@ipn.mx, eacostag@ipn.mx

***Resumen*— En este trabajo introducimos la relación entre los Objetos de Aprendizaje (OA) y el aspecto instruccional mediante la intención de aprendizaje. Basados en este concepto, ejemplificamos como la misma entidad digital puede convertirse en diferentes OA de acuerdo a la definición de la intención de aprendizaje. Definimos las características de los Objetos de Aprendizaje para dispositivos Móviles (OAM) que son el marco de una serie de guías basadas en diversos estándares. Estas guías tiene la intención de garantizar que el OAM sea reusable, interoperable, modular, portable, accesible, adaptable entre otras y con ello crear nuevas oportunidades para el aprendizaje móvil. Como resultado desarrollamos un agente de software denominado VOAM capaz de desplegar los OAM diseñados atendiendo las guías propuestas.**

Keywords-component; m -learning, aprendizaje, móviles

I. INTRODUCCION

La revolución tecnológica está cambiando nuestras vidas, actualmente podemos participar en conversaciones prácticamente desde cualquier lugar con la infraestructura tecnológica que lo hace posible. Los estudiantes están dejando a un lado los medios como libretas y lápiz y están sustituyéndolos por herramientas como computadoras portátiles, teléfonos móviles etc. Además las bibliotecas digitales y multimedios educativos han tomado una relevancia importante en los últimos tiempos como repositorios de conocimiento. Los medios digitales tienen visibles ventajas con respecto a los métodos tradicionales y por supuesto también inconvenientes.

En la actualidad el aprendizaje a través de dispositivos móviles, conocido como m-learning, es un tema de importancia en la investigación, porque le confiere al estudiante independencia del lugar y del horario, esto se apega al paradigma de aprendizaje "anytime and anywhere" [17] [3]. El número de personas que utilizan dispositivos como notebooks, PDA y teléfonos móviles se incrementa día a día. Por lo que la oportunidad que representa el uso de estos adelantos tecnológicos en el área educativa es invaluable [1] [4] [5] [19].

Los avances tecnológicos como el incremento en el ancho de banda, mayor espacio de almacenamiento, incremento del poder de cómputo, el uso de multimedia, entre otros, dificultan la distribución y visualización de los materiales y contenidos educativos ya que estas capacidades no son homogéneas en los dispositivos móviles.

Los materiales y contenidos educativos diseñados para computadoras personales y portátiles, encapsulados como objetos de aprendizaje (OA), no pueden ser fácilmente desplegados en dispositivos móviles por lo que es necesario el establecimiento de guías para su diseño. Estas guías deben tomar en cuenta las tecnologías más recientes y ser independientes de la teoría instruccional y pedagógica utilizada para la concepción y diseño de los Objetos de Aprendizaje para Móviles (OAM).

En particular hay tres aspectos importantes en los cuales la investigación en esta área está centrada y son [2]:

1. El desarrollo de modelos pedagógicos apropiados para el aprendizaje en móviles y las restricciones que este ambiente impone.
2. Usar la experiencia ganada en el aprendizaje basado en computadoras personales y adaptarlo a ambientes móviles.
3. Diseñar, desarrollar e implementar los ingredientes técnicos necesarios para apoyar el aprendizaje en dispositivos móviles.

En nuestro trabajo nos centramos en las dos últimas áreas mencionadas anteriormente. En la primera definimos las características de los OAM, buscamos adaptar los estándar IMS [7] y SCORM [18], usados ampliamente con OA, haciéndolos más apropiados para entornos móviles considerando las restricciones de seguridad, memoria, poder de cómputo y espacio de almacenamiento, además proponemos una serie de guías que ayudan al diseño y la construcción de OAM. En la segunda área, desarrollamos el software que permite visualizar los OAM y que es altamente portable.

II. DEFINICIONES

La definición de las características de un OA varía de acuerdo al punto de vista del autor, consideramos que debe ser diseñado pensando en cinco aspectos: reusable, portable, interoperable, modular y accesible [13] [15] [16] [19] [20]. Estas características obligan el establecimiento y uso de estándares para su encapsulamiento, distribución, despliegue y navegación de forma local mediante un visualizador o a través

de Internet con un sistema de administración del aprendizaje (LMS por sus siglas en inglés).

Definición 1 Objeto de Aprendizaje (OA). Un objeto de aprendizaje es una entidad digital que tiene una intención de aprendizaje y que además cumple con las siguientes características.

- ***Reusable:*** *El LMS es el encargado de entregar el contenido educativo en forma de un OA, este debe de tener una granularidad adecuada para que pueda ser usado en un contexto educativo diferente para el cual fue diseñado.*
- **Interoperable:** *Esto significa que el OA debe tener comunicación con el LMS para compartir información acerca de la interacción del estudiante con el OA. Esta comunicación se lleva a cabo mediante la API ECMAScript de la IEEE [6].*
- **Modular:** *El OA debe ser lo suficientemente coherente y visto como una unidad indivisible, pero también lo suficientemente pequeño para cumplir con la característica de reusabilidad. Aunque el OA es empaquetado usando IMS, este estándar no restringe la granularidad del objeto, esto permite crear objetos tan extensos o tan pequeños como sean necesarios.*
- **Accesible:** *Esto significa que el OA debe de tener una descripción pública de la intención de aprendizaje y del contenido educativo, con lo cual pueda ser descubierto, localizado y reutilizado. Esto es descrito mediante los metadatos que siguen el estándar LOM [10].*
- ***Portable:*** *Este concepto significa que el OA pueda ser visualizado y consultado a pesar de los cambios tecnológicos y del dispositivo usado.*

En esta definición podemos ver que la intención de aprendizaje juega un rol importante en el OA. Una entidad digital, por ejemplo una imagen de una célula vegetal, no puede ser considerada un OA si no tiene una intención de aprendizaje, para nuestro ejemplo la imagen permite al estudiante conocer su estructura que posteriormente tendrá que identificar en un microscopio. Inclusive esta entidad digital podría convertirse en un OA totalmente diferente si el objetivo fuese resaltar las diferencias con una célula animal. En nuestra definición de OA establecemos la conexión entre lo tecnológico y lo pedagógico, refiriéndonos e éste último como intención de aprendizaje en un sentido muy general que tomará particularidades de acuerdo al diseño instruccional.

Definición 2 Objeto de Aprendizaje para dispositivos Móviles (OAM). Un objeto de aprendizaje para dispositivos móviles reúne las características de un OA y debido a la naturaleza móvil en términos de espacio y tiempo también debe cumplir lo siguiente:

- ***Individual****: En el sentido de que pueda adaptarse al estilo de aprendizaje del estudiante.*
- ***Disponible****: El OAM debe de estar disponible en cualquier lugar sin importar el medio o la forma de comunicación con el LMS.*
- ***Adaptable:*** *Esto significa que el OAM debe adaptarse al contexto del aprendizaje y a las habilidades y conocimientos del estudiante.*
- ***Sencillo de usar:*** *En cuanto a la navegación a través del material y la interacción con los usuarios.*

El principal obstáculo para cumplir con lo anterior está relacionado de manera directa con la falta de estándares para los OAM. En la siguiente sección proponemos un par de modificaciones al estándar IMS y SCORM ampliamente usados para la construcción OA, de forma que sean más apropiados para el m-learning. Estas modificaciones permiten utilizarlos en la construcción de OAM en conjunto con las guías propuestas.

III. ADAPTACIÓN DE LOS ESTANDARES PARA LOS OAM

La principal dificultad que se enfrenta los diseñadores de OAM, es la heterogeneidad entre los dispositivos móviles, aunado a que los estándares existentes no consideran esta diversidad ni sus limitaciones.

A continuación mencionamos algunas guías y las adaptaciones al estándar IMS y SCORM necesarias para el diseño e implementación de los OAM. Consideramos dos escenarios generales, el primero de ellos cuando el agente de software tiene acceso al OAM de forma local y el segundo cuando el acceso es remoto a través de un LMS.

A. Reusable

Como lo hemos expuesto la reusabilidad de un OAM depende del grado de granularidad y de la modularidad que posea. Los estándares IMS y SCORM no imponen límites al tamaño de los objetos por lo que pueden usarse para OAM con diferentes granularidades. Por otro lado para que sea reusable es necesario conocer la intención de aprendizaje por lo que recomendamos.

G1. Definir la intención de aprendizaje haciendo uso de los metadatos y el LOM [10].

