Identificación de Usuarios Basado en el Reconocimiento de Patrones de Tecleo

Daniel Acevedo
Universidad Central de Venezuela, Facultad de Ciencias,
Escuela de Computación, Caracas, Venezuela
dacevedo@acmgrp.com

and

Glemarys Hernández
Universidad Central de Venezuela, Facultad de Ciencias,
Escuela de Computación, Caracas, Venezuela
glema@cantv.net

and

Eugenio G. Scalise P.
Universidad Central de Venezuela, Facultad de Ciencias,
Escuela de Computación, Centro ISYS, Caracas, Venezuela
escalise@acm.org

Resumen

En este trabajo se plantea un método para la identificación de usuarios basado en el reconocimiento patrones de tecleo utilizando una Red de Base Radial. Para la realización de las pruebas de reconocimiento se tomaron datos generados por los eventos de teclado de una aplicación de mensajería instantánea por Internet. Durante el entrenamiento del modelo se utilizaron datos de tecleo de diecisiete usuarios de habla hispana. Tales datos están conformados por el tiempo transcurrido entre pares de letras tecleadas consecutivamente y el par de letra tecleado por el usuario. Estos pares fueron tomados de una lista de cuarenta pares seleccionados durante el estudio. Como resultado se obtuvo un módulo de reconocimiento de patrones de tecleo con resultados de reconocimiento aceptables.

Palabras claves: inteligencia artificial, redes neuronales, redes neuronales RBF, patrones de tecleo, biometría, identificación de usuarios.

Abstract

In this work it is presented a method for the user identification based on the pattern recognition of keystrokes, using a Radial Base Neural Network. For the accomplishment of the recognition tests it were used data generated by the events from keyboard of an instant messaging program. During the training of the model, it were used keystroke data of seventeen hispanic speech users. Such data contains the time passed between pairs of consecutively letters and the pair of letters keyed in by the user. These pairs were taken from a list of forty pairs selected during the study. As a result, we have obtained a recognition module of keystrokes with acceptable recognition levels.

Keywords: artificial intelligence, neural networks, radial basis function networks, keystroke pattern, biometry, user recognition.

Introducción

Desde tiempos inmemoriales, la información ha jugado un papel importante para el hombre. Esto se evidencia en los diferentes métodos utilizados para asegurar su confidencialidad. Durante el antiguo Egipto, la escritura no era accesible al común de la gente, garantizando que sólo un grupo reducido de personas pudieran acceder a la información. Posteriormente, el ejército romano utilizó el cifrado del Emperador Julio Cesar para ocultar sus mensajes, desplazando el alfabeto tres letras, siendo imposible descifrar el mensaje sin tener conocimiento de ello. En la Segunda Guerra Mundial, Churchill y Roosevelt se comunicaban telefónicamente sólo si estaban seguros de que no lo estuvieran espiando, o que si lo hacían no los entenderían. [8]

La información es sinónimo de poder. Resulta fácil imaginar lo que podría suceder si se conoce toda la información que maneja la NASA, el departamento de seguridad de los EEUU o las instituciones bancarias a nivel mundial.

Por otra parte, la sociedad actual demanda cada vez mayor información y los medios utilizados para transmitirla se encuentran, generalmente, al alcance de muchas personas, lo que constituye una gran ventaja: la información se encuentra disponible para ellas. Sin embargo, no todos están dispuestos a compartir la información que poseen, por lo que es necesario implementar mecanismos de seguridad que limiten el acceso sólo a personas autorizadas. De igual manera, se debe garantizar que la información proviene de fuentes confiables debido al valor asociado a ésta.

Es por ello que en este artículo se plantea una alternativa biométrica para la identificación de usuarios que contribuye a incrementar la seguridad de los sistemas. El mismo se estructura de la siguiente manera: se presenta el planteamiento del problema, luego se expone la técnica de reconocimiento de patrones utilizada en la identificación de usuarios, junto con los resultados obtenidos, finalizando con las conclusiones de la investigación.

1 Planteamiento del problema

La información es un bien que adquiere cada vez mayor relevancia. No solo debe ser protegida de posibles ataques y limitar el acceso a ella, sino además, se debe garantizar que proviene de fuentes confiables.

La identificación del usuario o cliente es un punto fundamental para garantizar la seguridad en los sistemas de información. Un ejemplo de ello puede observarse en las instituciones bancarias que solicitan a sus clientes una clave compuesta por varios dígitos para movilizar su dinero con la tarjeta de débito. Igualmente, algunos celulares necesitan de un número de identificación personal (PIN) para poder iniciar sus funciones. Acceder a la mayoría de los servicios provistos en Internet requiere de un *password* o contraseña. Los Sistemas Operativos que funcionan en ambientes locales o de red utilizan también este mecanismo. Todas estas situaciones tienen algo en común: el uso de una clave personal para acceder al sistema y poder operar en él. Esta clave personal constituye a la vez un riesgo. Al ser información que puede ser compartida o descubierta, el sistema tiende a ser vulnerable al fraude.

