Año: 2021 Volumen: 1
Número 7, ISSN: 2448-623X

Autenticación por patrón de movimientos de mano para acceso a un laboratorio

J. I. Vega-Luna[1], M. A. Lagos-Acosta[1], G. Salgado-Guzmán[1], J. F. Cosme-Aceves[1], V. N. Tapia-Vargas[1]

***Resumen*—El objetivo del trabajo es realizar un sistema de autenticación, utilizando patrones de movimientos de la mano para autenticar acceso a un laboratorio de investigación. Con un arreglo de dos sensores gestuales PAC7620 conectados por I2C a un sistema embebido Raspberry pi, se realizó una muestra durante 3 segundos, de los patrones de movimiento dentro de un área de 30 cm por 30 cm y 30 cm de profundidad. El patrón de movimientos es leído con los sensores PAC7620 y se procesa la información, de tal forma que se compare con una base de datos previamente almacenada. El resultado de la comparación resultara la autenticación del usuario para permitir un acceso. El algoritmo se programó en Python con tres diferentes módulos principales: como la captura de usuarios, ajuste de sensores y funcionamiento de la autenticación. El hardware utilizado es un kit embebido de Raspberry, dos sensores, un display LCD y teclado numérico. Las pruebas realizadas fueron capturar los patrones de 20 usuarios y replicar la simulación de intento de autenticación con cien repeticiones por usuario. Se repitió la prueba capturando patrones de 5 segundos. Los resultados obtenidos fueron en promedio 93 % de autenticaciones válidas. La colaboración de este sistema es la falta de contacto para poder autenticar y con esto se puede tener un acceso más higiénico, el patrón de uso puede asemejarse a los que utilizan los usuarios en un smartphone. Es un sistema funcional para donde es necesaria una higiene estricta.**

***Palabras claves*—Autenticación, control de acceso, PAC7620, sensor gestual, Raspberry PI.**

***Abstract*—The objective of the work is to carry out an authentication system, using patterns of hand movements to authenticate access to a research laboratory. Using an array of two PAC7620 gesture sensors connected by I2C to a Raspberry pi embedded system, movement patterns were sampled for 3 seconds within a 30 cm by 30 cm and 30 cm depth area. The movement pattern is read with the PAC7620 sensors and the information is processed in such a way that it is compared with a previously stored database. The result of the comparison will be the authentication of the user to allow access. The algorithm was programmed in Python with three different main modules: such as user capture, sensor tuning, and authentication operation. The hardware used is a Raspberry embedded kit, two sensors, an LCD display and a numeric keypad. The tests carried out were to capture the patterns of 20 users and replicate the authentication attempt simulation with one hundred repetitions per user. The test was repeated capturing 5 second patterns. The results obtained were on average 93% valid authentications. The collaboration of this system is the lack of contact to be able to authenticate and with this it is possible to have a more hygienic access, the pattern of use can be like those used by users on a smartphone. It is a functional system where strict hygiene is necessary.**

***Keywords*—Autentication, access control, PAC7620, gestual sensor, Raspberry PI.**

I. Introducción

Los sistemas de autenticación para control de acceso en áreas restringidas son cada vez más comunes, y específicamente en para lugares donde se tiene tecnología que requiere confidencialidad. En este último año de pandemia COVID-19, el requisito de sanidad nos hizo recapacitar en estos conceptos de privacidad de la información referente a resultados de laboratorios, el desarrollo de nuevas vacunas y la seguridad de acceso en áreas con posible contaminación. Los laboratorios cuentan con mayores restricciones en cuanto a seguridad física de los que ahí laboran, ya que el uso de trajes especiales que cubren la mayor parte del cuerpo hace casi imposible a un usuario realizar una autentificación por medios biométricos. Las tecnologías de autenticación biométrica como reconocimiento facial, reconocimiento de iris, reconocimiento de huellas dactilares / palmares, reconocimiento de voz y autenticación acústica del oído, como son las mejores en su tipo, proporcionando las soluciones más adecuadas a las necesidades de los usuarios. Además, al combinar múltiples sistemas de autenticación biométrica, las soluciones brindan una seguridad aún más sólida, como se muestran algunos métodos en la Figura 1.