B. Interoperable

El estándar SCORM define dos tipos de de recursos de aprendizaje, denominados "Asset" y "SCO" (Sharable Content Objects). Los Asset son los bloques básicos de construcción que permiten crear otros Asset o SCO. Los SCO a diferencia de los Asset permiten una comunicación con el LMS. La interrogante que surge es ¿Cómo podemos logar la comunicación entre el SCO y el LMS?

G2. El SCO debe comunicarse con el LMS a través del ECMAScript Mobile Profile haciendo uso del Script definido en XHTML Mobile Profile [23].

Aunque la implementación del ECMAScript no está definida, será favorecida si se usa un lenguaje portable como Java atendiendo las limitantes de la JME.

C. *Modular*

Cada OAM es modular a través del paquete IMS, que contiene el archivo imsmanifest que describe al OAM y además en el paquete se encuentran todos los recursos necesarios para desplegarlo. Cada paquete debe de ser autocontenido y garantizar que el agente tenga acceso a todos los recursos en la localización que dicta el imsmanifest.

Para los OAM el empaquetado debe atender las siguientes recomendaciones:

G3. Si el acceso al OAM es de forma local, este debe estar contenido en una carpeta sin subniveles y sin compactar que contendrá el archivo imsmanifest y todos los recursos multimedia necesarios para construir el OAM.

G4. Si el acceso al OAM es remoto a través de un LMS, el OAM puede estar contenido en un "Package Interchange File" (PIF) que este compactado, que cumpla con el estándar RFC 1951 y tenga extensión .zip. Además deberá contener todos los recursos multimedia necesarios para construir el OAM.

Las dos recomendaciones obedecen a las restricciones de acceso al sistema de almacenamiento que algunos dispositivos imponen, y a la cantidad limitada de memoria y poder de cómputo.

Para el escenario local, no existe garantía que se tenga accesos a todos los recursos, sí un Asset apunta a un archivo remoto mediante una URL. Al incluir todos los archivos en el PIF sorteamos este problema.

Por otro lado, evitar compactar el PIF ahorra memoria y tiempo de cómputo. Restringir la creación de subdirectorios evita que la URL´s apunten a recursos almacenados en subcarpetas, de lo contrario la creación de subdirectorios es necesaria, tal operación no está garantizada en todos los dispositivos.

Estas dos recomendaciones no afectan al OAM remoto, por el contrario la modularidad del OAM quedará bien limitada a los recursos almacenados en el paquete y no ha recursos ubicados en sitios remotos.

Tampoco afecta a la reusabilidad de los OAM, en este sentido recomendamos que:

G5. Los recursos remotos a los que apuntan los Asset deben almacenarse en el mismo paquete que los locales.

Derivado de esta recomendación proponemos las siguientes modificaciones a SCORM, útiles para dispositivos móviles.

M1. Los Asset y SCO solo podrán hacer referencia a recursos contenidos en el PIF mediante una URL relativa que apunte a los recursos situados en la carpeta raíz del PIF.

M2. Los nombres de los archivos de los recursos deben ser únicos en el ámbito del PIF.

D. *Accesible*

En general los OAM deberán tener una descripción haciendo uso de los metadatos. Esta descripción es útil para la búsqueda localización y reutilización, por lo que en el escenario local OAM podrá prescindir de ella. Esto origina lo siguiente:

G6. Un OAM debe poseer una descripción usando metadatos cuando este alojado en un repositorio de objetos de aprendizaje (ROA) o en un LMS, de lo contrario los metadatos podrán omitirse.

Esta guía permitirá reducir el tamaño de un OAM y por lo tanto el ancho de banda para su transmisión. El LMS tendrá que ocuparse de eliminar los metadatos cuando el OAM sea entregado a un agente de software para su visualización local.

E. *Portable*

Los recursos Asset o SCO, pueden contener cualquier tipo de archivo lo que dificulta la portabilidad. Ambos hacen referencia a un recurso conocido como punto de lanzamiento y que generalmente es una página web.

Esto plantea dos preguntas: ¿Qué tipo archivos deben de incluirse en los Asset y SCO para garantizar su portabilidad?, ¿Cómo podemos garantizar que se muestren al usuario correctamente?

Para esto, proponemos lo siguiente:

G7. Utilizar archivos de audio de formato wav, arm y mid como recursos.

G8. Utilizar archivos de video en formato mpg como recursos.

G9. Utilizar archivos de imagen en formato png, jpg o gif como recursos.

G10. Utilizar como recursos páginas web que cumplan con el estándar XHTML Mobile Profile al menos en la conformación del documento y en el uso de estilos.

G11. Los puntos de lanzamiento para los SCO deberán ser páginas web que cumpla completamente con el estándar XHTML Mobile Profile.

G12. Los puntos de lanzamiento para los Asset deberán ser páginas web que cumpla con el estándar XHTML Mobile Profile al menos en la conformación del documento y en el uso de estilos.

F. *Individual*

El OAM puede adaptarse al estilo de aprendizaje con ayuda del LMS, el cual realizará las transformaciones a los recursos basadas en el perfil del estudiante.

G13. Ofrecer el mismo recurso educativo usando diferentes estrategias y multimedios como imágenes, audio y video.

G. *Disponible*

El escenario remoto requiere que el dispositivo móvil tenga acceso al LMS que se encarga de servir el OAM considerando las guías de la G6 a la G12. La otra posibilidad es:

G14. Si el dispositivo no cuenta con acceso remoto al LMS, el OAM debe ser almacenado de forma local siguiendo las recomendaciones G3 y G5.

H. *Adaptable*

Como lo hemos dicho, el LMS deberá tener conocimiento del perfil del estudiante para adaptar el OAM de acuerdo a los conocimientos previos y habilidades. Esta tarea demanda poder de cómputo como se observa en [2], por lo que difícilmente podrá llevarla a cabo un dispositivo móvil.

G15. El LMS debe adaptar el OAM móvil de acuerdo al perfil del estudiante y al contexto de aprendizaje, mediante los elementos de organización y secuencia definidos en SCORM.

Esto garantiza que la taxonomía del OAM permanezca intacta y el LMS determine la secuencia de consulta ocultando o condicionando la visualización de elementos del OAM.

Por ejemplo en un curso de fotografía, constituido de una parte teórica y una práctica, donde es necesario que el estudiante haya cumplido satisfactoriamente con los créditos teóricos para permitirle continuar con la práctica. Posiblemente el estudiante haya cursado ya el bloque teórico o tomado algún curso equivalente, lo que lo exime de cumplir con los créditos teóricos. El LMS deberá conocer esta situación y adaptar el OAM.

I. *Sencillo de usar*

Los dispositivos móviles poseen interfaces limitadas en comparación con las computadoras personales. Por esta razón es importante considerar la navegación del contenido educativo en el OAM, el acceso y su comportamiento. Lo que da origen a la siguiente recomendación.

G16. Para el diseño del contenidos educativo de un OAM debe tomarse en cuenta las recomendaciones del Mobile Best Practices [12].

IV. CASO DE ESTUDIO

El Instituto Politécnico Nacional [8], es una de las instituciones de educación pública en México con presencia en gran parte de su territorio, ha adoptado la educación a distancia bajo su modelo educativo y actualmente ofrece programas de posgrado, licenciatura y bachillerato, donde participan 1398 estudiantes. A sí mismo ofrece cursos de formación y actualización con una matrícula de aproximadamente 20,000 participantes. Por estas razones es prioritario explorar las oportunidades del aprendizaje en dispositivos móviles.

Como parte de esta investigación encuestamos a un grupo de 100 estudiantes del nivel licenciatura, los resultados son los siguientes:

a) El 92% de los estudiantes cuentan con teléfono móvil.

b) El 94% de los dispositivos cuenta con pantalla a color, el 27% cuenta con servicio de Internet y el 85.7% de los teléfonos soportan la tecnología Java.

c) Los principales usos que le dan al teléfono celular en orden de importancia son:

1. Hacer llamadas
2. Mandar mensajes de texto y multimedia
3. Visualizar documentos
4. Tomar fotos y videos
5. Navegar en Internet
6. Escuchar música
7. Ejecutar aplicaciones

La visualización de documentos y la navegación en Internet se encuentran entre los primeros lugares de los usos del teléfono móvil, así que los estudiantes poseen las habilidades necesarias para llevar a cabo estas tareas. Por otro lado, el acceso a los OAM vía Internet pude ser problemático ya que solo el 27% de los estudiantes encuestados cuentan con este servicio. Considerando lo anterior, diseñamos el Visualizador de Objetos de Aprendizaje para dispositivos Móviles (VOAM) que permite el acceso local al OAM o el acceso a través de Internet mediante un LMS.

