La Mecatrónica en México, Enero 2018, Vol. 7, No. 1, páginas 46 – 58.
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

Artículo seleccionado del
4° Congreso Internacional
de Sistemas Embebidos (ICES18)

Plataforma Electrónica para el Acceso a Edificios y/o Casas Mediante Código QR Encriptado

Troncoso-Ramos Jonathan Armando, Rodríguez-Reséndiz Juvenal✉, Pedraza-Ortega Jesús Carlos, Ramos-Arreguín Juan Manuel.

✉juvenal@uaq.mx

Universidad Autónoma de Querétaro, Facultad de Ingeniería.

Resumen

En el presente artículo se describe la implementación de un algoritmo de encriptación basado en permutación de elementos usando un código QR (Quick Response) para la gestión de acceso al personal autorizado, utilizando las capacidades que ofrece un sistema embebido. Los sistemas embebidos basados en arquitectura ARM (Advanced RISC Machine), poseen características que los convienen en soluciones muy robustas, tales como poco consumo energético, escalables, y una alta disponibilidad de librerías de uso libre para el desarrollo de soluciones. El algoritmo se gestionó a partir del lenguaje de programación Python utilizando OpenCV (Open Source Computer Vision Library), lo cual hace posible la lectura del código QR, permitiendo o denegando el acceso según sea el caso. Se realizaron pruebas con la finalidad de medir el progreso en cada etapa de desarrollo hasta llegar al sistema final, el cual cuenta con un interfaz gráfico diseñado en Python con una administración centralizada para la gestión eficiente de usuarios, consultas de registros y acceso al sistema de encriptación de una manera simple, lo anterior permite una rápida respuesta del algoritmo en su validación de información para denegar o conceder el acceso al personal interno dentro de las instalaciones.

Palabras clave: encriptación, código QR, OpenCV, sistemas embebidos, Python, ARM.

Abstract

This work presents the development about the implementation for an encryption algorithm based on elements permutation. Using a QR code that manages the access for authorized personnel, based on capabilities that embedded systems offer. Embedded systems based on ARM architecture have some characteristics that turn them on trustworthy solutions. Some of these solutions are low power consumption, the capacity for being modular and the availability of many open sources to development solutions. These allows the development of low consumption and high efficiency systems according to necessities. The algorithm was programmed on Python language, this language counts with many open sources which support the general propose of the algorithm, the incorporation of OpenCV permitted reading an identification of elements for the final QR code. According to the methodology used for managing the access, an image was obtained with a camera (applying encrypted QR code), in order to be processed by the algorithm and get the username for the one that requested the access. Then a request is made in order to consult database, as result the algorithm validates the information (in case this exists).

Keywords: Encryption, QR code, OpenCV, Embedded Systems, Python, ARM.

1. Introducción

Actualmente existe una amplia gama de sistemas de seguridad comerciales que permiten gestionar el acceso a edificios de manera precisa, mediante el uso de tarjetas inteligentes, contraseñas ingresadas desde un panel hasta reconocimiento de huella dactilar, sin embargo, el avance tecnológico proporciona herramientas más completas que permiten al atacante robar los datos de los usuarios del sistema. Citado lo anterior las necesidades de la sociedad han cambiado con el paso de los años, lo que ha generado el desarrollo de soluciones a partir de nuevas tecnologías y algoritmos que permiten la implementación de sistemas de seguridad robustos, brindado mayores características de protección a los datos de los usuarios.

El sistema de seguridad propuesto en el presente trabajo incorpora un algoritmo de encriptación basado en permutación de elementos en un código QR desarrollado en una plataforma embebida con arquitectura ARM, en conjunto con una cámara, permite resolver deficiencias en el almacenamiento de los datos de los usuarios, así como el aprovechamiento de los recursos para un acceso eficiente en el lugar designado que se desee instalar.