Los factores de autenticación aplicados en seres humanos se clasifican generalmente en los tipos siguientes: Algo que la persona “es”, algo que la persona “tiene”, algo que la persona “sabe” y algo que la persona “hace”. Uno de los métodos de autenticación que los usuarios consideran más seguro es el biométrico con la huella dactilar [1]. La combinación de varios de estos factores hace más robusta la autenticación, pero no siempre se puede tener el conjunto de

* vlji@azc.uam.mx.

[1]*Universidad Autónoma Metropolitana-Azcapotzalco, Departamento de Electrónica, Área de Sistemas Digitales, Av. San Pablo 180, Colonia Reynosa, C.P. 02200, Ciudad de México, México.*

varios factores ya que la puede hacer más compleja para los usuarios.

Figura 1. Medios de autenticación biométrica

Los métodos de acceso a lugares restringidos, a través de un método de identificación, han sido un tema de preocupación desde que fue necesario el resguardo de tecnología de punta. [2]. No es un asunto de poca importancia tomando en cuenta que en los últimos siete años han sido robados 112,000 millones de dólares mediante fraudes relacionados con la usurpación de la identidad digital, según un informe de IBM. Es por eso que, la industria no cesa en su empeño de buscar herramientas cada vez más seguras, cómodas y de bajo costo que aseguren que los usuarios son quienes dicen ser. Considerando que cada vez se llevan a cabo más operaciones delicadas en línea, es imperativo superar el sistema de usuario y contraseña usado durante décadas el cual presenta grandes deficiencias.

Los diversos métodos de autenticación para control de acceso no siempre son lo más accesible, ya que existen áreas restringida como en los laboratorios dedicados [3] al desarrollo y uso de alta tecnología, en los que es necesario algún otro resguardo físico como lo son: cubre bocas, caretas protectoras, trajes que cubren todo el cuerpo, guantes especiales, etc. En la Figura 2 se muestran algunos productos para protección física.

Los métodos de protección física limitan los tipos de autenticación o simplemente los hacen más complejos, si se requiere autenticar con iris, es algo muy difícil cuando se tiene una careta, si se requiere autenticar por rostro no cualquier algoritmo lo realiza si se tiene puesto un cubrebocas, si se requiere autenticar por huella digital o la palma de la mano, será algo complejo con un guante que no se debe quitar por contaminación [4]. La autenticación que usan medios sin contacto del tipo biométricos, son limitadas en tareas donde se tienen limitantes físicas, aquí es donde se utiliza los factores de autenticación algo que la persona "sabe" y algo que la persona "hace", el realizar un movimiento especifico por la persona es algo que también sirve como medio de autenticación.

Figura 2. Accesorios para protección física

Los sistemas de autenticación usados para acceder a instalaciones se basan típicamente en la utilización de tarjetas de identidad, tarjetas inteligentes o métodos biométricos. Actualmente, los métodos de autenticación más comunes se basan en texto o palabras clave y no ha sido posible crear palabras clave de fácil uso y robustas. Las investigaciones realizadas al respecto han explorado técnicas que no usan palabras claves [5] y hace uso de métodos de autenticación para acceso a la nube basado en Lenguaje de Marcado para Confirmaciones de Seguridad (SAML-Security Assertion Markup Language) [6] o en códigos QR de dos niveles, uno público y el otro privado, el nivel público funciona como los códigos QR clásicos para almacenar información y el nivel privado usa patrones de textura para almacenar información codificada [7]. Otros métodos de autenticación usan palabras clave graficas (GAU-Graphical User Authentication), creados combinando dos imágenes cuyo principio de funcionamiento es que las personas recuerdan más objetos visuales que textos [8] o utilizando memorias SD y tarjetas de encriptación.