A. *Arquitectura y diseño*

La arquitectura de la aplicación se muestra en la figura 1, consta de un LMS alojado en un servidor donde el OAM es depositado por el profesor. El VOAM reside en el dispositivo móvil y podrá tener acceso al OAM de dos formas como se describe a continuación. El OAM puede ser enviado como un paquete PIF que deberá descompactarse y ser transferido al dispositivo móvil para su almacenamiento con ayuda de una computadora personal o a través de Internet. El LMS también puede servir el OAM como una página web, por lo que podrá estar disponible si el dispositivo cuenta con este servicio. Almacenar el OAM en el dispositivo permite revisarlo el número de veces que el estudiante considere necesario sin que ello genere un costo por el uso del servicio de Internet e inclusive cuando no esté disponible.

El VOAM tiene una interfaz amigable, conformada por una barra de navegación similar a un navegador web y varias opciones contenidas en un menú, con el cual los usuarios pueden realizar las tareas de navegar por el contenido, ocultar la barra de navegación, consultar la ayuda, entre otras.

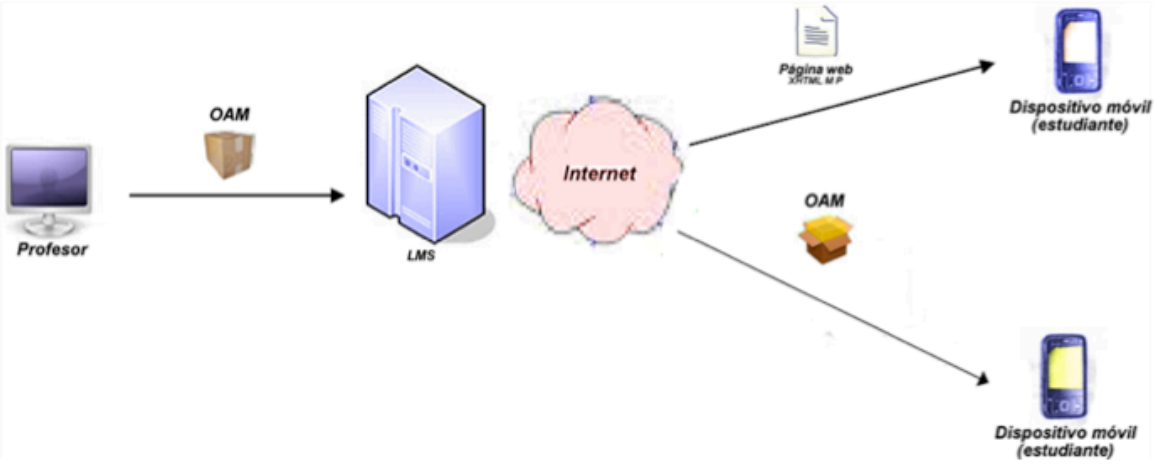


Figura 1. Arquitectura de la aplicación VOAM

Además identifica las ligas visitadas, permite reproducir clips de audio y video sin la necesidad de una aplicación adicional como se observa en la figura 2. A través del VOAM el usuario puede consultar el OAM almacenado en el dispositivo móvil o a través de un LMS, haciendo casi imperceptible la diferencia. Desarrollamos el VOAM utilizando la tecnología Java, ya que cada vez más teléfonos y dispositivos móviles la incluyen. Por otro lado también nos dimos a la tarea de construir el Ambiente Cooperativo de Apoyo al Aprendizaje para Funciones Tutoriales (ACAAFT) que permite a los profesores diseñar OAM y contar con un repositorio de recursos digitales.

Figura 2. Contenido educativo del OAM que pertenece al curso Computación Aplicada.

B. Resultados

Construimos varios OAM siguiendo las guías propuestas y los estándares señalados. Estos OAM contienen recursos como páginas web, imágenes, clips de audio y video. Publicamos estos recursos para que estuvieran disponibles para los alumnos del curso Computación Aplicada del nivel licenciatura, impartido en modalidad semi-presencial.

Para evaluar la efectividad del aprendizaje formamos dos grupos, el primero llamado M y el segundo S cada uno con 18 alumnos. El grupo M revisó la unidad de aprendizaje "Aplicación de fórmulas y funciones a la bioestadística" mediante los OAM, mientras que el grupo S consultó los contenidos de la misma unidad haciendo uso de los OA que se han utilizado a lo largo de varios ciclos escolares en el curso semi-presencial. Los OAM y OA incluyen dos evidencias de aprendizaje tituladas "Operadores" e "Introducción de fórmulas".

Los resultados de la evaluación de estas evidencias fueron analizados usando una prueba estadística t con un intervalo de confianza de 95%, este análisis nos permite concluir que no existe diferencia entre los resultados obtenidos por el grupo S y M en la actividad "Operadores" ni tampoco en la actividad "Introducción de fórmulas", aunque en esta última la diferencia es más acentuada como se observa en la figura 3.

Los alumnos que consultaron los OAM opinaron que los materiales están más sintetizados comparados con los del curso semi-presencial, gracias a que incluyen más videos y clips de audio. Otros opinaron que la navegación es sencilla, similar a una página web. La mayoría considera que los OAM son útiles ya que pueden consultarlos en el trayecto a casa o en cualquier sitio.

En resumen, el uso del IMS y SCORM para empaquetar y distribuir los OAM diseñados les confiere la modularidad. La inclusión de los metadatos siguiendo el LOM habilita al LMS para eliminarlos cuando el OAM es entregado a un dispositivo móvil, con el fin de reducir su tamaño. El uso de los estándares XHTML Mobile Profile y la inclusión de recursos multimedia en los formatos sugeridos garantizan la portabilidad. La especificación de la taxonomía del OAM y la secuencia de navegación como lo dice el SCORM, abre la posibilidad de que el LMS adapte el contenido y su secuencia, de acuerdo a las necesidades y estilo de aprendizaje del estudiante cumpliendo con la adaptabilidad e individualidad.

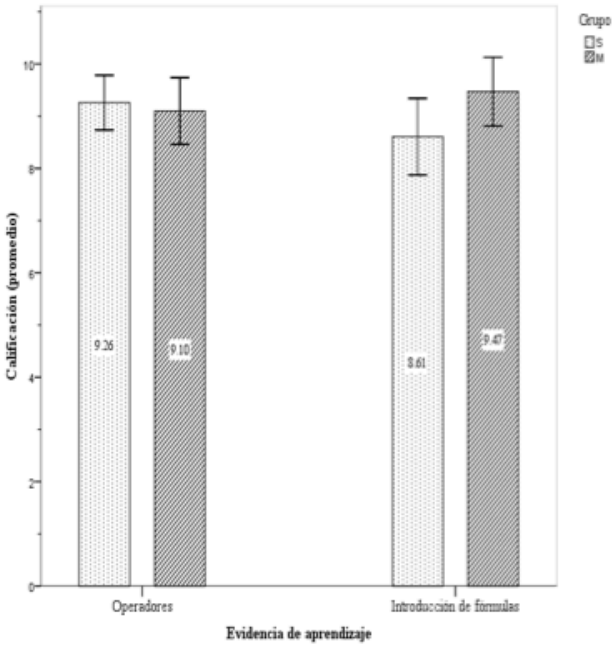


Figura 3. Calificaciones promedio obtenidas por el grupo S y M en las evidencias de aprendizaje "Operadores" e "Introducción de fórmulas".

La consideración del Mobile Best Practices en el diseño de los contendidos educativos permitió que la interacción y la navegación con el OAM fueran sencillas. Por último la arquitectura permite consultar el OAM a través de Internet o ser almacenado en el dispositivo móvil.

V. Trabajos Relacionados

El desarrollo de aplicaciones para consultar material educativo en dispositivos móviles ha recibido bastante atención en los últimos años. Seong [17] propone varias guías que contemplan las habilidades y estilos de aprendizaje, la interacción con el dispositivo móvil y el diseño de la interfaz. Estas guías se enfocan en el desarrollo de portales educativos y no en objetos de aprendizaje, dejando de lado la individualidad, la adaptabilidad y la disponibilidad, características de los OAM que proponemos en este trabajo.

