Año: 2020 Volumen: 1
Número 6, ISSN: 2448-623X

# SISTEMA DE AUTENTICACIÓN BASADO EN BOTONES MULTICOLORES

J. I. Vega-Luna[1], M. A. Lagos-Acosta[1], G. Salgado-Guzmán[1], J. F. Cosme-Aceves[1], F. J. Sánchez-Rangel[1], L. López-Aparicio[2], V. N. Tapia-Vargas[1].

***Resumen*—Se presenta un sistema de autenticación basado en botones multicolores. El sistema se compone de un arreglo matricial de teclas de 3x3. Cada tecla tiene asociado un led RGB. El control de la matriz se realiza con un microcontrolador Arduino Mega 2560 y el procesamiento de la información y cifrado es a través de una tarjeta Raspberry Pi. El sistema genera combinaciones aleatorias de colores, distintas para cada tecla, de forma tal que el usuario debe presionar la secuencia de teclas de colores preestablecida y personalizada como su autenticación para usar un dispositivo o entrar a una instalación. Para autenticarse, el usuario debe suministrar en tiempo y forma la secuencia preestablecida. Los resultados de las pruebas indicaron que las autenticaciones acertadas fueron 95%, el tiempo promedio para suministrar las cuatro combinaciones fue 4.2 segundos y la secuencia de colores a recordar con más eficiencia fue de cuatro colores.**

***Palabras claves*— Arduino, autenticación, botones multicolores, led RGB, Raspberry Pi.**

***Abstract*—This paper presents an authentication system based on multicolored buttons. The system consists of a 3x3 key matrix array. Each key has an RGB LED associated. The control of the matrix is carried out with an Arduino Mega 2560 microcontroller and the processing of the information and encryption is through a Raspberry Pi card. The system generates random combinations of colors, different for each key, so that the user must press the sequence of preset and customized color keys as their authentication to use a device or enter an installation. To authenticate, the user must provide the preset sequence in a timely manner. Test results indicated that successful authentications were 95%, the average time to type the four combinations was 4.2 seconds and the sequence of colors to remember more efficiently was four colors.**

***Keywords*— Arduino, authentication, multicolored buttons, Raspberry Pi, RGB led.**

## I. . INTRODUCCIÓN

Los sistemas de autenticación de usuarios son cada vez más importantes en las nuevas tecnologías digitales de acceso a áreas restringidas, validación en cajeros automáticos y acceso a información en equipos de cómputo, entre otros usos. Los sistemas más comúnmente usados validan la autenticación de usuarios empleando una clave numérica compuesta de cuatro a ocho dígitos. Los sistemas de autenticación que ocupan más de ocho dígitos son inviables e imprácticos por la dificultad de recordar cadenas numéricas grandes.

Un sistema digital para proporcionar acceso y uso de recursos a personas autorizadas debe detectar y excluir las no autorizadas. El acceso es controlado usando un procedimiento de autentificación para establecer con cierto grado de confianza la identidad del usuario y conceder privilegios y acceso autorizado a recursos e instalaciones.

Para intentar determinar la identidad de un individuo, se aplica una o varias pruebas declaradas previamente, las cuales deben cumplirse para autorizar el acceso o uso de recursos. Los factores de autenticación aplicados en seres humanos se clasifican generalmente en los tipos siguientes: 1) Algo que el usuario “es”, 2) Algo que el usuario “tiene”; 3) Algo que el usuario “sabe”; 4) Algo que el usuario “hace”; 5) Autenticación mediante dos factores "algo que el usuario tiene", más "algo que sabe", y 6) Autenticación de triple factor, compuesta por "algo que el usuario tiene", más "algo que sabe", más "quién es". Uno de los métodos de autenticación que los usuarios consideran más seguro es el biométrico con la huella dactilar [1].

Los métodos de acceso a servicios digitales a través de un proceso de identificación han sido un tema de preocupación desde que el inicio de la Internet [2]. No es un asunto de poca importancia tomando en cuenta que en los últimos seis 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.