El módulo PAC7620 de la marca PixArt Imaging Inc, integra la función de reconocimiento de gestos usando una interconexión con la interfaz I2C en un solo chip y realiza un procesamiento de imágenes que forma un sistema de sensor analítico [9]. Puede reconocer 9 gesticulaciones de manos humanas como moverse hacia arriba, hacia abajo, izquierda, derecha, hacia adelante, hacia atrás, en sentido circular en el sentido de las agujas del reloj. También es posible consultar varios valores como el tamaño del objeto, el brillo y la posición, así como la salida de los datos sin procesar. La

innovación basada en la visión del reconocimiento de gestos de la mano es una pieza esencial de la comunicación humano-PC. En las últimas décadas, el teclado y el ratón asumen un trabajo notable en la comunicación humano-PC [10]. No obstante, atribuible a la rápida mejora de los equipos y la programación, se han requerido nuevos tipos de estrategias de comunicación humano-PC. Específicamente, los avances, por ejemplo, el reconocimiento del discurso y el reconocimiento de gestos reciben una consideración extraordinaria en el campo de la comunicación humano-PC.

El gesto es una imagen de conducta física, incorpora gesto corporal y gesto de la mano. Se divide en dos clasificaciones: gesto estático y gesto dinámico [11]. Para lo anterior, la postura del cuerpo o el gesto de la mano significa un signo. Para lo último mencionado, el desarrollo del cuerpo o la mano transmite algunos mensajes. El gesto se puede utilizar como un dispositivo de correspondencia entre PC y humanos. En gran medida, no es lo mismo que las técnicas habituales basadas en equipos y puede lograr la colaboración entre humanos y PC a través del reconocimiento de gestos. El reconocimiento de gestos decide el propósito de la persona a través del reconocimiento del gesto o el desarrollo del cuerpo o partes del cuerpo. En las décadas anteriores, numerosos especialistas se han esforzado por mejorar la innovación en el reconocimiento de gestos con las manos. El reconocimiento de gestos con las manos tiene un aliciente extraordinario en numerosas aplicaciones, por ejemplo, la comunicación a través del reconocimiento de gestos [12], la realidad ampliada (realidad generada por computadora), los traductores de comunicación basados en gestos para discapacitados y el control de robots.

II. Parte Técnica del Artículo

En la realización de este trabajo la metodología seguida fue dividir el diseño en cuatro bloques modulares como se muestra en la Figura 3. Las etapas son las siguientes: Control maestro RBPI, Arreglo de sensores, la pantalla LCD y el teclado numérico.

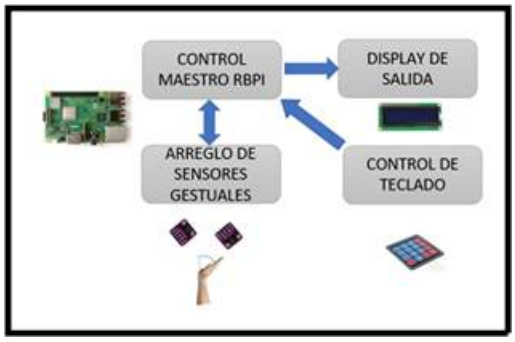

Figura 3. Bloques que integran el sistema

A. Control maestro

Para realizar este módulo se utilizó una tarjeta Raspberry Pi 3 con la imagen de sistema operativo Raspbian en una tarjeta de memoria SD. Posteriormente, se conectaron los siguientes dispositivos periféricos a la tarjeta Raspberry: el teclado, el ratón y el monitor HDMI. A continuación, se actualizaron los parches y herramientas de red ejecutando desde una sesión de terminal los comandos *apt-get update* y *apt-get upgrade*.

En la puesta a punto fue importante no arrancar servicios de red innecesarios, ya que esto podría causar explotación de alguna vulnerabilidad e intrusión por esta causa. El único servicio arrancado con fines administrativos fue *ssh* para poder acceder al sistema embebido y configurar la tarjeta utilizando una sesión de terminal remota. Los parámetros de red: dirección IP, máscara y puerta de enlace, se establecen de acuerdo a la red donde este sistema sea instalado. El siguiente paso consistió en la descarga de la distribución del lenguaje de programación Python usada para desarrollar las interfaces con los clientes del teclado.