Por otro lado, hacer uso de Internet para intercambiar información es muy común hoy día para quienes tienen acceso al medio. Un estudio realizado en España por AIMC [3] revela que el 95.3% de los usuarios de Internet utiliza el servicio de correo electrónico, el 38.8% participa en charlas interactivas o *chats* y un 18.2% hace uso de los foros de discusión. De aquí que sea importante tener la certeza de que la información proviene realmente de quien dice provenir. Una manera de garantizarlo es a través de la identificación de los usuarios que intervienen en el intercambio.

La tecnología biométrica resulta una alternativa al momento de reconocer o identificar a un individuo, ya que utiliza las características del mismo para su identificación. De este modo, sólo el usuario es propietario de la información. Dichas características pueden ser físicas, tales como las huellas dactilares, el contorno del rostro y la retina, o aprendidas, puesto que miden el comportamiento del usuario, tales como el timbre de voz y la firma manuscrita. Sin embargo, los equipos utilizados para captar estas características resultan bastante costosos y, por consiguiente, poco disponibles para el usuario común.

Otra alternativa biométrica menos costosa está basada en la dinámica de tecleo del usuario. La misma consiste en identificar a un individuo tomando en cuenta el modo de teclear un texto, ya que se ha demostrado que cada individuo posee patrones únicos de tecleo asociados a la velocidad de tecleo o a la presión ejercida al teclear [4].

Entonces, teniendo en cuenta lo importante que es mantener la seguridad y las necesidades de tener un método alternativo de bajo costo para el reconocimiento de usuarios, se desarrolló un sistema reconocedor de patrones de tecleo [1] capaz de diferenciar a un usuario de otro, utilizando como equipo de adquisición de datos el teclado, tomando en cuenta la velocidad del usuario al teclear como característica de tecleo. Como métrica se utilizó el intervalo de tiempo registrado entre un par de letras tecleadas de manera consecutiva.

En detalle, el sistema desarrollado captura los eventos de teclado del usuario y registra los tiempos entre pulsaciones. Con esa información se construye una plantilla de reconocimiento que permite identificar unívocamente a un usuario, es decir, se determinan los patrones de tecleo asociados a éste.

Para efectuar el reconocimiento, se utilizó una de las técnicas de reconocimiento de patrones que mejor desempeño obtuvo en las pruebas que se realizaron para tal fin.

1.1 Ambiente de trabajo

Lo más importante para un sistema de identificación de usuarios es el grado de certeza de contar con un método efectivo para el reconocimiento o identificación. Es por ello que fue necesario que el sistema reconocedor de patrones de tecleo a desarrollar arrojase resultados confiables, reconociendo efectivamente a un individuo y rechazando eficazmente a los intrusos, distinguiendo entonces entre un grupo de individuos.

Un sistema que permita reconocer a un individuo por medio de la velocidad de éste al teclear puede tener múltiples aplicaciones. La facilidad de uso que proporciona al usuario y el bajo costo que representa al no necesitar equipos de avanzada tecnología, lo hacen una opción para el reconocimiento de usuarios bastante atractiva. De esta manera, el sistema a desarrollar debía ser independiente y usable, es decir, capaz de brindar las facilidades necesarias para que pudiera ser utilizado por cualquier aplicación que generara eventos de teclado. Adicionalmente, debía permitir el uso de éste en diferentes escenarios.

Para darle respuesta a cada uno de los requerimientos planteados, el sistema reconocedor de patrones de tecleo se desarrolló como un módulo independiente de reconocimiento, en el cual se implementaron las funciones pertinentes al método de reconocimiento de patrones seleccionado, y que permitiese establecer una conexión con otras aplicaciones.

Para probar el desempeño del módulo en el reconocimiento de patrones de tecleo, fue necesario diseñar e implementar una plataforma de operación donde se pudiesen realizar las pruebas y así verificar si el reconocimiento se realizó exitosamente. Dicha plataforma cuenta con los siguientes elementos:

- Un generador de eventos de teclado (AGE): Esta aplicación es la encargada de captar las interrupciones de teclado y generar los eventos de teclado del individuo en estudio. Entre los AGEs más comunes que pueden ser utilizados para el reconocimiento se tienen editores de texto, clientes de correo y *chats*.
- Un filtro-receptor (AFR): Esta aplicación monitorea todos los eventos de teclado proveniente de AGE, registra los tiempos ocurridos entre pares de teclas y filtra la información que va a ser suministrada al módulo.
- Un almacén de datos (AD): Este elemento es el responsable de almacenar las plantillas de reconocimiento de cada usuario encontradas durante la etapa de entrenamiento. Una plantilla de reconocimiento representa las características únicas del usuario utilizadas para la identificación a partir de ejemplos biométricos.