El problema de la portabilidad ha recibido diferentes enfoques, en [11] [14] los contenidos están limitados a foros y noticias en línea mientras que en [3] [9] [21] [22] los autores utilizan varios agentes inteligentes para determinar el formato del contenido de acuerdo al dispositivo, esto significa que el proceso de adaptación se lleva a cabo por el LMS. Bajo esta propuesta, para transformar los contenidos exitosamente es necesario conocer por anticipado el tamaño de pantalla y los formatos de audio y video admitidos por la gran variedad de dispositivos móviles que existen hoy en día. La utilización de recursos multimedia en los formatos que sugerimos permite que el VOAM los adapte en el momento en el que son consultados, lo que elimina la necesidad de conocer las características a priori. Por otra parte el VOAM es capaz de detectar la interfaz del dispositivo móvil, por ejemplo si se trata de una pantalla táctil, permitiendo al alumno consultar los contenidos con mayor facilidad.

En [2] se usa una ontología descrita en XML para representar los conceptos y las asociaciones que existen entre ellos, lo que facilita la adaptación de los contenidos según el usuario que los consulta. Este sistema comparado con el VOAM, es poco portable ya que solo funciona en un conjunto limitado de PDA.

VI. Conclusiones y Trabajo Futuro

En este trabajo establecemos la relación entre los OA y el aspecto instruccional mediante la intención de aprendizaje, además definimos las características de los OAM, basados en ellas proponemos varias guías útiles para su diseño e implementación. Estas guías incluyen el uso de estándares que facilitan el desarrollo de los OAM. Considerando estas guías desarrollamos un software portable llamado VOAM con el cual los estudiantes pueden navegar a través de los contenidos educativos del OAM.

Construimos varios OAM apegándonos a estas guías, posteriormente los publicamos en un LMS donde fueron consultados por alumnos mediante una variedad de dispositivos móviles. El estudio comparativo realizado nos permite concluir que no existe diferencia significativa en el aprovechamiento de los alumnos que consultaron los OAM y los que hicieron lo propio con los OA.

El uso de estándares le permite al alumno que cuenta con un browser y acceso a Internet consultar el OAM sin la necesidad del VOAM, en esta situación el LMS tiene la responsabilidad de guiar la navegación. Las guías propuestas garantizan la portabilidad del OAM y su visualización sin contar con una conexión a Internet.

Existen diversas direcciones que deseamos explorar para los trabajos futuros. Planeamos investigar la posibilidad de adaptar los OAM y OA a las habilidades, estilos de aprendizaje y conocimientos de los estudiantes extendiendo las capacidades del LMS para convertirlo en un LMS inteligente. Otro aspecto de interés es averiguar la forma de transformar OA en OAM y viceversa, teniendo en mente que los objetos OAM están sujetos a varias restricciones.

Por otro lado estamos interesados en evaluar las estrategias de aprendizaje más apropiadas para los OAM, ceñidas por los recursos multimedia disponibles, la capacidad de cómputo y las interfaces de los dispositivos móviles. Otros trabajos incluyen la representación de la intención de aprendizaje de tal forma que permita construir OAM y OA de forma automática o inclusive cursos completos, seleccionando los contenidos educativos de un repositorio con la premisa de cumplir con la intención de aprendizaje.

Referencias

[1] Alexander, B. Going Nomadic: Mobile Learning in Higher Education. *EDUCAUSE Review*, Vol. 39, No. 5, 2004, 28–35.<http://www.educause.edu/pub/er/erm04/erm0451.asp>.

[2] Berri, J., Benlamri, R., and Atif, Y. 2006. Ontology-based framework for context-aware mobile learning. In *Proceedings of the 2006 international Conference on Wireless Communications and Mobile Computing* (Vancouver, British Columbia, Canada, July 03 - 06, 2006). IWCMC '06. ACM, New York, NY, 1307-1310.

[3] Cao, Y., Tin, T., McGreal, R., Ally, M., and Coffey, S. 2006. The Athabasca University mobile library project: increasing the boundaries of anytime and anywhere learning for students. In *Proceedings of the 2006 international Conference on Wireless Communications and Mobile Computing* (Vancouver, British Columbia, Canada, July 03 - 06, 2006). IWCMC '06. ACM, New York, NY, 1289-1294.

[4] Chan, T., et al. Educational Metadata for Mobile Learning, In *Procedings 2nd IEEE Int. Workshop on Wireless and Mobile Technologies in Education*, 2004.

[5] Chittaro, L. Visualizing Information on Mobile Devices. *IEEE Computer*, March 2006, 40-45.

[6] IEEE 1484.11.2 Standard for Learning Technology – ECMAScript Application Programming Interface for Content to Runtime Services Communication (2003). http://www.ieee.org/

[7] IMS Content Packaging specification (2003). http://www.imsglobal.org/learningdesign/index.html.

[8] Instituto Politécnico Nacional http://www.ipn.mx.

[9] Kukka, H. and Ojala, T. 2006. mobileDOK: culture in your pocket. In *Proceedings of the 3rd international Conference on Mobile Technology, Applications &Amp; Systems* (Bangkok, Thailand, October 25 - 27, 2006). Mobility '06, vol. 270. ACM, New York, NY, 42.

[10] Learning Object Metadata. (LOM) (2002). http://ltsc.ieee.org/wg12/20020612-Final-LOM-Draft.html

[11] Lee, W. and Lu, C. 2003. Customising WAP-based information services on mobile networks. *Personal Ubiquitous Comput.* 7, 6 (Dec. 2003), 321-330.

[12] Mobile Best Practices 1.0. http://www.w3.org/TR/mobile-bp/

[13] Mostefaoui, S. K., Maamar, Z., and Giaglis, G. M. 2008 *Advances in Ubiquitous Computing: Future Paradigms and Directions*. IGI Publishing.

[14] Nakahara, J., Hisamatsu, S., Yaegashi, K., and Yamauchi, Y. 2005. iTree: does the mobile phone encourage learners to be more involved in collaborative learning?. In *Proceedings of Th 2005 Conference on Computer Support For Collaborative Learning: Learning 2005: the Next 10 Years!* (Taipei, Taiwan, May 30 - June 04, 2005). Computer Support for Collaborative Learning. International Society of the Learning Sciences, 470-478.

[15] Polsani, P. R. Use and Abuse of Reusable Learning Objects Journal of Digital Information, Volume 3 Issue 4, Article No. 164, 2003 -Martinez, M. *Designing learning objects to mass customize and personalize learning*. In D. A. Willey (Ed) (2000).

[16] Ryu, H. and Parsons, D. 2008 *Innovative Mobile Learning: Techniques and Technologies*. Information Science Reference - Imprint of: IGI Publishing.

[17] Seong, D. S. 2006. Usability guidelines for designing mobile learning portals. In *Proceedings of the 3rd international Conference on Mobile Technology, Applications &Amp; Systems* (Bangkok, Thailand, October 25 - 27, 2006). Mobility '06, vol. 270. ACM, New York, NY, 25.

[18] The Sharable Content Object Reference Model. (SCORM) (2004) http://www.adlnet.gov/Technologies/scorm/default.aspx.

[19] Vavoula, G. N. and Sharples, M. 2002. KLeOS: A Personal, Mobile, Knowledge and Learning Organisation System. In *Proceedings IEEE international Workshop on Wireless and Mobile Technologies in Education* (August 29 - 30, 2002). M. Milrad, H. U. Hoppe, and Kinshuk, Eds. WMTE. IEEE Computer Society, Washington, DC, 152.

[20] Vinha, A. 2005. Reusable learning objects: theory to practice. *SIGCSE Bull.* 37, 3 (Sep. 2005), 413-413.

[21] Wains, S. I. and Mahmood, W. 2008. Integrating m-learning with e-learning. In *Proceedings of the 9th ACM SIGITE Conference on information Technology Education* (Cincinnati, OH, USA, October 16 - 18, 2008). SIGITE '08. ACM, New York, NY, 31-38.

[22] Wang, S., Chen, Q., and Behrmann, M. 2008. Agent-based ubiquitous m-learning portal for K-12 teachers. In *Proceedings of the 5th international Conference on Soft Computing As Transdisciplinary Science and Technology* (Cergy-Pontoise, France, October 28 - 31, 2008). CSTST '08. ACM, New York, NY, 525-529.