La principal ventaja de utilizar un código QR con texto cifrado, radica en que la información siempre estará protegida ante posibles ataques externos, permitiendo que los datos puedan ser exclusivamente leídos de manera correcta, la cámara en conjunto con el algoritmo verificará al usuario que intenta acceder para conceder el permiso o denegarlo según sea el caso. Programando más casos críticos de riesgo que impidan el robo de datos de los usuarios del sistema, como el cifrar los datos almacenados, llevar un control de los usuarios registrados, gestión centralizada desde un panel de administrador; con la finalidad de proporcionar mayor panorama ante las situaciones de vulnerabilidad del sistema que puede generar un atacante; poniendo medidas más fuertes de seguridad que impidan el cumplimiento del objetivo por parte del atacante tales como; obtener los datos para usos no autorizados o entrar de manera no permitida a las instalaciones.

2. Sistemas de seguridad

Uno de los retos más importantes que actualmente enfrentan las autoridades y sociedad es la violencia y la seguridad, como antecedente de ello se encuentra el nivel de percepción de la población sobre este tema en las entidades federativas referida en la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE), publicada el 30 de septiembre de 2014, reportando un incremento en la percepción de la inseguridad en este año del 73.3%, frente al 72.3% del año pasado. En el Estado de Querétaro, las cifras reportadas por el Sistema Nacional de Seguridad indican un incremento constante en la incidencia delictiva pues de 26,032 delitos registrados por las autoridades en el año 2012 se proyecta que al final de este año ascienda a 30,942 ilícitos, destacando por su número los robos y las lesiones. Atendiendo su objetivo de atender las necesidades sociales, es fundamental que la investigación científica y el desarrollo tecnológico, presenten soluciones capaces de resolver los problemas que nos aquejan como sociedad, teniendo como principal objetivo las instituciones públicas de educación superior. Lo anterior tiene como marco normativo el Plan Nacional de Desarrollo (PDN) 2013-2018, teniendo entre sus objetivos hacer del desarrollo científico, tecnológico y la innovación pilares para el progreso económico y social sostenible. Por su parte, el Programa Especial de Ciencia y Tecnología e Innovación 2014-2018 establece a la seguridad ciudadana como tema prioritario para el Sector de Ciencia, Tecnología e Innovación; a su vez, el Plan Querétaro 2015 incluye entre sus grandes ejes de desarrollo, la Seguridad y Estado de Derecho y alineado a los grandes ejes de desarrollo el Programa Estatal de Ciencia y Tecnología 2010-2015, en su objetivo estratégico 4 determina el promover la aplicación del conocimiento científico y tecnológico a la solución de problemas específicos del sector productivo y social, que contribuyan al desarrollo sustentable del estado. Analizando las causas básicas de una determinada amenaza, la seguridad humana identifica los cambios estructurales, internos o externos, y los de comportamiento que se necesitan para mitigar sus consecuencias, y en la medida de lo posible evitar que se vuelvan a repetir en un futuro.

La biometría es usada para muchos propósitos, tales como la detección de criminales, identificación, el control de acceso entre otros [1]. Las características biométricas se pueden dividir en dos clases principales [2]:

Fisiológicas. Relacionado con la forma del cuerpo y que varía de persona a persona con respecto a los diferentes rasgos físicos, citando ejemplos como: la forma del cuerpo, forma del rostro, geometría de la mano, reconocimiento de iris.

Comportamiento. Están relacionados con el comportamiento de la persona, algunos ejemplos de este caso son: la firma, dinámica de pulsaciones de teclas.

Uno de los problemas de seguridad que presentan los sistemas de autentificación biométrica es el robo de identidad, que es consecuencia del almacenamiento de las plantillas (remota o localmente) dentro del sistema, siendo principal objetivo de los atacantes, una solución a este tipo de vulnerabilidad es el cifrado de la plantilla antes de su almacenamiento o transmisión a través de un canal inseguro [3].