Un estudio realizado por investigadores de la Universidad de California reveló hasta qué punto un atacante puede aprovechar el entorno para obtener contraseñas sin necesidad de malware. Los investigadores descubrieron que es posible detectar las teclas presionadas usando el calor corporal dejado en ellas, incluso siguiendo

[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.*
[2] *Estudiante de Doctorado en Ciencias Biomédicas. Facultad de Medicina de la Universidad Autónoma de Coahuila, Unidad Torreón, Torreón, Coah., México.*
* vlji@azc.uam.mx.

Año: 2020 Volumen: 1
Número 6, ISSN: 2448-623X

las recomendaciones de seguridad. Sólo es necesario que el atacante use una cámara térmica para mostrar iluminadas las teclas usadas como se muestra en la Figura 1. El estudio determinó que usando una cámara de rango medio se puede determinar las teclas pulsadas en un teclado normal, hasta un minuto después de haberlas presionado, ya que el plástico de las teclas retiene el calor corporal suficiente para distinguirlas durante ese tiempo.

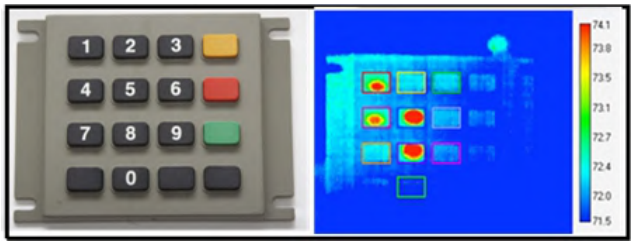


Figura 1. Marcas térmicas en teclado numérico

Comúnmente, los usuarios realizan la autenticación y se retiran momentáneamente del equipo o sistema de acceso, tiempo suficiente para que alguien pase por delante del sistema con una cámara térmica y registre las teclas que han sido pulsadas al iniciar una sesión. Con esta información se puede acceder al sistema, sobre todo si es una contraseña corta, como por ejemplo un PIN bancario de cuatro dígitos o un código de verificación [3]. No hace falta ser un experto para lograrlo, causando que el ataque sea más peligroso.

Los ataques denominados Thermanator, así llamados porque usan un termógrafo, son realizados por un adversario interno que registra a los usuarios a través de los residuos térmicos dejados al suministrar la contraseña. El objetivo es aprender la contraseña de la víctima utilizando una cámara térmica. El atacante cuenta con un minuto para grabar el teclado antes que los residuos térmicos se disipen. No se necesita presencia de la víctima descuidada, ya que la grabación de la imagen se realiza después que se retira. No es necesario ningún conocimiento previo de la víctima para analizar las imágenes térmicas, aunque ayuda el uso de contraseñas inseguras.

Los sistemas de autenticación usados para acceder a instalaciones se basan típicamente en la utilización de tarjetas de identidad, tarjetas inteligentes o métodos biométricos. Las investigaciones realizadas al respecto han explorado técnicas que no usan palabras claves [4] 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) [5] 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 [6]. 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 [7] o utilizando memorias SD y tarjetas de encriptación [8].

Los algoritmos de criptografía actuales necesitan mejorar la seguridad de las claves intercambiadas en la transferencia de información. El uso de estos algoritmos incrementa el costo de los sistemas y tiempo de procesamiento. Sin embargo, son importantes ya que tratan de evitar el robo de información. Desafortunadamente, la criptografía puede lograr confidencialidad, pero no integridad, de tal forma que los últimos años las investigaciones se han enfocado también en: la autenticación de la transmisión de datos en teléfonos inteligentes [9], redes inalámbricas de sensores usando interpolación polinomial [10], métodos para detectar plagio de código de programas sin intervención humana [11], encriptamiento de la información en cajeros automáticos, o ATM, usando códigos QR [12], prevención de fraudes para transacciones bancarias en línea usando criptografía visual extendida y códigos QR [13], detección de robo de información confidencial, o Phishing, usando comparación de código fuente HTML y similitud del coseno [14], cifrado de información basado en etiquetas de longitud de autenticación usando códigos Reed-Solomon [15] y mantener la confidencialidad e integridad de la información transmitida usando un canal que utiliza el algoritmo AES (Advanced Encryption Standard) y códigos de autenticación de mensajes Hash (HMAC-Hashed Message Authentication Code) [16].