[23] XHTML Mobile Profile. (2004). http://www.openmobilealliance.org/.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos
Número 4, Volumen 3, Año 3. Julio 2011
Artículos con arbitraje

Application of educational Websites in higher education

Alejandro Larrauri Sánchez
School of Engineering E.S.I.M.E. Campus. Culhuacán
I.P.N.
México, D.F.
alarrauri@ipn.mx

***Abstract*— This paper describes the training given in 2009, to a group of professors of the Instituto Politécnico Nacional in Mexico City, at the school of Engineering (E.S.I.M.E campus Culhuacán), for creating their own educational website, the application of this website in their classes during one semester, and the evaluation of the students' academic improvement.**

Keywords-training; educational website; academic improvement; HTML commands

I. INTRODUCTION

There is a strong necessity to improve the process of teaching-learning of the subject matters pertaining to Engineering, and to make the most of the new telecommunication technologies in the educational area. This paper describes the training of a group of teachers of higher education for the development of their own websites and the use of these websites in their classes during one semester. It also describes how to determine the effect of this kind of teaching on the students' academic improvement. The work deals with technologies now at our disposal, such as Internet and webpages; it describes the various facets involved in the making of didactic material for its publication in the World Wide Web, the development of a web site, its application with the students and the evaluation of its effect on the academic improvement of the students.

.

II. TRAINING OF THE TEACHERS

A. Selecting the teachers

There was no special consideration of the qualifications of the teacher to take the training course, the main requisite was that they were given some subject matter in an engineering school and that they knew the basics of word processors and the Internet. The final sample size was of 60 teachers of different backgrounds: mathematics, physics, electronics, humanities.

B. Particularities of the course

The course was of 2 weeks duration, 3 hours a day working in the laboratory. The participants learned the main HTML commands and its application in a HTML document. Depending on the participant's skill, the different webpage editors were studied for the making of a HTML document. Each participant created a website with a free webhosting service, having as a result of the training course that 90% of the original participants created their own website.

The results of the training course were obtained from the websites created by the participants. A sample of these websites (still effective in December 16th-2010), is given:

http://www.serhumano.mex.tl
http://www.soni.mex.tl
http://www.lauraweb.mex.tl
http://www.cbapesimec.mex.tl
http://www.delabarrera.mex.tl
http://www.metodologiamimi.mex.tl
http://www.maquinaselectricas.mex.tl
http://www.redestecnologicas.mex.tl
http://www.pcejudo.mex.tl
http://www.rutacritica.mex.tl
http://www.proyectomecanico.mex.tl
http://www.aulavirtualdealgebra.mex.tl
http://www.humanidadesacg.mex.tl
http://www.fisicaesimecuipn.mex.tl
http://www.osvaldolopezgarcia.mex.tl
http://www.rosyomy.mex.tl
http://www.ortizcomp.mex.tl
http://www.fisicaclasicaeym.mex.tl
http://www.larrauri.mex.tl

III. APPLICATION OF THE WEBSITES

Having ready the corresponding website, each participant applied it with his/her groups, during one semester. Depending of the particular subject, the participant was asked to incorporate not just information in their website, but activities that interest the students in active learning. The participant should, as a minimum, incorporate in his/her website:

- Instructor's notes
- Pre-class readings
- Tutorials
- Models

- Puzzles
- Quick quizzes
- QuickLabs
- Homework papers
- Solved problems and homework

The website must be designed so that it is a tool for the teacher to encourage students in active learning, to develop needed skills for the particular subject. The activities incorporated in the Website must be of such a nature that the student be active, not passive. The given information must be used for the students' understanding of a situation and the underlying theoretical basis to analyze the situation, plan and carry out a solution, and check their solution to see if it is reasonable [19].

IV. RESULTS

A. *Questionnaires*

At the end of the semester, each participant filled in questionnaires to determine the students' academic improvement after using the website for their classes. The questionnaires included questions to grade aspects like:

- Assistance of the website in the teacher's daily work in class
- Student's academic improvement before and after using the teacher's website
- Students' concept of teacher's website
- Communication with students, colleagues, faculty and parents
- Quality of website's material
- Grade of assistance the website gives to the students
- Students' attendance
- Students' attention
- Students' involvement in class

B. *Results*

- 90% of the teachers take their website as a powerful tool for their classes
- 55% express that it is easy to upload homework in their website, instead of photocopying.
- 40% upload the particular lesson before class
- 25% upload exercises to be solved at the laboratory instead of in the classroom
- 90% upload homework
- 95% upload lessons
- 100% upload final grades
- 95% upload solved problems, exams
- 100% incorporate links to sites of interest
- 100% improve their classes using their websites

C. *Results evaluation using Non-Parametric Statistics*

Finally, participant teachers were asked to assign a score from 1 to 5 to the academic improvement of their students **before** and **after** using their websites as a tool for their classes. Table 1 shows the scores obtained from a sample of 30 teachers:

Teacher:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Before:	3	4	3	2	4	2	2	1	5	4	5	3	2	2	1
After:	4	5	3	4	5	3	2	4	5	4	4	5	5	3	2

Teacher:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Before:	3	4	4	4	3	2	1	4	2	2	4	1	4	5	6
After:	2	5	5	3	3	5	2	5	1	3	4	3	5	3	5

Table 1. Scores assigned by the participant teachers before and after using their website in their classes

The answers were used to determine if there is a difference in the academic performance of the students when the teacher uses his/her website and when the teacher does not use it. Two tests of the Non-Parametric Statistics were used: the Sign Test and the Wilcoxon Sign Test.

i) Sign Test

If the score is higher "*Before*", a plus (+) sign is assigned, otherwise it is assigned a minus (–) sign; but if there is a "*tie*", no sign is assigned. Both null Hypothesis (Ho) and alternative hypothesis (H_1) have to be postulated, as well as the significance level to use the Table of Values under the Normal Curve (Z Table), to determine the Acceptance and Rejection Zone. (Fig.1)

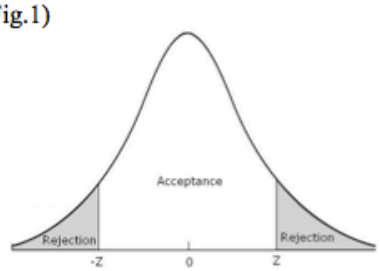


Fig.1. Acceptance and Rejection Zone for Sign Test

With the sample size (not taking onto account the "ties") and the number of plus signs (x) , the value of Z is calculated:

$$Z=(x-\mu)/\sigma$$

where

n=sample size

μ= expected value = n*p = n*(0.5)

$\sigma=(0.25n)^{1/2}$

Finally, Z calculated is placed in the proper zone, according to its value; if it falls in the "Acceptance" zone then Ho is accepted : "There is no difference in the academic improvement of the students "*Before*" and "*After*" the teacher´s website is used in class; if Z calculated falls in the "Rejection" zone, Ho is rejected and H_1 is accepted:"There is a difference in the students' academic improvement before and after the teacher's webpage is used.

ii) Wilcoxon Sign Test

This test takes into account the differences between pairs of scores; these differences give a clue about the characteristics of both scores, in this case the students' academic improvement before and after the teacher used his/her website. Table 2 shows the teachers' scores and the corresponding differences

Teacher	Before	After	Difference	Absolute Difference
1	3	4	1	1
2	5	5	0	0
3	2	1	-1	1
4	2	4	2	2
5	4	5	1	1
6	2	3	1	1
7	1	2	1	1
8	5	4	-1	1
9	4	5	1	1
10	5	4	-1	1
11	3	4	1	1
12	2	5	3	3
13	2	5	3	3
14	2	3	1	1
15	1	2	1	1
16	3	2	-1	1
17	4	5	1	1
18	4	5	1	1
19	4	3	-1	1
20	3	3	0	0
21	2	5	3	3
22	1	2	1	1
23	5	5	0	0
24	2	1	-1	1
25	2	3	1	1
26	4	4	0	0
27	1	3	2	2
28	4	5	1	1
29	5	3	-2	2
30	3	5	2	2

Table 2. Differences between scores assigned by the participant teachers before and after using their website in their classes.

The acceptance and rejection zone are determined exactly as in the sign test, using the significance level and the Table of Values under the Normal Curve, now Z calculated is determined as follows:

$$Z=(T-\mu_T)/\sigma_T$$

where

$\sigma_T=((n(n+1)(2n+1))/6)^{1/2}$

n= sample size – number of zeros

T= sum of range with sign

$\mu_T= 0$

In this case, Ho was rejected, the sample "before" and the sample "after" are not identical, then the perception of the academic condition is different and leads us to the conclusion that it is better after the teacher uses his/her website in class.