1.2 Captura de datos

Para la captura de los datos se utilizó el producto del servicio de mensajería por Internet MSN Messenger versión 4.6 como un AGE para probar el módulo de reconocimiento dada las siguientes ventajas:

1. La frecuencia de uso de este servicio por parte de sus usuarios genera gran cantidad de información de tecleo que puede ser usada en el reconocimiento de los individuos en estudio.
2. La gran cantidad de usuarios que posee el servicio facilita la búsqueda de individuos para probar la aplicación.
3. La aceptación del servicio entre sus usuarios facilita el hecho de que más individuos se sumen al estudio.
4. El producto puede descargarse gratuitamente vía Internet y su instalación resulta sencilla.
5. Cuenta con un API que facilita la obtención de los eventos generados por esta aplicación, de manera transparente para los usuarios.

Como AFR se desarrolló una aplicación, denominada TGD, que guarda la información de cada par de letras tecleadas consecutivamente y el tiempo transcurrido entre una y otra letra para todas las ventanas de conversación de MSN Messenger que el usuario mantenga con otras personas.

La validez de los datos desempeña un rol importante para la precisión del reconocimiento. Al basar el estudio en registro de tiempos, la manera en que midan los datos debe garantizar que las mediciones sean independientes a los ciclos de reloj del procesador de la máquina del usuario. Para registrar el tiempo de tecleo entre dos letras se utilizó una función tomada del API de Windows llamada `TimeGetTime` [10]. Esta función retorna el tiempo actual del sistema en milisegundos y su resultado no varía en relación a la velocidad del procesador. La misma es comúnmente utilizada en aplicaciones que demandan una alta resolución en el tiempo, tales como programas 3D, donde se cuenta la cantidad de cuadros desplegados por segundo.

Para el muestreo de los tiempos de tecleo en las ventanas de conversación de MSN Messenger se utilizó la función `SetWindowsHookEx` [10], perteneciente también del API de Windows. Esta función está disponible dentro de una librería de enlace dinámico (DLL) y captura todos los eventos de teclado generados en el ambiente para así poder tomar el tiempo transcurrido entre cada par de letras tecleadas consecutivamente. Para identificar cuáles de estos eventos ocurren dentro del ambiente de una ventana de conversación de MSN Messenger, se utilizó la función `CallWindowProc` [10], también perteneciente al API de Windows y disponible dentro de un DLL.

El resultado del monitoreo de las letras escritas en MSN Messenger y el tiempo que transcurre entre la ocurrencia de cada una de ellas es almacenada en un archivo de registro. El formato del almacenamiento de los datos en el archivo es el siguiente: al inicio del mismo se encuentra el correo del usuario que se conectó al servidor de MSN Messenger, posteriormente, en cada una de las líneas siguientes se tiene la información de cada par de teclas presionadas dentro

de una ventana de conversación y el tiempo transcurrido entre ellas.

Para detectar cuando un usuario se está conectando al servidor de MSN Messenger, se utilizó el API de MSN Messenger versión 4.6 [10]. Esta interfaz permite capturar entre otros mensajes, los eventos de conexión al servidor, junto con el correo con el que se está haciendo la autenticación del usuario.