Los sistemas caóticos poseen características como ergodicidad, diversidad de datos, sensibilidad a condiciones iniciales, parámetros de control, compartibles con propiedades criptográficas tales como permutación, difusión, secuencia pseudoaleatorias y complejidad del sistema base, permitiendo desarrollo en cifrado de imagen [3].

El término criptografía proviene de dos vocablos griegos: criptos que significa oculto o escondido y grafos, que significa escritura. A partir de la definición anterior, la criptografía tiene como estudio la escritura oculta. Específicamente, la criptografía transforma un mensaje con significado pleno usando claves o cifras que ocultan el verdadero significado de este. Uno de los objetivos de la criptografía es la protección de la información dado que actualmente los ataques tienen como objetivo la obtención de datos relevantes, el atacante se vale de una serie de técnicas, herramientas que le permitan descifrar el mensaje y hacerse de la información, teniendo como necesidad el diseño de algoritmos robustos que permitan elevar el grado de seguridad en datos sensibles para evitar ataques que terminen en pérdidas masivas de información [4].

La eficiencia de los sistemas de seguridad radica en el número de casos de riesgos que puedan abarcar para evitar que el atacante obtenga información o pueda acceder de manera no autorizada para cometer actos ilícitos en el espacio asignado, llevando al desarrollo de nuevas soluciones basadas en las tecnologías de la información como la implementación de algoritmos basados en métodos criptográficos; permitiendo la codificación y cifrado de la información de los usuarios del sistema. El sistema de seguridad presentando en este artículo tiene como prioridad el cuidado de la información de los usuarios del sistema, tomando como fundamentos estudios y análisis de algoritmos de cifrado para gestionar el acceso mediante el uso de un código QR, abarcando más casos de riesgos y brindando mayor grado de protección al entorno donde opera el sistema.

La transposición es una de las dos grandes técnicas de transformación de texto plano. En una transposición las letras del texto plano se mezclan o desordenan siguiendo un determinado algoritmo para obtener un anagrama. Un anagrama se presenta cuando una palabra tiene las mismas letras con el mismo número de apariciones, pero en un orden diferente. Por ejemplo, el criptograma OTERCES es una de las 7! =5040 transposiciones o anagramas posibles del texto plano secreto, en este caso el resultado del algoritmo es poner al revés la palabra [4].

Una de las principales desventajas de utilizar este método radica en la longitud del texto que se quieren cifrar, en este caso si la cadena de texto plano legible es corta, se puede descifrar la palabra de manera relativamente rápida y sencilla dado que los escenarios ante las combinaciones posibles no son demasiadas; por otro lado si el texto tiene una longitud considerable el método de cifrado por transposición se vuelve muy viable dado que las combinaciones posibles aumentan radicalmente, y resulta prácticamente imposible descifrar sino se tiene la clave, llave o el protocolo correcto.

Una de las técnicas más usadas para el cifrado de texto plano es la sustitución, respetando la posición de cada letra de la cadena de texto, pero cada letra es sustituida en su posición por otra de un alfabeto propuesto haciendo que el texto cifrado no sea legible y carezca de sentido sino se tiene la clave o llave necesaria para descifrar el texto. Es un método de cifrado bastante eficiente para cadenas de texto cortas dado que si se aplica un análisis estadístico y se encuentra cierto comportamiento o patrón se puede descifrar el texto con facilidad y hacerse de la información se tenga o no permiso de acceso a ella.

Los alfabetos de sustitución propuestos son la base para la formación de anagramas para el proceso de cifrado de texto a continuación se muestra un ejemplo:

Alfabeto plano: a b c d e f g h i j k l m n o p q r s t u v w y z

Alfabeto B: @ # $ & % / n H Q 5 6 1 0 9 3 7 P Q M A J K 4 2 L

Como se mencionó anteriormente se puede aplicar un análisis estadístico que de pauta de la asignación del alfabeto plano al alfabeto B en cada posición correspondiente, para dificultar más que el atacante tenga la llave que le permita descifrar el texto, adicionalmente al alfabeto propuesto se le agregan símbolos los cuales hacen más complicado adivinar el patrón de cada posición del texto original, a este tipo de sustitución se le conoce como homófona. Los métodos en los que solo se emplea un alfabeto de sustitución se denominan monoalfabéticos, por otro los que utilizan dos o más alfabetos se les denominan polialfabéticos.