In both tests, the Sign Test and the Wilcoxon Sign Test, it was obtained that there is an academic improvement when the teacher uses his/her website during his classes.

V. Conclusion

There is evidence that the use of a website in imparting a subject matter improves the academic performance of the students. The proposal to use a website is in accordance to the present day tendencies of education, as well as with the requirements of distance education, open university, part time students and adult education. With respect to the technology used, this research proves that computers, Internet and specifically the World Wide Web may be used by higher education teachers to create websites to be used in their classes.

From the analysis of the results, 87% of the participant teachers declare that the academic performance in their respective subjects has improved in a regular basis, 67% declare that the website gives them support in their daily work with their classes; finally, the two Non-parametric Tests carried out revealed an improvement in the students' academic performance.

The results of this research confirm the opinion about present day students, in the sense that they use the new technologies extensively, particularly, they use Internet to find information more than any other means (for example the library). Teachers must take advantage of this situation in order to have all kinds of information available to their students via Internet and the World Wide Web.

References

[1] Armand St-Pierre and Campagna Isabelle, "La creación de paginas Web," Ed. Trillas, 1999.

[2] Carnevale, Dan. "Distance education can bolster the bottom line, a professor argues". Chronicle of Higher Education. Vol. 46 Issue 9, pA60, 1/5p, 1999.

[3] Dede, D. "The evolution of distance education: Emerging technologies and distributed learning". The American Journal of Distance Education, 10(2), 4-36, 1996.

[4] Dillich, Sandra."Classrooms go on line". Computer Dealer News, Vol.15 Issue 41, p30, 1/2p, 1999

[5] Fleming, Jennifer."Web navigation: Designing the user experience". Sebastopol, Calif.: O'Reilly, 1998.

[6] Gamble, K & Raney, B. "Teaching through the Web".http://teachonweb.org/teaching/teaching.html, 1998.

[7] "Guiding Principles and Practices for the Design and Development of Effective Distance Education". A Report of the Faculty Initiative Funded by a grant from the AT&T Foundation. Penn State University, 1997.

[8] Harrower, Tim."The newspaper designer's handbook", 4th ed. Boston: McGraw-Hill. 1998.

[9] Jonassen, D., Davidson, M., Collins, M., Campbell, J., & Hagg, B.B. "Constructivism and computer-mediated communication" The American Journal of Distance Education, 9(2), 7-26, 1995

[10] Larrauri S. Alejandro "Training teachers in the Accounting and Business Administration area for the creation of didactic material and its publication in the World Wide Web" Master Thesis. U.N.A.M. México. 2004.

[11] Leduc, St. Pierre "HTML Creación y Difusión de Páginas Web" Ed..Trillas 1999.

[12] Nielsen, Jakob. "*The alertbox: Current issues in Web usability*". http://www.useit.com/alertbox, 1999.

[13] Nielsen, Jakob. "Designing Web usability: The practice of simplicity". Indianapolis, Ind. New Riders, 1995.

[14] Read, Brock."Blackboard´s Chairman Edits a Scholarly Work on the Internet and Higher Education", 2002.

[15] Rosenfeld, Louis, and Peter Morville." Information architecture for the World Wide Web". Sebastopol, Calif.: O'Reilly, 1998.

[16] Sklar, Joel. "Principles of Web design". Cambridge, Mass.: Course Technology, 2000.

[17] Masie, E."Advice for designer of online learning—think small. Technology for Learning. Principles of Good Practice for Electronically Offered Academic Degree and Certificate Programs". http://www.wiche.edu/Telecom/projects/principles.htm , 1997.

[18] Serrano, Carolina Task Force for the American Council on Education and The Alliance: An Association for Alternative Programs for Adults."Guiding Principles for Distance Learning in a Learning Society",1996.
http://www.pbs.org/learn/als/publication/agenda/97fall/credo.htm

[19] R.A. Serway and R.J. Beichner "Physics for Scientists and Egineers", Harcourt College Publishers 5th ed., vol. 2, 2000.

[20] Turgeon, A."Implication of web-based technology for engaging students in a learning society". Journal of Public Service and Outreach, 2(2), 32-37, 1997

[21] Veen, Jeffrey. "The art and science of Web design". Indianapolis, Ind.: New Riders, 2001.

Proposed security architecture for mobile communication

R. Vignettes-Bautista , L. Palacios-Luengas , G. Delgado-Gutiérrez , R. Vázquez-Medina *Member, IEEE*

rvignettes0900@ipn.mx, lpluengas@msn.com,
gdelgadog0902@ipn.mx, ruvazquez@ipn.mx

Instituto Politécnico Nacional, SEPI-ESIME
Culhuacán.

Abstract—This paper examines the characteristics and deficiencies of some security systems actually implemented in the communication of mobile devices. It proposes a system architecture able to warranty the services of authentication, confidentiality, integrity, and non-repudiation in cellphone mobile communications, independent from the cellular network and the phone company. In this proposal, the appropriated and efficient for the technological and computing resources available cryptographic protocols are shown.

Index Terms—Mobile Computing, Cryptography, Computer Security

1 Introducion

The use of the communications on the GSM[1] networks using mobile phones and people's pleasing to mobile devices is more frequently. Besides, the essential to look for information and information exchange using cellular network has brought real mobility. However, the wireless communications channels on the GSM networks are still more insecure than before. Due to this, any person could get information such as the dialing number, replace information and probably the most important thing record phone calls. As a matter of fact, the GSM system provides a security degree using A5/2 protocol encryption in Mexico. Nevertheless, this standard has been broken in several times verify the attacks on[1]. For this reason it is important to provide highly reliable tools as well as advance on the development of efficient tools that allow information protection thus satisfying user security demands. In this paper we propose a system for security data exchange in the GSM network environment. The purpose of this, is to establish secure sessions using Public key infrastructure *(PKI)*, communication protocols of negotiation and cryptography parameters. This protocol will allows users to communicate and authenticate with other members using a digital certificate, with these parameters a session key is generated using asymmetric cryptography such as Elliptic Curves Cryptography *(ECC)*. Besides, in the exchange communication stage it is necessary uses a key to encryption/decryption the information between devices using symmetric cryptography such as DES, AES, Twofish etc. to provide confidentiality. Likewise the system proposal must offer the following security characteristics: confidentially (in transmission or storage of information), integrity (no change can be made undetectably), authentication (determining whether someone or something is, in fact, who or what it is declared to be) and non-repudiation (the sender should not be able to deny sending the message)[2].

- *Instituto Politécnico Nacional, SEPI, ESIME-Culhuacan, Av. Santa Ana No. 1000 Col. San Francisco Culhuacan Delegación Coyoacán, 04430 México D. F.*
E-mail: rvignettes0900@ipn.mx, lpluengas@msn.com, gdelgadog0902@ipn.mx, ruvazquez@ipn.mx

1. *Global System for Mobile Communications*

2 GSM Networks Authentication and Confidentiality

Nowadays, mobile networks communications security is based on the own GSM security in which the standard establishes protocols A3 *(SIM card authentication over GSM network)*, A5 *(mobile-GSM base cyphering algorithm)*, and A8 *(A5 Key generation algorithm)*, as the responsible

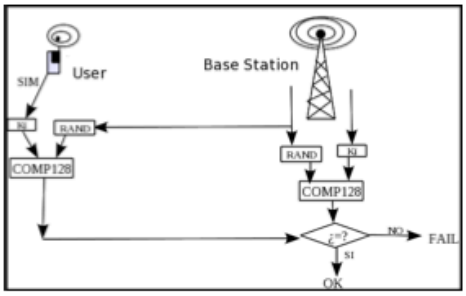


Fig. 1. Authenticacion and Keys Generation

for the security[3].

In Mexico, referents A3 and A8 are implemented for the algorithm COMP128, with a low security level, that is why SIM cards cloning are relatively simple [4]. A3 and A8 consist in the generation of key sessions and authentication by comparing a pre-shared secret K1, hosted in the SIM module *(subscriptor identification module)*, and the base station.

The COMP128 algorithm requires of a 128-bits pseudorandom number, generated by the base station, and shared to the SIM besides the 128 bits of K1, which go through an iterated compression, with a butterfly form, obtaining 64 bits that are used as a key for the A5 cyphering. Refer to figure 1.