1.3 Selección de pares

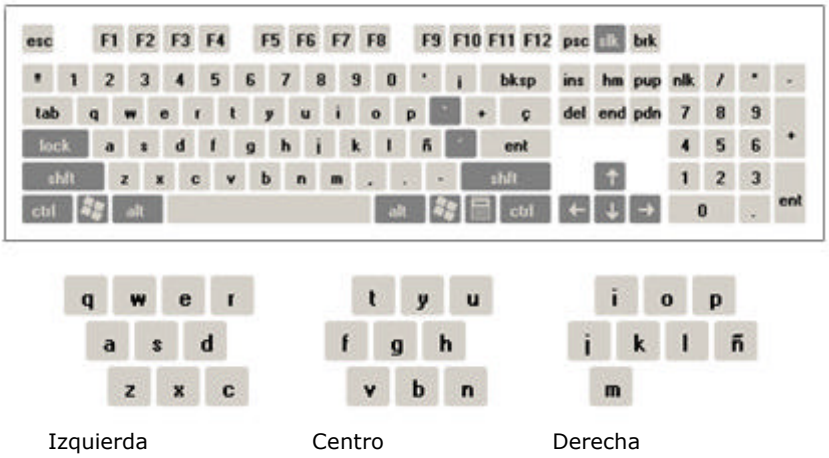
La métrica seleccionada para realizar el reconocimiento es la velocidad del usuario al teclear, teniendo en cuenta el tiempo que toma éste al pulsar dos teclas de manera consecutiva. Como es de esperarse, no fue necesario analizar toda los datos suministrados por el usuario. Si se observan los pares de letras que se pueden formar a partir del alfabeto, resulta evidente que existen combinaciones que son poco probables que ocurran al escribir un texto, tales como el par wx o el par qz, tomando en cuenta que el idioma utilizado en todas las conversaciones es en español. Adicionalmente, dependiendo del contexto en donde se esté escribiendo, se van a usar o dejar de usar ciertas palabras y con ello, ciertos pares pueden tener más o menos número de ocurrencias. Estas diferencias se observan al redactar una carta a una institución, al escribir un correo personal o al chatear con amigos.

Luego, teniendo en cuenta que se utilizó el MSN Messenger como un generador de eventos de teclado, fue necesario analizar los pares de letras con mayor número de ocurrencias entre los usuarios al utilizar esta aplicación. Para tal fin se desarrolló un programa que registra todos los eventos de teclado generados por el usuario al utilizar el MSN Messenger, al cual se le llamó TGD. Cuando se producen eventos de teclado, se registran los pares de letras asociados a los eventos ocurridos. Los eventos correspondientes a números o caracteres especiales fueron ignorados. De esta manera, se produce un archivo de registro con la información de los pares de letras tecleados consecutivamente al enviar un mensaje a algún contacto del usuario en MSN Messenger.

Es importante resaltar que la pulsación de un caracter especial, como el acento, o una tecla de control, como *shift*, entre un par de letras trae como consecuencia que dicho par no sea tomado en cuenta para el estudio, ya que las letras pertenecientes al par no fueron tecleadas de manera consecutiva.

TGD fue instalado a un grupo de treinta usuarios con el objetivo de recolectar datos referentes a los mensajes escritos por éstos al mantener una conversación. Teniendo en cuenta la frecuencia con que es utilizado Messenger entre las personas que conformaron el grupo, se estimó que el tiempo de uso de TGD fuese de dos semanas. Una vez culminado este tiempo, sólo siete usuarios tenían información relevante para el estudio y los archivos generados por estos usuarios fueron procesados con el fin de determinar los pares con mayor número de ocurrencias entre ellos.

Cada usuario generó un archivo de registro que fue tabulado y comparado con el resto de los usuarios. Para cada individuo, los pares fueron ordenados de mayor a menor de acuerdo al número de ocurrencias del par y numerados para obtener la posición de éste en cada individuo. Luego, para obtener la posición del par en el grupo, se promedió la posición que ocupaba el par en cada uno de los individuos. Esta última posición fue utilizada para seleccionar los pares que serían usados para el reconocimiento de todos los usuarios del sistema.



Izq – Izq: ES, EN, AS, ER, DE, AR, RA, RE, DA, SE, SA
Cen – Cen: UN, NT
Der – Der: LO, MO
Izq – Cen: UE, TA, TE, AN, ST, NA, ND
Cen – Der: NO, ON, TO
Izq – Der: LA, OS, CO, DO, OR, IE, AL, ME, MA, RO, EL, PA, SI, LE, AM

Figura 1. Distribución espacial de pares en el teclado.

Al analizar los pares con mayor número de ocurrencias, se evidenció que la gran mayoría de éstos se encontraban ubicados del lado izquierdo del teclado. Para que la distribución de los pares sobre el mismo fuese regular, además

del promedio ocupado en el grupo, se verificó la posición del par sobre el teclado, dividiendo el espacio ocupado por las teclas de letras en seis regiones: izquierda-izquierda, centro-centro, derecha-derecha, izquierda-centro, centro-derecha, izquierda-derecha (ver Figura 1).

Durante un análisis de factibilidad de reconocimiento de patrones de tecleo realizado previamente [AHS02], se trabajó con diecinueve pares de letras. En vista de que los primeros diecinueve pares en ese estudio no cubrían las tres regiones, se decidió aumentar progresivamente el número de pares hasta que las tres estuviesen cubiertas. De esta manera, el número de pares seleccionados para el desarrollo de la aplicación fue de cuarenta.