Los centros de datos son la parte medular de la economía digital, el big data, la nube, la inteligencia artificialy y la Internet de las Cosas (IoT-Internet Of Things). El acceso a este tipo de instalaciones debe ser controlado para no comprometer la seguridad de información y equipo [17]. Los últimos desarrollos dirigidos a la autenticación y encriptación para el control de acceso a centros de datos, han trabajado usando: mapas de pixeles de temperatura absoluta y emisión de la palma de la mano obtenidos con un termógrafo infrarrojo [18], códigos convolucionales y la función XOR, encriptación a través del protocolo de la generación de claves distribuidas (DKG-Distributed Key Generation) y códigos RaptorQ [19].

El trabajo aquí presentado tiene como objetivo mitigar esta vulnerabilidad para evitar el ataque Thermanator, usando un simple concepto: el cambio de posición de las teclas en cada autenticación a través de un teclado de colores en lugar de dígitos en el que cada solicitud de autenticación cambia la posición de los colores a mostrar. Comunicar el afecto correcto, un sentimiento, una experiencia o una emoción es fundamental para crear una

comunicación visual atractiva al recordar una autenticación. Las diferentes propiedades de color, claridad, croma y tono, las diferentes propiedades de paleta, combinaciones y distribución de colores, contribuyen a diferentes interpretaciones afectivas en la visualización de información donde la cantidad de colores es típicamente menor a las paletas ricas utilizadas en diseño. Un ejemplo de combinaciones se muestra en la Figura 2.

## II. Parte Técnica del Artículo

En la realización de este trabajo la metodología seguida fue dividir el diseño en cuatro etapas como se muestra en la Figura 3. Las etapas son las siguientes: la fuente de alimentación, el actuador de la contrachapa eléctrica, la pantalla táctil LCD y el sistema embebido Raspberry Pi 3.

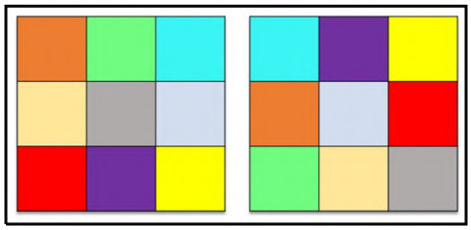

Figura 2. Teclado multicolor con cambios de posición aleatorios

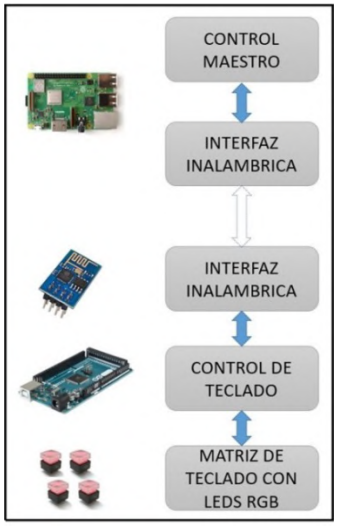


Figura 3. Diagrama de bloques del sistema desarrollado

### *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 se encuentra instalada la base de datos de los códigos de autenticación válidos y la inicialización para cada uno de los módulos cliente instalados. La base de datos creada para la generación de colores es de nueve gamas, que corresponden a las nueve posiciones de la matriz de leds 3x3 utilizada, numeradas de cero a ocho. Esta tabla se envía a los clientes donde se ubican las matrices de teclas con led RGB para inicializar la representación de los colores. En la Tabla I se muestran los parámetros de ancho de pulso de la señal PWM usada para generar cada gama.

TABLA I
TABLA DE CÓDIGOS DE COLOR UTILIZADOS PARA GENERAR EL COLOR POR PWM EN CADA LED RGB

| Pulsos para generar PWM | | | |
|---|---|---|---|
| Código | Red | Green | Blue |
| 0 | 200 | 25 | 190 |
| 1 | 43 | 80 | 63 |
| 2 | 98 | 110 | 215 |
| 3 | 72 | 49 | 23 |
| 4 | 170 | 25 | 220 |
| 5 | 100 | 42 | 43 |
| 6 | 38 | 189 | 25 |
| 7 | 180 | 35 | 40 |
| 8 | 178 | 90 | 69 |

La tabla de códigos PWM es generada en el módulo maestro y puede ser modificada fácilmente para tener las diferentes paletas de color. La idea principal fue generar una lista aleatoria de ubicación de las diferentes gamas de colores a desplegar en el teclado como se muestra en la Figura 4. Esta lista se genera y transmite cada vez que el cliente realiza una autenticación valida o fallida, que en este trabajo es de cuatro selecciones de color.