En este módulo de control maestro se controlan las etapas de mantenimiento, la primera opción de alta /baja de usuarios y análisis de movimientos. En el mantenimiento se realiza el ajuste de las señales que nos dan los sensores, realizando movimientos específicos solicitados por el sistema (sube mano), se confirma que el sistema esta ajustado adecuadamente con la información que muestra en el display. La opción 2 de alta de usuarios se refiere a la grabación durante 3 segundos de los movimientos generados por la mano de la persona para caracterizar el movimiento, haciendo varias repeticiones para que se tenga el menor error, el usuario se dará de alta asignándole un número y a continuación se solicita el realizar el movimiento dentro del área especificada, para que así se grabe el movimiento del usuario.

También se pueden dar de baja usuarios atendiendo a las diferentes opciones del menú mostrado en el display. En la tercera opción del menú de selección con el teclado, se inicia el proceso de identificación del gesto o movimiento de la mano durante 3 segundos. Al aproximar la mano al área donde se censa el movimiento el sistema inicia la captura de los movimientos y realiza una captura de los diferentes movimientos realizados usando la información de los dos sensores, para que con esto se tenga una mayor precisión, como resultado a esta serie de movimientos nos muestra el resultado en el display con el numero asignado al usuario (usuario valido o usuario NO validado). En la Tabla I se muestran los diferentes gestos que se pueden sensar y en la Figura 4 el área de reconocimiento del movimiento de la mano.

TABLA I
TABLA DE IDENTIFICACIÓN DE GESTOS

Gestos identificados por el sensor PAC7620		
Código	función	Significado
0	UP	movimiento de la mano hacia arriba
1	DOWN	movimiento de la mano hacia abajo
2	LEFT	movimiento de la mano hacia la izquierda
3	DERECHA	movimiento de la mano hacia la derecha
4	CLOCKWISE	movimiento de la mano girando en sentido de las manecillas
5	COUNTER-CLOCKWISE	movimiento de la mano girando en sentido contrario a las manecillas
6	PUSH FORWARD	movimiento de la mano hacia el frente
7	PULL AWAY	movimiento de la mano hacia atrás
8	HAND WAVE	movimiento de la mano en ondas

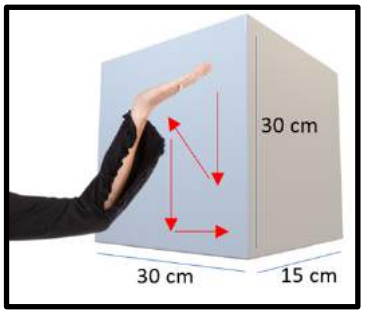

Figura 4. Área de reconocimiento de movimiento de mano

En el momento en el que se registraron los movimientos del usuario, se registraron los códigos de movimientos durante los 3 segundos que duró la grabación del patrón del usuario. Como se muestra en la Tabla II.

TABLA II
TABLA DE IDENTIFICACIÓN DE GESTOS

Base de datos de usuarios registrados		
Usuario	nombre	Registro de patrones
0	Maria	8,2,3,1,2
1	Pedro	0,1,3,4,6,1,0
2	Luisa	7,6,7,6,5
3	Raúl	4,3,2,3,1,0

En el momento en el que la cadena que se está sensando es igual a una de las cadenas de identificación de la tabla se toma como usuario autenticado y lo muestra en el display.

B. Arreglo de sensores

Este bloque se encarga de enviar la información de los gestos identificados por un par de sensores PAC7620. Los sensores están ubicados en el centro del área que virtualmente se visualiza como en el fondo de un cubo, uno está en posición angular de 90° girado con respecto al otro.

El propósito de utilizar los dos sensores es que con esto tendremos mayor precisión en los movimientos registrados. En el momento que el sensor uno indica que hubo movimiento a la derecha el otro sensará que fue hacia arriba, si es así entonces se procesa la información y se valida como un movimiento identificado correctamente. En el plano x y será de la misma manera, en Z serán los mismos movimientos identificados en los dos sensores como se muestra en la Figura 5.