En la figura 1 se muestra los campos de estudio de la criptografía, así como una breve clasificación, ejemplificando el contexto de su evolución hasta llegar a lo que hoy conocemos como criptografía y su alcance con los métodos de cifrado más usados.

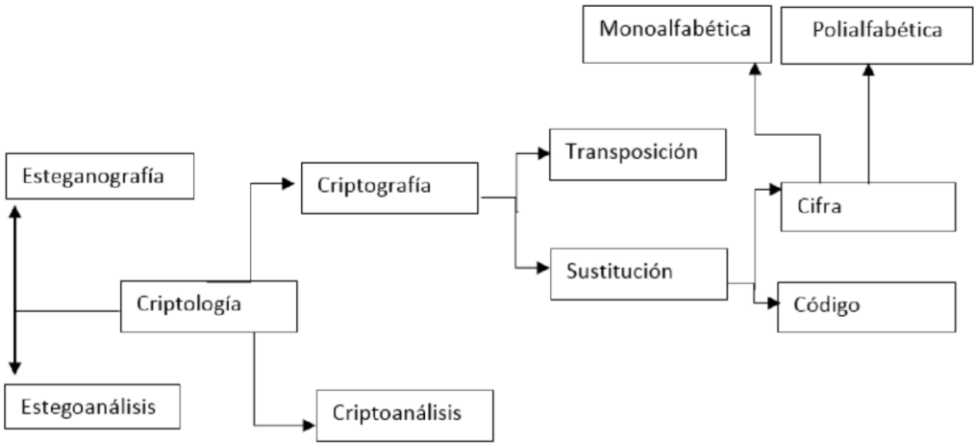


Figura 1. Ciencia del estudio de la escritura secreta y sus campos.

2.1 Algoritmo cifrado de texto

El proceso de cifrado contempla en primer lugar la creación de una plantilla cifrada de una plantilla clara, utilizando un algoritmo basado en la arquitectura de permutación-difusión (modificación de posición-valor) mediante secuencias caóticas del mapa logístico. El procedimiento de cifrado considera como plantilla clara $P \in [0,255]$ con una longitud de $l = 2072$ (bytes). Por otro lado, el mapa logístico puede ser descripto por la ecuación (1) [2].

$$xi + 1 = ax(1 - xi) \quad (1)$$

En donde $xi \in (0,1)$ representa el estado del sistema $a0 \in (0,1)$ es la condición inicial y $a \in (3,994)$ el parámetro de control para genera secuencias aleatorias (caos) y descartar ventanas periódicas. Los sistemas caóticos al igual que el mapa logístico tienen una desventaja para su implementación en sistemas de cifrado tales como rasgos caóticos discontinuos, distribución no uniforme, prioridad y espacio de llaves reducido, por otra parte, las ventajas son la simple estructura lo que facilita su implementación y la alta tasa de salida.

A continuación, se enlistan los pasos que engloban el proceso de generación de un sistema cifrado:

- Se establece un rango de 128 bits (32 caracteres hexadecimales)
- K ∈ [0-9, A-F] para generar secuencias caóticas en dos mapas logísticos a partir de los siguientes parámetros de entrada:

  i) 32 dígitos para la llave secreta
  ii) Parámetros de control $H_1, H_2, \ldots H_{32}$ donde H ∈ [0-9, A-F]

Obteniendo los datos necesarios se plantean las ecuaciones (2), (3), (4) y (5) tomando el rango de los parámetros de control [3].