Once the session key among the base station and the SIM module is accorded, this is used as a seed in the generation of a pseudorandom sequence produced by A5/1 or A5/2 which is a LFSR stream cypher[5]. With the LFSR, the traffic is cyphered among the mobile and the base station. It is remarkable that this cypher can be attacked without breaking A3 and A8 previously, the attack can even carried out on real time [6] using an ordinary computer, with at least two conversation minutes the session key could be found, this will allow that subsequent data is deciphered easily, which results worrying. Moreover, these algorithms (A3, A5 and A8) have never been submitted to public scrutiny, which generates doubts about possible weaknesses, some of them can be observed at [1].

3 Mobile Applications for Secure Communication

Considering what has been said, it is obvious that, recently, many companies have put up for sale mobile applications that ensure mobile communications, like Apple, with the application Encrypt SMS available on iTunes, or the application SSL VPN by StoneSoft. The functionality of these applications is similar among them; they work on a peer to peer communication, where a session key is shared through an asymmetric cyphering. Later, regular traffic is delegated to a symmetric cyphering. Despite this, SIM module cloning is feasible because identity impersonation is not covered by all the applications, added to this, susceptibility to a man in the middle attack is an important insecurity factor.

4 Cryptography for Mobile Computing

4.1 Symmetric Ciphering

This kind of cyphering is used to maintain the confidentiality of cyphered information, which can be only intelligible knowing the key with which it was cyphered, known as the secret key, symmetric cyphers are relatively fast and that is why they are used to cypher traffic in a safe channel.

AES algorithm *(Advance Encryption Standard)*, since its' beginning as a new cyphering standard[7] of the United States government, in 2001, has no effective attacks known, besides than in the contest proposed by the NIST[2], was the best, compared to other algorithms like Twofish, for efficiency and a better hardware implementation reasons, that is why AES is considered as the optimum candidate for symmetric cyphering in mobiles.

4.2 Asymmetric Ciphering

Asymmetric cyphering, where the key used for the cyphering process is the same than the one for the deciphering process, we have the same inherent problem for the secret key sharing,

2. *National Institute of Standards and Technology*

in other words, a safe channel is required to share the key. In order to solve this, in 1976, the first asymmetric cypher for key sharing was published[8].

In this protocol, there is a pair of keys, a public key and a private key, with these two keys, a secret among two entities can be shared on a non-safe channel. Towards 1985, elliptic and hyper elliptic curves about finite fields F_{q^e} theory has been used in cryptographic applications due to a greater efficiency compared with other methods.

An interesting comparative using a mobile device and a laptop as a server [9] delivers results that show how cryptography of elliptic curve is more efficient than RSA; this is for both, conventional, and mobile computing. We can notice that ECC is the best option for mobile devices. To implement this cryptographic protocol, NIST recommends ECDSA *(Ellpitic Curve Digital Signature)* with SHA as a hash function for a digital signature. For a guide for this scheme implementation refer to [10].

5 Proposes Architecture

5.1 Fundaments

A Public Key Infraestructure *(PKI)* allows users to authenticate with others, and use their digital certificates that contain the digital public key to establish a session key, as well as digital signing of information. Through this, they can communicate in a safe way among them, due to confidentiality in cyphering, authenticity in digital certificates, integrity and non-repudiation
with digital signature.

An important actor on PKI is the Certification Authority or CA, which is the responsible for the generation and administration of certifies, and their renewal once they have expired. User in CA, in this case, mobile devices must, for the first instance, fully authenticate with the CA. As seen on previous paragraphs, Sims can be cloned and would not be enough to have PIN *(Personal Identification Number)* embedded on the SIM

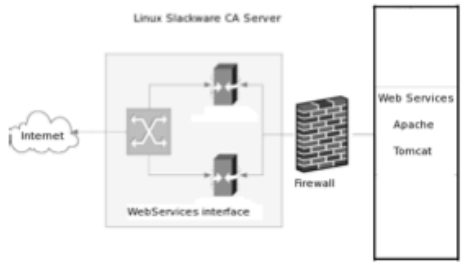


Fig. 2. CA Server Implementation

to identify the mobile, that is the reason why another identifier is needed; this is unique and printed on hardware, known as the IMEI[3]. The IMEI and the public user key added to other classic data from the user like name, phone, ...etc, are delivered to the CA which extends a digital certificate that is unique for an specific user and which can be required publicly.

On the mobile device, there is the security application, which besides storing digital trusted certificates related to the user's phone number, generates keys using ECC, and besides, cyphers traffic with AES in OFB *(output feedback)* mode[11] in order to manage it as a stream cyphering, using resources from the mobile device or with cryptographic hardware assistance via USB or Bluetooth.

5.2 Description

An emitter user wants to call another one in a safe way, uses the security application, which automatically sends an SMS[4] that contains a request, its digital certificate, in case of not being a trusted source, and a pseudorandom number cyphered with the public key of the receptor, obtained through the digital certificate delivered by the CA.

The receptor user detects the message and the application recognizes the user as a trusted one if it finds the digital certificate related to that number in its database, on the other hand, it looks for it on the emitter

3. *International Mobile Equipment Identity,*
4. *Short Message Service*

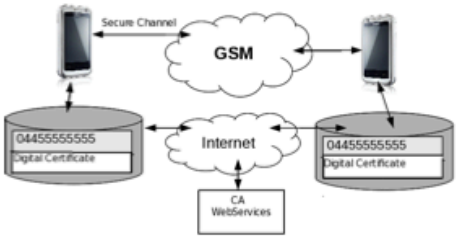


Fig. 3. PKI Scheme for mobile application

message. The security application deciphers the pseudorandom number and sends the emitter, if required, a SMS with the digital certificate of the receptor and the number received, with another pseudorandom number, generated in the receptor and cyphered with the public key of the emitter.

The security application automatically recognizes the SMS and verifies the certificate is legitimate. If it is valid, deciphers the pseudorandom number with its private key, these numbers will be the secret key in the stream cyphering established.

Once the secret key is shared, the security applicative calls immediately the receptor, cyphering the traffic, and the receptor answers deciphering also, this generates a safe communication channel, as shown in the figure3. The session key can last for a call or more, depending on the parameters accorded on the mobile security application.

5.3 Implementation Requirements

This CA implementation through internet, placing two servers in cluster, before the firewall exposes the web services that the CA offers, as shown in the figure 2, using a balancer to deliver the amount of information among the two servers with the intention of not exposing the CA to possible external attacks, the most severe of them is from far away, the robbery of the private key of the CA, that is why it must be always guarded cause of its protection depends the security of the whole infrastructure.

Web services of the CA can be consumed by the mobile devices with an application based on the API of the device and the framework offered by the manufacturer, this application has the primary function of asking the CA for digital certificates, as well as extend requests to revoke or renew these certificates. For the implementation a GNU/Linux Slackware distribution is used as the operating system added to Security Enhanced Linux, Apache and Tomcat as webserver, and servlets host respectively.

6 Conclusion

After observing the actual security of the GSM network, it can be classified as not sufficient secure, that is why using external applications independent from the network and the phone company is a viable option in measure of a cost-benefit balance among performance and security.

Also we can notice the high efficiency obtained through cryptographic processes, specifically Elliptic Curve Cryptography, for this reason, on the next years, it will have a greater importance, even relieving RSA, overall if the development of more and better reconfigurable hardware implementations on cryptographic primitives that can optimize the device's performance is considered.

Commercial applications offer confidentiality and integrity, but a great amount of them does not offer a trusting authentication and non-repudiation. The architecture presented, which consists on a mobile application and a CA server, offers these four security-required services, offering an option on mobile devices security that is viable with the disadvantage of depending on the speed of SMS transmission for keys exchange.

Acknowledgments

This paper is framed on the support provided by the CONACyT scholarships ID-244598, ID-372164 and the support on the project SIP-20102510 of the Instituto Politécnico Nacional.

REFERENCES

[1] E. Barkan; E. Biham; N. Keller. *Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication.* Israel Institute of Technology.

[2] S. Díaz Santiago. *Generación de Sucesiones Criptográficamente Fuertes.* Universidad Autónoma Metropolitana.Tesis de Maestría. 2005.

[3] M. Suominen. *Security of Communication Protocols* Helsinki University of Technology, S-38.153. 2003.