El dispositivo espera recibir la secuencia de códigos de color presionados y compara con la base de datos almacenada en este módulo. En caso de encontrase listada la secuencia en la base de datos, envía un código de autorización al usuario.

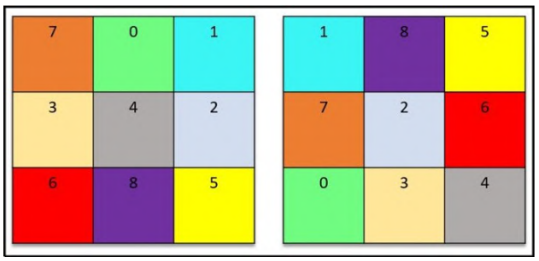


Figura 4. Asignación aleatoria de colores para diferentes capturas

### *B. Interfaz inalámbrica*

Este módulo se encarga de enlazar el control maestro con el control del teclado de forma inalámbrica utilizando tecnología WiFi. En que respecta al módulo de control maestro, se programó la interfaz inter construida del Raspberry utilizando bibliotecas de comunicación en red con Python para las diferentes entradas y salidas de información. El módulo utilizado que controla las comunicaciones en red del lado del cliente Arduino Mega, es un circuito ESP8266, el cual es un módulo versátil y de bajo costo usado para la comunicación empleando la pila de protocolos TCP/IP.

### *C. Control de teclado*

El control del teclado se encarga de esperar la inicialización enviada por el módulo maestro y generar las señales PWM para establecer el color en cada uno de los leds RGB del botón. Está compuesto por una tarjeta Arduino Mega 2560, con múltiples salidas PWM para obtener las diferentes gamas de color utilizados en la paleta que envía el modulo maestro y como entradas la matriz de conmutación para detectar y registrar las combinaciones presionadas. Al presionar un botón, se genera una interrupción y se captura la combinación de la tecla presionada que está directamente relacionada con un color en la tabla de inicialización de la matriz de 3x3.

Al recibir cuatro códigos de color presionados por el usuario, este módulo envía la información al dispositivo maestro para cotejar el código en una base de datos, en cuanto el modulo maestro retorna la respuesta se encienden durante un segundo todos los leds RGB, si la respuesta es afirmativa se enciente el color verde durante un segundo y si es negativa se enciente el color rojo. Esto indica si fue acertada la selección y retorna al estado de espera de nuevos códigos para repetir el proceso.

### *D. Matriz de teclado con leds RGB*

Esta matriz fue diseñada con botones del tipo E-switch, modelo ULP12OAP1RSSCL1RGB los cuales contienen un led RGB y un conmutador de un polo dos tiros, como se indica en la Figura 5.

Se utilizó una matriz con botones en arreglo de tres renglones por tres columnas, la cual está compuesta por nueve botones o teclas cada uno con un led RGB incluido. Para tener un manejo individual del color de cada led, el control de la iluminación de los éstos se realizó a través de los renglones de activación y las columnas activando las salidas RGB por PWM.

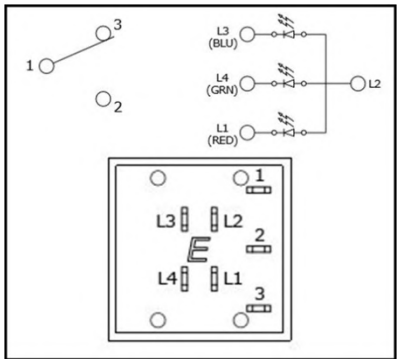


Figura 5. Diagrama y posición de terminales del switch con *leds RGB*

## III. RESULTADOS

Para la realización de las diferentes pruebas se realizó la programación por el lado del control maestro y los clientes, de tal forma que fuera más fácil realizar la estadística de los resultados obtenidos. Primeramente, se modificó el código para tomar el tiempo desde que se presiona el botón con la primera combinación hasta que se presiona el cuarto botón correctamente. Con esto, se generó una tabla de datos la cual se graficó para mostrar el tiempo al presionar las teclas en cada muestra como se muestra en la Figura 6.