Los pares seleccionados para el estudio fueron los siguientes: ES, EN, UE, AS, ER, LA, DE, AR, TA, NO, RA, TE, AN, OS, CO, ST, DO, ON, OR, RE, IE, AL, ME, LO, MA, RO, EL, PA, TO, MO, UN, SI, DA, NA, SE, LE, ND, AM, SA y NT. En la Figura 1 se muestra la distribución de los pares sobre el teclado.

2 Técnica de Reconocimiento de Patrones utilizada en la Identificación de Usuarios

Una vez identificados los pares a utilizar, fue necesario determinar la técnica de reconocimiento de patrones que mejor resultado arrojara para el reconocimiento de patrones de tecleo. Las técnicas de reconocimiento seleccionadas para tal prueba fueron las siguientes: método estadístico basado en una distribución normal [6], mínima distancia [6], k-vecinos [5], perceptrón multicapa [7] y red de función de base radial [11]. Para ello, se realizaron un conjunto de pruebas con diferentes métodos, donde los datos utilizados fueron recolectados durante cuatro semanas a través del MSN Messenger y almacenados en un archivo de registro. Se analizaron un total de diecisiete archivos correspondientes a tiempos de tecleo de diecisiete usuarios distintos.

Para obtener unos resultados confiables, se realizaron un total de cinco pruebas con distintos datos del archivo de registro para cada uno de los métodos probados. Con los datos obtenidos de cada usuario, se formaron cinco particiones disjuntas. Para cada prueba, se combinaron cuatro particiones para entrenar el sistema y una para realizar el test de reconocimiento.

Los resultados arrojados por las pruebas realizadas en [2] mostraron que una red de base radial tiene un mejor desempeño que el resto de las técnicas de reconocimiento de patrones utilizadas. En lo que resta de este trabajo se mostrarán las pruebas realizadas sobre un reconocedor de patrones de tecleo que utiliza una red neuronal de base radial (RBF) para realizar el reconocimiento.

2.1 Red de Función de Base Radial (FBR)

Las redes de función de base radial (RBF) [11] se caracterizan por tener un entrenamiento híbrido, que incorpora aprendizaje supervisado y no supervisado. La arquitectura de este tipo de red es de tres capas: capa de entrada, capa oculta y capa de salida.

Las neuronas de la capa de entrada no realizan ningún tipo de procesamiento, simplemente envían los valores de entrada a la capa oculta. En la capa oculta se calcula la distancia que separa el vector de entrada de los centroides de esta capa, aplicándole luego una función gaussiana. En la capa de salida se realiza un procesamiento lineal.

El aprendizaje se realiza en dos etapas. Se entrena primero la capa oculta y luego la capa de salida. En la capa oculta se determinan los centroides y las desviaciones estándares para los vectores de entrada, mientras que en la capa de salida se determinan los valores de los pesos.

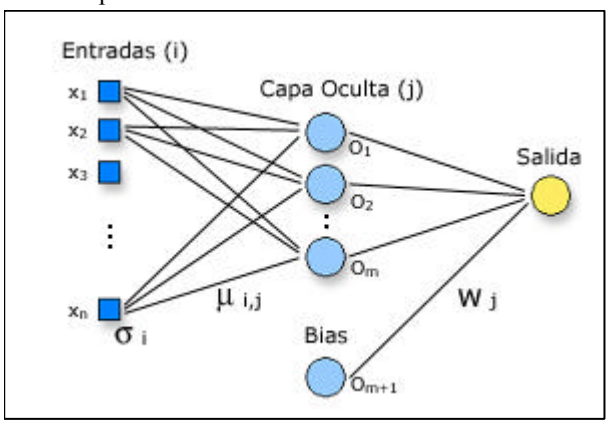


Figura 2. Arquitectura de una RBF

En la Figura 2 se puede observar la arquitectura de la red utilizada en el Módulo de Reconocimiento. Para el desarrollo del módulo, se determinaron tanto los centroides μ_{ij} por valor de entrada χ como número de neuronas existentes en la capa oculta, utilizando para ello el algoritmo de k-medias [9]. Luego, los valores para las desviaciones estándares de cada neurona i de la capa de entrada se calcularon como la mayor de las distancias existentes entre los centroides para esa neurona. Una vez encontrados estos valores, la segunda etapa consistió en hallar los valores para las conexiones entre la capa oculta y la capa de salida que permitieran una mayor

convergencia de la red.

2.2 Experimentos y Resultados

El primer experimento realizado para la evaluación de este método se basó en la verificación de usuarios, el cual indica, a partir de valores de entrada (tiempos de tecleo) y el identificador del usuario, si efectivamente se trata del usuario que se identificó. De esta manera, existe una plantilla de reconocimiento por cada individuo del grupo. Los valores usados para determinar las medias y las desviaciones estándar fueron los tiempos de tecleo por cada par que pertenecían al individuo al cual se le iba a construir la plantilla de reconocimiento.