[4] C. Brookson *GSM Security and Encryption.* Computer Science Division, University of California, Berkeley, 1994.

[5] B. Schneier. *Applied Cryptography. Protocols, algorithms and source code in C.* John Wiley & Sons, 1994.

[6] A. Biryukov; A. Shamir. *Real Time Cryptanalysis of the Alleged A5/1 on a PC* The Weizmann Institute Rehovot.1999.

[7] National Institute of Standards and Technology. *Advanced Encryption Standard (AES).* Federal Information Processing Standards Publication 197 FIPS PUB197. November 26, 2001.

[8] W. Diffie; M. E. Hellman. *New directions in cryptography.* IEEE Transactions on Information Theory. 1976.

[9] C. E. López Peza *Sistema de Seguridad para Intercambio de Datos en Dispositivos Móviles* Departamento de ingeniería eléctrica sección de computación, CINVESTAV.Tesis de Maestría. 2005.

[10] Nist National Institute of Standards and Technology. *Digital Signature Standard (DSS).*Federal Information Processing Standards Publication 186-3. FIPS PUB186-3. November 26, 2001.

[11] A. Menezes; S. Vanstone; P. van Oorschot. *Handbook of Applied Cryptography.* CRC Press, 1997.

[12] C.E. Shannon. *A mathematical theory of comunications.* Laboratorios Bell,Tech. J. 1948

[13] D. Kahn.*The Codebreakers.* The Comprehensive History of Secret Communications from Ancient times to the Internet. Scribner, 1967.

[14] N. koblitz; A. H. Koblitz; A. J. Menezes *Elliptic curve cryptography: The serpentine course of a paradigm shift.* Journal of Number Theory. 2008.

[15] R.L. Rivest; A. Shamir; L. M. Adleman.*A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM, 21, 120-126, 1978.

[16] RSA Laboratories. *RSA Cryptography Standard.* PKCS #1 v2.1. 2002.

[17] T. Farley. *The Cell Phone Revolution.* American heritage of invention & technology. ISSN 8756-7296.2007

[18] W. Stallings. *Cryptography and Network Security. Principles and Practices.* 3a ed. Prentice Hall. 2003.

Rodrigo Vignettes Bautista Graduate from ESCOM as *Computer System Engineer* in 2009, by the Intituto Politécnino Nacional. During this year, he developed activities on the business environment as consultor in informatic security. Actually, he is studying the first semester of the Master in *Security and Information Technologies Engineering* in the postgraduated section at ESIME Culhuacán. His areas of interest are Cryptography, Computer Security and Operating Systems. *rvignettes0900@ipn.mx*.

Leonardo Palacios Luengas. Received the title of *Communications and Electronics Engineer*, with an speciality in communication in year 2003, by the Instituto Politécnico Nacional. He worked as an electronic Designer at the CINVESTAV from Instituto Politécnico Nacional in the project MARINA-2002-CO1-3199 form the sectorial background CONACyT- Secretara de Marina. Actually, he is studying the first semester of the master in *Sciences of Microelectronis Engineering* in the postgraduate section at ESIME Culhuacán. His experience is based on the areas of Digital Electronic Design and Embedded Systems Programming. His areas of interest are Electronic Cryptography and Communications. *lpluengas@msn.com*.

Guillermo Delgado Gutiérrez Graduate from ITESM as *Electronic Systems Engineer* on 2008. He worked as field engineer on oil platforms, programming security systems (Emergency Shut Down and Gas & Fire Detection) for a year and a half. Actually, he is studying the first semester of the master in *Sciences of Microelectronis Engineering* in the postgraduate section at ESIME Culhuacán. His areas of interest are Digital Security, Signals Processing and Digital Forensics. *gdelgadog0902@ipn.mx*

Rubén Vázquez Medina, Member, IEEE Born in Mexico City in 1966. Received the title of *Electronic Engineer* with speciality in Communications at the Universidad Autónoma Metropolitana, at Iztapalapa. Then he received the degree of Master in Science with speciality in Electric Engineering with option in Telecommunications on September 1991 at the CINVESTAV. He obtained the PhD at Universidad Autónoma Metropolitana, at Iztapalapa on October 2008. He was chief of the Postgraduate section at ESIME Culhuacn from March 2003 to August 2006. Actually he I professor at the ESIME Culhuacn form IPN, on the programs of postgraduated in the Master in *Sciences of Microelectronis Engineering* and the Master in *Secutiry and information Technologies Engineering* as well as the PhD in Communications and Electronic. His areas of interes are cryptography, steganography, Informatic Forensics and Digital Forensics. *ruvazquez@ipn.mx*

Instrucciones para los autores

Los artículos que se someten a **RISCE** deben contener resultados inéditos y originales, no haber sido publicados con anterioridad ni haber sido sometidos simultáneamente a otra revista científica. Si el artículo ha sido presentado, sometido o publicado en alguna otra parte, deberá informarse al coordinador editorial. Los artículos deben ajustarse a las siguientes especificaciones:

- Idioma Inglés (anexar un resumen y palabras clave en español)
- Idioma Español (anexar un resumen y palabras clave en Inglés)
- Procesador de texto admitido: MS-Word.
- Tamaño de página: carta , utilizar un solo lado de la hoja. Máximo 10 páginas.
- Márgenes: izquierdo 2.5 cm y derecho 2 cm., superior 2.5 cm e inferior 2.5 cm.
- Autores: primer nombre seguido de los dos apellidos (sin abreviaturas), abajo: afiliación y e-mail.
- Tipo de letra del texto regular: Times o Times New Roman de 10 pt (título original 22 pt; secciones 11.5 pt, subsecciones 11.5 pt, en negritas).
- Texto: a una columna y con espaciado sencillo (renglón seguido).
- Resumen/Abstract: entre 70 y 150 palabras, colocado al principio del texto, seguido del de Español o inglés según sea el caso.
- Palabras clave/Keywords: colocadas después del resumen en negritas, y no más de 10.
- Imágenes y fotografías: deben ser de alta calidad, con colores bien definidos y contrastantes, en mapa de bits (no sectorizadas) en formato JPG e incrustadas en el texto de forma que se puedan manipular independiente.
- Fórmulas: Deberán de presentarse en formato de tabla sin bordes, centradas y la numeración de c/u justificada a la derecha con negritas en mapa de bits, no vectorizadas.
- Pies de figura. Deben mencionarse dentro del texto y numerarse de manera consecutiva con un tipo de letra Times New Roman 9 puntos
- Cabecera de tabla. Deberá presentase en la parte superior de la tabla un numeración consecutiva y descripción con tipo de letra Times New Roman 9
- Referencias:

En cualquier caso el nombre del autor del artículo o publicación web deberá mostrarse al principio. Deberán ordenarse conforme aparezcan dentro del texto encerradas entre paréntesis cuadrado —[ ]‖. A continuación algunos ejemplos:

[1]. Baldonado, M., Chang, C.-C.K., Gravano, L., Paepcke, A.: The Stanford Digital Library Metadata Architecture. Int. J. Digit. Libr. 1 (1997) 108–121

[2+. Bruce, K.B., Cardelli, L., Pierce, B.C.: Comparing Object Encodings. In: Abadi, M., Ito, T. (eds.): Theoretical Aspects of Computer Software. Lecture Notes in Computer Science, Vol. 1281. Springer-Verlag, Berlin Heidelberg New York (1997) 415–438

[3]. van Leeuwen, J. (ed.): Computer Science Today. Recent Trends and Developments. Lecture Notes in Computer Science, Vol. 1000. Springer-Verlag, Berlin Heidelberg New York (1995)

[4]. Michalewicz, Z.: Genetic Algorithms + Data Structures = Evolution Programs. 3rd edn. Springer-Verlag, Berlin Heidelberg New York (1996)

Instrucciones:

Enviar el archivo en extenso a la siguiente dirección electrónica: ebustosf@gmail.com

Los revisores técnicos le harán llegar sus observaciones y modificaciones, las cuales deberá realizar y reenviar el archivo corregido al correo arriba mencionado.

El comité editorial se comunicara mediante correo electrónico indicándole la aceptación o rechazo del artículo.

Se le solicitará autorización para publicación; en caso de aceptar se le indica la cuenta donde debe hacer el depósito por cobro de publicación y el costo, el cual no debe exceder de $1000.00 pesos mexicanos.

Reserva de Derechos 04-2008-062613190500-203