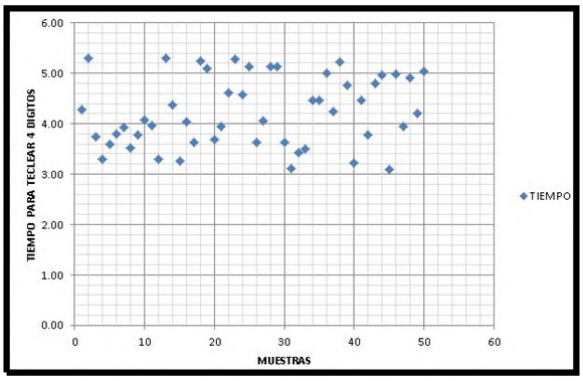


Figura 6. Tiempos de suministro de claves de 50 usuarios

La segunda prueba se realizó modificando el código de programación y las bases de datos, para modificar la cantidad de códigos de color a recordar por los usuarios. Se inició con tres códigos de color, posteriormente con cuatro y después con cinco colores diferentes de la paleta especificada. En las tres pruebas participaron diferentes personas en diferentes tiempos y se tomó en cuenta los aciertos y errores según la combinación de colores a recordar, a partir de esto se obtuvieron los resultados indicados en la gráfica de la Figura 7.

La muestra de usuarios fueron personas entre 20 y 55

Año: 2020 Volumen: 1
Número 6, ISSN: 2448-623X

años de edad sin limitantes físicas como deficiencias visuales o motrices en las manos. A los usuarios que realizaron las pruebas se les entregó impreso el patrón de colores a suministrar con una antelación de 30 minutos, inmediatamente después se les realizaron las pruebas.

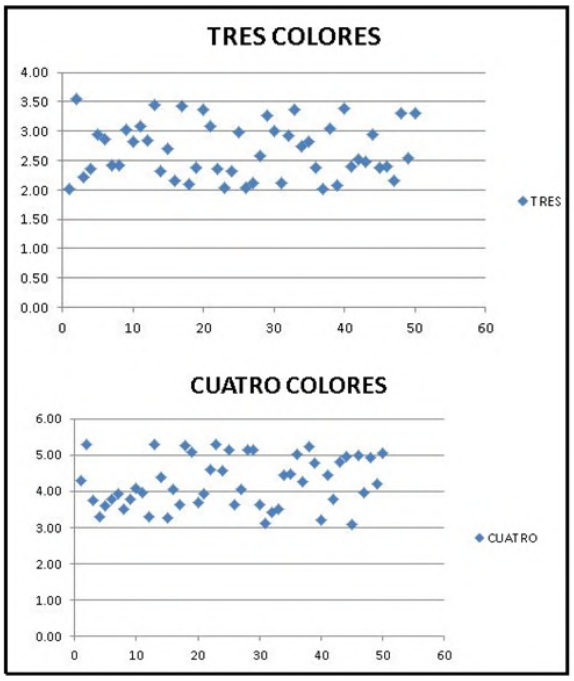


Figura 7. Tiempos de suministro de claves de tres y cuatro colores

## 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. En el caso de personas con capacidad mental limitada se se debe ajustar el sistema para usar una paleta de colores convencionales y para usuarios que tengan mayores habilidades de memorización se puede crear una paleta de colores más compleja y una cadena de combinaciones de más colores, esto pensando en autenticaciones que requieran mayor seguridad. En la Figura 8 se muestra la matriz de teclas construida.