El número de neuronas en la capa de entrada fue de cuarenta, correspondiente a los cuarenta pares de letras seleccionados. El vector de entrada contiene tiempos de tecleo para cada par seleccionado; se utilizaron entre 12 y 30 vectores de tiempo por cada usuario. La cantidad de neuronas utilizado para la capa oculta fue de veinticinco. Al tratarse de verificación de usuarios, en la capa de salida existe una única neurona cuya salida es igual a 1 para indicar que reconoció y 0 en caso contrario.

Se realizaron un total de cinco pruebas con conjuntos disjuntos de vectores de tiempo para el entrenamiento y el reconocimiento. En la Tabla 1 se presentan los resultados de la verificación de usuarios para este método, donde la columna **IND** indica el número del individuo en estudio, las columnas Prueba i identifican el número de la prueba, la columna A representa el nivel de aceptación (total de entradas reconocidas como pertenecientes al usuario IND entre el total de tiempos del usuario IND), las columna EFA y EFR exponen el error de falsa aceptación (cuando un usuario no autorizado es aceptado por el sistema) y el error de falso rechazo (cuando un usuario autorizado es rechazado por el sistema) respectivamente, mientras que la columna PA muestra el promedio del nivel de aceptación para el individuo IND.

IND	Prueba 1			Prueba 2			Prueba 3			Prueba 4			Prueba 5			PA
	A	EFA	EFR	A	EFA	EFR	A	EFA	EFR	A	EFA	EFR	A	EFA	EFR	
1	0,64	0,05	0,36	0,55	0,1	0,45	0,64	0,07	0,36	0,73	0,12	0,27	0,73	0,06	0,27	0,65
2	0,58	0,05	0,42	0,75	0,06	0,25	0,75	0,04	0,25	0,83	0,08	0,17	0,67	0,04	0,33	0,72
3	0,7	0,07	0,3	0,7	0,05	0,3	0,43	0,05	0,57	0,7	0,07	0,3	0,78	0,06	0,22	0,66
4	0,81	0,07	0,19	0,71	0,07	0,29	0,62	0,05	0,38	0,48	0,07	0,52	0,76	0,07	0,24	0,68
5	0,88	0,04	0,12	0,85	0,03	0,15	0,79	0,04	0,21	0,82	0,05	0,18	0,67	0,04	0,33	0,8
6	0,67	0,06	0,33	0,44	0,07	0,56	0,67	0,04	0,33	0,44	0,07	0,56	0,44	0,06	0,56	0,53
7	1	0,03	0	0,67	0,07	0,33	0,5	0,05	0,5	0,5	0,07	0,5	0,75	0,06	0,25	0,68
8	0,71	0,05	0,29	0,81	0,07	0,19	0,9	0,06	0,1	0,86	0,06	0,14	0,86	0,05	0,14	0,83
9	0,88	0,02	0,12	0,92	0,03	0,08	0,92	0,04	0,08	0,84	0,01	0,16	0,8	0,01	0,2	0,87
10	0,64	0,02	0,36	0,86	0,02	0,14	0,79	0,01	0,21	0,93	0,04	0,07	0,79	0,03	0,21	0,8
11	1	0,05	0	0,8	0,05	0,2	0,87	0,07	0,13	0,8	0,04	0,2	0,6	0,05	0,4	0,81
12	0,83	0,1	0,17	0,75	0,1	0,25	0,5	0,09	0,5	0,58	0,04	0,42	0,75	0,07	0,25	0,68
13	0,88	0,08	0,12	0,88	0,08	0,12	0,94	0,03	0,06	0,88	0,06	0,12	0,71	0,03	0,29	0,86
14	0,93	0,06	0,07	0,7	0,09	0,3	0,7	0,09	0,3	0,81	0,11	0,19	0,67	0,07	0,33	0,76
15	0,67	0,04	0,33	0,89	0,03	0,11	0,67	0,03	0,33	0,78	0,03	0,22	0,72	0,05	0,28	0,74
16	0,87	0,01	0,13	0,76	0,02	0,24	0,76	0,01	0,24	0,83	0,02	0,17	0,87	0,01	0,13	0,82
17	0,67	0,07	0,33	0,79	0,06	0,21	0,67	0,07	0,33	0,85	0,09	0,15	0,76	0,07	0,24	0,75
	0,79	0,05	0,21	0,75	0,06	0,25	0,71	0,05	0,29	0,74	0,06	0,26	0,72	0,05	0,28	0,74

Tabla 1. Resultados para el RBF con 25 neuronas

Los resultados obtenidos para esta prueba muestran que el porcentaje general de reconocimiento se encuentra alrededor del 74%, lo que significa que de cada 100 intentos de reconocimiento, aproximadamente 74 serán reconocidos. El nivel de aceptación para cada individuo del grupo de estudio está por encima del 65%, excepto para el individuo 6 que posee un valor de 53% de aceptación, sin embargo la cantidad de vectores utilizados para el entrenamiento de la red de este individuo fue el menor de todo el grupo.