$$\frac{(H_1,H_2,\ldots H_8)10}{2^{32}+1} \quad (2)$$

$$\frac{(H_9,H_{10},\ldots H_{16})10}{2^{32}+1} \quad (3)$$

$$\frac{(H_{17},H_{18},\ldots H_{24})10}{2^{32}+1} \quad (4)$$

$$\frac{(H_{25},H_{26},\ldots H_{32})10}{2^{32}+1} \quad (5)$$

Las ecuaciones anteriores representan el proceso de generación de la llave secreta. Para la distribución de la llave secreta en los mapas logísticos pueden ser descriptos con las ecuaciones (6), (7), (8) y (9) [3].

$$\alpha_1 = 3999 + (\alpha_1 * 0.001) \quad (6)$$

$$\alpha_1 = (\mathrm{A} + B + Z)\ mod\ 1 \quad (7)$$

$$\alpha_2 = 3999 + (\alpha_2 * 0.001) \quad (8)$$

$$\alpha_2 = (\mathrm{A} + B)\ mod\ 1 \quad (9)$$

En el caso para las variables $\alpha_1$representan al mapa logístico 1 y α_2 representan al mapa logístico 2 en el proceso de distribución [3].

Tomando lo anterior como antecedente para la generación del algoritmo a implementar se consideró una muestra inicial de 25 elementos cada uno de ellos con un valor posicional clave para la iteración en un mapa logístico propuesto de elementos de la misma cantidad que la muestra inicial. La mejora implementa un nuevo posicionamiento de los valores iniciales, resultando en un criptograma no

tan obvio como en la primera versión, de la misma manera se realiza una serie de operaciones extras para agregar “ruido” para que elevar la complejidad de encriptación de la información original.

El análisis de componentes principales es útil cuando se hayan obtenidos datos de un número de variables, en donde se creen que hay alguna redundancia en esas variables, la redundancia significa que algunas de las variables son correlacionadas entre sí, reduciendo la muestra inicial a 25 elementos de entrada para la generación del criptograma [5]. El algoritmo itera elementos obteniendo su equivalente en base a sus posiciones y operaciones mencionadas anteriormente, en la figura 2 muestra el diagrama de flujo que describe el proceso de encriptación y desencriptación desarrollado.

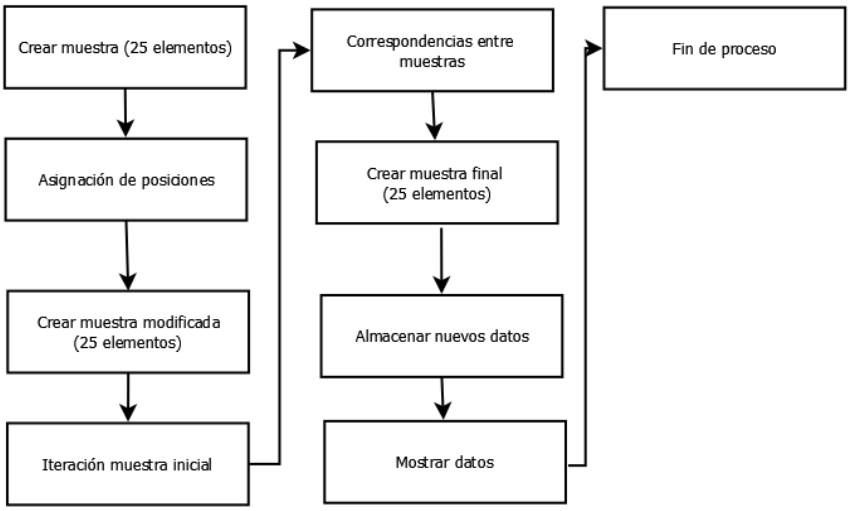


Figura 2. Diagrama proceso de encriptación.

3. Sistemas embebidos basados en arquitectura ARM

Se puede definir como sistema embebido a un sistema electrónico que tiene como fin el realizar una(s) tareas específicas para un fin deseado. Los sistemas embebidos pueden incluir elementos de hardware y software que contribuyan a la realización del fin propuesto [6].