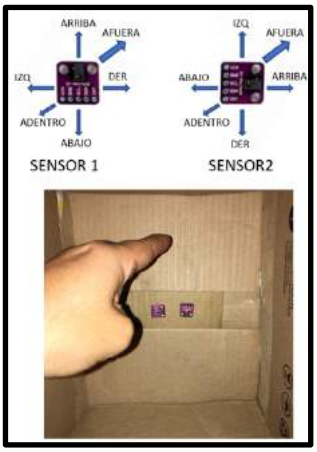

Figura 5. Posición de arreglo de sensores y movimiento de mano

C. Control de teclado

El bloque control del teclado se encarga de seleccionar las diferentes funciones como se había mencionado: etapas de mantenimiento, alta/baja de usuarios y análisis de movimientos. Al iniciar la ejecución del código ´por medio del teclado y el display, se lleva a cabo la selección según describe las opciones en el display.

III. RESULTADOS

Se realizaron las pruebas indicadas a continuación para poder concluir el funcionamiento del sistema. Se tomó un grupo de diez usuarios cuyo patrón de movimiento fue dado de alta previamente en el sistema. Se les solicitó realizar el patrón de movimiento uno a uno con pausas de cinco segundos por diez usuarios y el resultado de las veces que se autenticó el movimiento se sumó por cada muestra. Se graficó la cantidad de aciertos para los diez usuarios por muestra y se promedió el número de aciertos como se muestra la Figura 6.

El promedio de aciertos obtenido fue 93%. Las condiciones en las que se realizaron los muestreos fueron utilizando movimientos de mano en adultos sin accesorios en los dedos, como anillos. Dos de los diez usuarios utilizaron guantes de látex de color negro, los cuales fueron los que

menos aciertos tuvieron al muestrear. Se realizaron pruebas con los mismos usuarios y condiciones, pero utilizando un solo sensor lo cual registro solo 81% de aciertos.

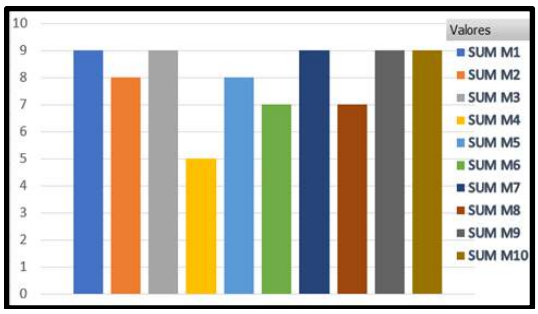

Figura 6. Gráfica de aciertos al muestrear (M#) realizadas a diez usuarios diez ocasiones a cada uno

IV. DISCUSIÓN, CONCLUSIÓN Y RECOMENDACIONES

El resultado de este trabajo fue un sistema de autenticación diferente a los convencionales, con diversas adecuaciones a realizar según el medio donde se utilizará. Algunos de los usuarios al registrar sus patrones en los tres segundos, llegaron a tener entre 5 y 7 diferentes movimientos. Los usuarios que registraron movimientos más rápidos fueron los que tuvieron más falsos positivos durante la autenticación que los que obtenían menos. Al utilizar mayor cantidad de sensores en diferentes posiciones radiales, fue mayor la precisión en los resultados de las capturas de los movimientos. Tan solo de utilizar un sensor a utilizar dos, aumento la precisión en 12%.

Para evitar fallos a nivel usuario, se recomienda llevar a cabo los movimientos más pausados y menos complicados, para que sean más fácil de realizar y recordar. El utilizar accesorios en las manos representó dificultad en la lectura de los movimientos, lo cual es provocado por la diferencia entre la luz que se refleja en la mano en el momento de ser captada.

V. REFERENCIAS

[1] Mittra, P. y Rakesh, N (2016). "A desktop application of QR code for data security and authentication", in Procedings International Conference on Inventive Computation Technologies (ICICT), pp. 1-5.