También se observa que los valores obtenidos para el error de falsa aceptación (EFA) no supera el 6%, lo que muestra que es capaz de rechazar un individuo no autorizado el en 94% de las veces.

Otro de los experimentos realizados consistió en comprobar la capacidad del método para rechazar intrusos, determinando el error de falsa aceptación (EFA) para un grupo de cinco usuarios. Para cada individuo de la muestra, el experimento consistió en probar el nivel de rechazo de 13 vectores de tiempos, con la salvedad de que este procedimiento se realizó un total de 16 veces, una por cada usuario del grupo de estudio, excluyendo al individuo perteneciente la muestra. De esta manera, se realizó una correspondencia de los tiempos del individuo de la muestra con las plantillas de reconocimiento del resto de los usuarios del grupo.

En la siguiente tabla se muestra la cantidad de patrones reconocidos de los individuos en estudio, por los individuos

del entrenamiento.

	IND 3	IND 4	IND 6	IND 11	IND 12
1	0	0	0	0	0
2	0	0	2	0	0
3	*	3	4	2	3
4	2	*	2	0	0
5	0	0	0	0	0
6	0	4	*	0	2
7	0	0	0	4	0
8	0	0	0	0	0
9	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	*	0
12	0	3	2	0	*
13	0	0	0	0	0
14	0	7	5	0	3
15	0	1	1	1	0
16	0	3	3	0	0
17	6	0	1	0	0
EFA	0,0362	0,0950	0,0905	0,0317	0,0498

Tabla 2. Resultados del experimento 2

Como se puede observar en la Tabla 2, el porcentaje de falsa aceptación se encuentra alrededor del 5%, lo que indica que el método seleccionado es capaz de rechazar, con un 95% de efectividad, un intruso dentro del conjunto de entrenamiento.

El último experimento consistió en evaluar el desempeño del método al suministrar información incompleta a las plantillas de verificación, completándolas con las medias obtenidas en el entrenamiento para cada par, determinando el nivel de aceptación y el error de falso rechazo. Este experimento mide la variación entre el uso de patrones completos de usuarios y el uso de información histórica para el reconocimiento.

La muestra y los tiempos de tecleo utilizados para este experimento fueron los mismos que los del experimento anterior. Para crear el vector de tiempo de los 40 pares seleccionados, los tiempos registrados se tomaron en el orden en que fueron tecleados hasta completar 35 pares. El resto fue completado con los valores de las medias. Una vez construido el vector, era presentado a la red del individuo correspondiente para su reconocimiento. Luego, se presentó el mismo vector con las mismas características, completando los valores de las medias faltantes con valores reales del individuo.

En la tabla siguiente se muestra la relación de los resultados obtenidos al completar los valores de entrada del vector de verificación contra los vectores completados por valores de entrada del usuario.

	IND3	IND4	IND6	IND11	IND12	TOTAL	%
Número de plantillas completadas	209	170	119	187	153	838	
Reconocimiento de la plantilla completada igual al reconocimiento de la plantilla final	208	163	119	186	152	828	98,8
Reconocimiento de la plantilla completada diferente reconocimiento de la plantilla final	1	7	0	1	1	10	1,2

Tabla 3. Resultados del Experimento 4

Los resultados arrojados por este experimento muestran que para la cantidad de medias calculadas por individuo durante el reconocimiento, cinco en este caso, existe una variación en el reconocimiento del 1,2%, es decir, en el 98,8% de las veces el resultado del reconocimiento es igual completando el vector de tiempos que no haciéndolo. De esta manera, se puede utilizar este método para calcular la verificación de un individuo sin necesidad de tener el vector de reconocimiento completo utilizando información histórica del individuo al momento del entrenamiento.

3 Conclusiones

Para un escenario donde los tiempos registrados pertenecen a una aplicación de mensajería instantánea por Internet, específicamente a los cuarenta pares de letras con mayor número de ocurrencias para esa aplicación, en una muestra de diecisiete individuos, se determinó que una red neuronal basada en Funciones de Base Radial puede reconocer efectivamente a un individuo por sus características de escritura al utilizar el teclado.