En la actualidad, estamos en constante interacción con los sistemas embebidos sin saber que lo son, desde el celular que utilizamos, televisión, lavadora, etc. Los sistemas embebidos conforman una gran parte del desarrollo tecnológico, así como aportan soluciones a la vida cotidiana de la sociedad, aprovechando todos los recursos para obtener una gran eficiencia en los procesos asignados.

Los sistemas embebidos difieren un poco de los demás porque sus interfaces están directamente relacionados con el hardware del dispositivo, además de llevar un control de los recursos que se utilizan por operación lo cual los hace más eficientes y con menor consumo energético. Este tipo de sistemas pueden ejecutar operaciones de manera eficiente, manejando tiempos de respuesta sumamente rápidos de procesamiento. Sin embargo, son sistemas que requieren de personal capacitado para desarrollarlos o brindar mantenimiento según sea el caso.

En la actualidad la industria electrónica innova y presenta nuevas soluciones tecnológicas, demandando desarrollos más complejos en lapsos de tiempo más cortos, optimizando recursos y diseñando nuevas arquitecturas adaptables a las tecnologías de última generación. La implementación de los dispositivos programables trajo un cambio significativo al integrar hardware y software en componentes capaces de ser reconfigurables, sin perder características como la eficiencia energética, costo, y robustez [6].

En 1983 Acorn Computers Ltd comenzó la investigación de una nueva arquitectura el cual sería un procesador con un juego reducido de instrucciones (RISC). El diseño fue finalizado en el año de 1985, al que llamaron ARM1 (Acorn RISC Machine 1), este modelo contaba con 25000 transistores sin embargo fue sustituida rápidamente un año después por la versión mejorada ARM2, contaba con un bus de datos de 32 bits con un espacio de direcciones de 26 bits, junto con 16 registros de 32 bits. Eventualmente se consiguieron mejoras en los modelos como el ARM3 en 1990 logrando latencias de 25 Mhz, hasta llegar al modelo ARM6 que contaba con 35000 transistores mejorando la administración de los periféricos integrados, pero fue el diseño del procesador ARM7DMI el que marco un cambio significativo en el desarrollo tecnológico para la arquitectura ARM [7].

La arquitectura de 32-bits de ARM es la más utilizada por los dispositivos móviles hoy en día, existiendo variantes de procesadores de la gama Cortex, los cuales son diseñados para diferentes aplicaciones.

Cortex-A: Diseñados para aplicaciones.
Cortex-R: Diseñados a sistemas en tiempo real y empotrado (embebido). iii) Cortex-M: Diseñados a micro-controladores empotrados (embebido).

ARM se puede definir como una máquina con un conjunto de instrucciones reducidas que incorpora las siguientes características:

Un fichero de registro único.
Arquitectura de load/store donde las operaciones de procesamiento de datos solo operan en los contenidos de los registros y no directamente en la memoria. iii) Instrucciones simplificadas y reducidas para la decodificación de instrucciones. iv) Control de ALU (Arithmetic Logic Unit) y decodificador de instrucciones. v) Auto-incremento y decrementos de direccionamiento para optimización de bucles.

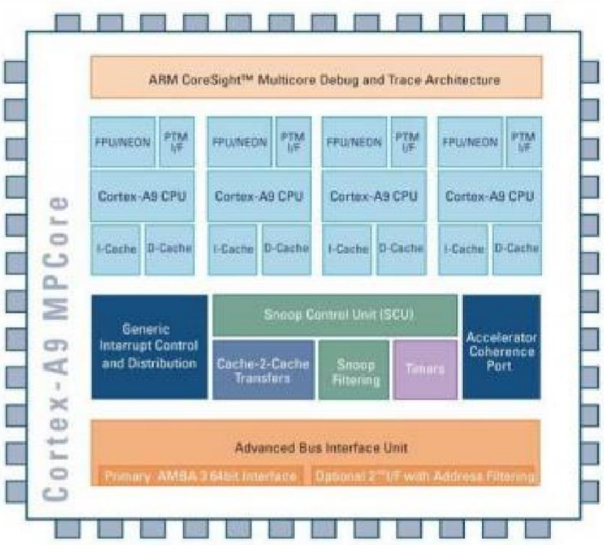


Figura 3. Diagrama de un procesador ARM de 4 núcleos.