[2] Lin, Z., Jiang, Z., Davis, L.S.: Recognizing actions by shape-motion prototype trees. In: 2009 IEEE 12th International Conference on Computer Vision. pp. 444-451 (Sept 2009). https://doi.org/10.1109/ICCV.2009.5459184

[3] Zhou, L.; Varadharajan, V. y Hitchens, M. (2015). "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage", *IEEE Transactions on Information Forensics and Security*, Vol. 10, Issue: 11, pp. 2381-2395.

[4] Kaczmarek, T.; Ozturk, E. y Tsudik, G. (2018). "Thermanator: Thermal Residue-Based Post Factum Attacks On Keyboard Password Entry", disponible en: https://arxiv.org/abs/1806.10189.

[5] Ying Wu and Thomas S Huang. Vision-based gesture recognition: A review. In International Gesture Workshop, pages 103–115. Springer, 1999.

[6] Jing, D.; Yan, J. y Fujiang, A. (2018). "An Improved Uniform Identity Authentication Method Based on SAML in Cloud Environment", *in Procedings IEEE Third International Conference on Data Science in Cyberspace (DSC)*, pp. 533-536.

[7] Tkachenko, Y.; Puech, W. y Destruel, C. (2016). "Two-Level QR Code for Private Message Sharing and Document Authentication", *IEEE Transactions on Information Forensics and Security*, Vol. 11, Issue: 3, pp. 571-583.

[8] Bilgi, B. y Tugrul, B. (2018). "A Shoulder-Surfing Resistant Graphical Authentication Method", *in Procedings International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1-4.

[9] M. Asadi-Aghbolaghi, A. Clap´es, M. Bellantonio, H. J. Escalante, V. Ponce-L´opez, X. Bar´o, I. Guyon, S. Kasaei, and S. Escalera. A survey on deep learning based approaches for action and gesture recognition in image sequences. In 2017 12th IEEE International Conference on Automatic Face Gesture Recognition (FG 2017), pages 476–483, 2017

[10] Matsuo, K.; Kanai, A. y Hatashima, T. (2018), "Dynamic Authentication Method Dependent on Surrounding Environment", *in Procedings IEEE 7th Global Conference on Consumer Electronics (GCCE)*, pp. 855-857.

[11] Zhou, P.; Xiao, M. y Xia, Z. (2015). "A Message Authentication Method for Wireless Sensor Networks Using Polynomial Interpolation", *in Procedings 2nd International Symposium on Dependable Computing and Internet of Things (DCIT)*, pp. 151-153.

[12] Fuzi, Mohd Faris Mohd, et al., "HOME FADS: A dedicated fire alert detection system using ZigBee wireless network," in Proceedings of Control and System Graduate Research Colloquium (ICSGRC), 2014.

VI. BIOGRAFÍA

Vega-Luna José Ignacio. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1985. Maestría en Ciencias de la Computación, UAM-Azcapotzalco, Cd. de México, 1990. Labora actualmente en el área de Sistemas Digitales del Departamento de electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores y sistemas operativos. El M. en C. Vega realiza investigación con redes inalámbricas de sensores y actuadores.

Lagos-Acosta Mario Alberto. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1992. Labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores y redes de computadoras. El Ing. Lagos realiza investigación con redes de computadoras.

Salgado-Guzmán Gerardo. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1992. Labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores y sistemas operativos. El Ing. Salgado realiza investigación con redes inalámbricas de sensores y actuadores.

Cosme-Aceves José Francisco. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1985. Labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Su línea de trabajo es lenguajes de descripción de hardware. El Ing. Cosme realiza investigación con sistemas embebidos y seguridad en redes de computadoras.

Tapia-Vargas Víctor Noé. Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1987. Maestría en Ciencias de la Computación, UAM-Azcapotzalco, Cd. de México, 1999. Labora actualmente en el Departamento de Electrónica de la UAM-Azcapotzalco. Sus líneas de trabajo son: aplicaciones de microprocesadores y microcontroladores, robótica e IoT.