El promedio de reconocimiento para un individuo fue de 74%, lo que significa que de cada 100 intentos, 74 resultarán exitosos y 26 resultarán fallidos, siendo este último el error de falso rechazo (EFR), es decir, que el 26% de las veces el individuo en cuestión será rechazado. Por otra parte, se tiene que al tratar de reconocer a un individuo con las características de tecleo pertenecientes a otro individuo de la muestra, el error de falsa aceptación (EFA) es de 5%, es decir, de cada 100 intentos, el individuo no será reconocido en 95 ocasiones.

Por otra parte, al realizar las pruebas para cada uno de los individuos, se observó que durante la etapa de entrenamiento para todos los métodos probados, el error de entrenamiento para un individuo tiende a disminuir a medida que aumenta la cantidad de información de tecleo de éste. Esto incide en la calidad del reconocimiento para cada individuo.

Los resultados obtenidos para verificar el nivel de rechazo indican que la probabilidad de reconocimiento al adicionar un individuo ajeno a la muestra es baja, pero superior al error de falso rechazo de los individuos del grupo de estudio. Esto permite observar que existe una separación de las características de los individuos de la muestra y que un individuo ajeno al estudio puede llegar a ser reconocido. En consecuencia, el método mantiene su efectividad en un entorno cerrado de individuos. Sin embargo, se pueden agregar nuevos individuos sin mayor problema agregando una nueva plantilla de reconocimiento, la cual se obtiene luego de un entrenamiento con datos del nuevo individuo.

En el último de los experimentos descritos, se pudo observar que cuando ya se tenían los valores para 35 pares de los 40 necesarios para el reconocimiento, los resultados eran muy similares a los obtenidos luego de esperar que los 40 pares fuesen completados. La diferencia era de aproximadamente un ±1.2%, por lo que se puede utilizar información histórica para completar el vector de tiempos durante el reconocimiento.

En resumen, el módulo de reconocimiento de patrones de tecleo desarrollado resulta ser una alternativa práctica, confiable y de bajo costo para la verificación de usuarios. Adicionalmente, por su característica modular (es un objeto COM) puede ser reutilizado entre diversas aplicaciones que generen eventos de teclado y requieran algún mecanismo de identificación basado en este tipo de información biométrica.

A nivel comercial, existen muy pocas aplicaciones basadas en este tipo de tecnología. Entre los productos comerciales disponibles en el mercado se destaca BioPassword de BioNet Systems [4] utilizado básicamente para reconocimiento de *passwords.* La mayoría de productos catalogados en esta categoría están basados en la captura y clasificación de información obtenida mediante teclado, pero no reconocimiento biométrico.

Referencias

[1] Daniel Acevedo y Glemarys Hernández. Desarrollo de un módulo de identificación de usuarios basado en reconocimiento de patrones de tecleo. Trabajo Especial de Grado. Escuela de Computación. Facultad de Ciencias. Universidad Central de Venezuela. Mayo 2003.

[2] Daniel Acevedo y Glemarys Hernández. *Técnicas de reconocimiento de patrones y redes neuronales artificiales (RNAs)*. Seminario de Investigación. Escuela de Computación. Facultad de Ciencias. Universidad Central de Venezuela. Octubre 2002.

[3] AIMC (Asociación para la Investigación de Medios de Comunicación). *Navegantes en la Red: Quinta encuesta AIMC a usuarios de Internet*. España: Enero, 2003. http://www.aimc.es

[4] Bionet System LLC. *Biopassword Keystroke Dinamics*. Technical Report. 2002. http://biopassword.com

[5] T.M.Cover and P.E.Hart. *Nearest Neighbor Pattern Classi?cation*. Trans.IEEE Inform.Theory, IT-13, pp21-27. 1967.

[6] K.Fukunaga. *Introduction to Statistical Pattern Recognition*. Academic Press, Inc. 1990.

[7] J. Hertz, A. Krogh y R.G. Palmer. *Introduction to the Theory of Neural Computation*. Addison-Wesley. 1991.

[8] Federico Kuhlmann y Antonio Alonso Concheiro. *Información y Telecomunicaciones*. Fondo de cultura Economica. México, 1997. http://www.cft.gob.mx/html/la_era/info_tel/it0.html

[9] J.B. MacQueen. *Some methods for classification and analysis of multivariate observations.* In Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability. Volume I, Statistics. University of California Press. 1967.

[10] MSDN Developer Center. http://msdn.microsoft.com

[11] Mark J.L. Orr. *Introduction to Radial Basis Function Networks.* Centre for Cognitive Science. University of Edimburgh. Scotland. April 1996. http://www.anc.ed.ac.uk/~mjo/papers/intro.ps.gz