En el caso de los usuarios que normalmente memorizaban la posición de las teclas para la autenticación, este cambio fue muy radical y hubo algunos que comentaron que no sería factible. Psicológicamente existen gamas de colores, tonos y brillos que ayudan más a ser memorizados que otros, por lo para seleccionar la paleta es necesario un estudio del ambiente donde se utilizará el sistema. La memorización a corto y largo plazo es otro de los aspectos que se deben tomar en cuenta para el ambiente donde se instale el sistema.

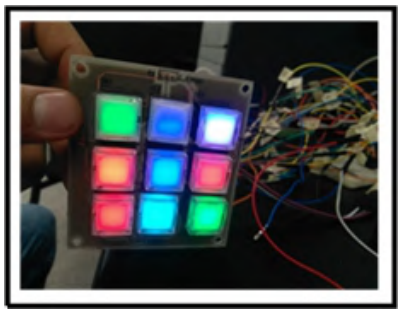

Figura 8. Teclado con colores RGB construido

## V. REFERENCIAS

[1] Joy, J. P. y Jyothis, T. S. (2016). "Secure authentication", Online *in Procedings International Conference on Green Engineering and Technologies* (IC-GET), pp. 1-3.

[2] 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.

[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] Morii, M.; Tanioka, H.; Ohira, K. (2017). "Research on Integrated Authentication Using Passwordless Authentication Method", *in Procedings IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, pp. 682-685.

[5] 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.

[6] 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.

[7] 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.

[8] Zhao, G.; Li, Y. y Du, L. (2015). "Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment", *in Procedings 2nd International Conference on Information Science and Control Engineering*, pp. 156-159.

[9] 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.

[10] 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.

[11] Gupta, N.; Gandhi, V. y Hariya, C. (2018). "Detection of Code Clones", *in Procedings International Conference on Smart City and Emerging Technology (ICSCET)*, pp. 1-4.
[12] Malathi, V.; Balamurugan, B. y Eshwar, S. (2017). "Achieving Privacy and Security Using QR Code by Means of Encryption Technique in ATM", *in Procedings Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, pp. 281-285.
[13] Khairnar, S.; y Kharat, R. (2016). "Online fraud transaction prevention system using extended visual cryptography and QR code", *in Procedings International Conference on Computing Communication Control and automation (ICCUBEA)*, pp. 1-4.
[14] Roopak, S. y Thomas, T. (2014). "A Novel Phishing Page Detection Mechanism Using HTML Source Code Comparison and Cosine Similarity", *in Procedings Fourth International Conference on Advances in Computing and Communications*, pp. 167-170.
[15] Zhilyaev, A. E.; y Gurova, E. B. (2018). "On the question of the authentication tag length based on Reed-Solomon codes", *in Procedings Moscow Workshop on Electronic and Networking Technologies (MWENT)*, pp. 1-5.
[16] Tamer, S. A. (2017). "Generated Un-detectability Covert Channel Algorithm for Dynamic Secure Communication Using Encryption and Authentication", *in Procedings Palestinian International Conference on Information and Communication Technology (PICICT)*, pp. 6-9.
[17] Suresh, T. y Murugan, A. (2018). "Strategy for Data Center Optimization: Improve Data Center capability to meet business opportunities", *in Procedings 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, pp. 184-189.
[18] Yu, H. L.; Li, Y. L. y Liao, T. Y. (2018), "Fast and Accurate Emissivity and Absolute Temperature Maps Measurement for Integrated Circuits", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 26, Issue: 5, pp. 912-923.
[19] Qiu, J.; Li, H. y Dong, J. (2017). "Biometrics Encryption Based on Palmprint and Convolutional Code", *in Procedings 2nd International Conference on Multimedia and Image Processing (ICMIP)*, pp. 187-190.

## 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.

**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.

**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 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.

**Sánchez-Rangel Francisco Javier.** Ingeniería Electrónica, UAM-Azcapotzalco, Cd. de México, 1987. Maestría en Ciencias de la Computación, UAM-Azcapotzalco, Cd. de México, 1999. Labora actualmente en la UAM-Azcapotzalco.

**López-Aparicio Liliana.** Estudiante de Doctorado en Ciencias Biomédicas. Facultad de Medicina de la Universidad Autónoma de Coahuila, Unidad Torreón. Su línea de trabajo es Investigación en Psicología.

**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.