En la figura 3 podemos apreciar la distribución de la arquitectura que conforma un procesador ARM Cortex de 4 núcleos, con ello se puede comprender más de la potencia de computo bruto que puede ofrecer una tarjeta electrónica basada en esta arquitectura para el desarrollo de un sistema embebido dedicado a la seguridad el cual estará en funcionamiento en tiempo continuo y estará realizando múltiples tareas a la vez.

4. Metodología

La metodología propuesta se presenta en la figura 4. Donde se considera como primera etapa el análisis de longitud de la cadena de texto, así como la evaluación de caracteres especiales, una vez obteniendo los resultados se propone en la segunda etapa permutaciones a cada elemento de la cadena de texto teniendo un panorama amplio de los patrones característicos de cada permutación. En la tercera etapa se comienzan a realizar pruebas de lectura del código QR con resoluciones soportadas por la cámara, permitiendo conocer las distancias ideales entre el código QR y el lente de la cámara para la búsqueda de correspondencias de puntos discretos en la imagen, los cuales podemos denominar como puntos de interés, seleccionados en ubicaciones distintivas de la imagen y obtener con la mayor precisión posible el texto [8].

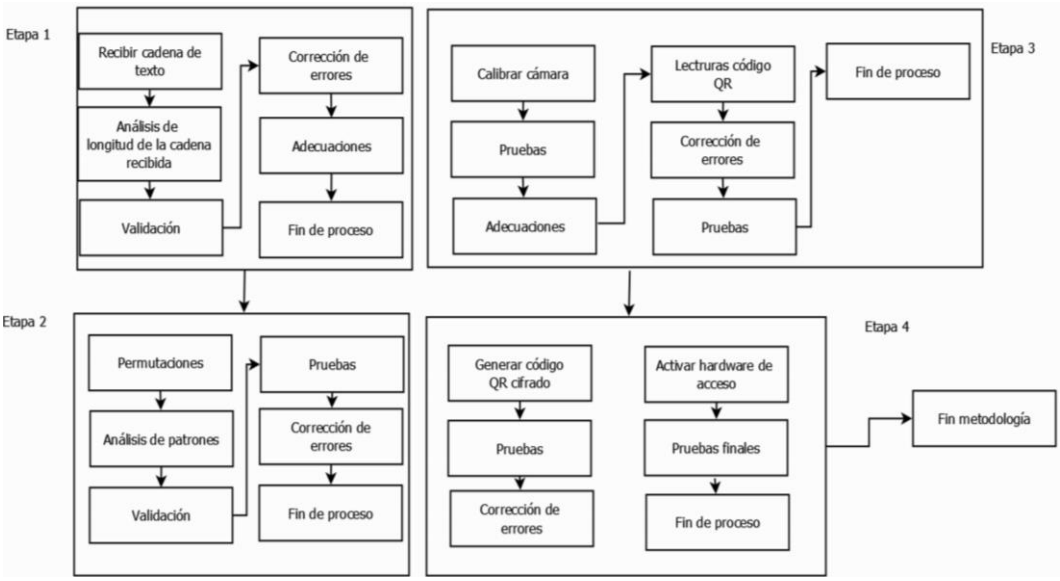


Figura 4. Metodología propuesta.

En la cuarta etapa se incorporó el texto cifrado en el código QR para su lectura y se obtuvieron las primeras lecturas para poder recuperar la cadena original, en este caso el nombre del usuario que se otorgó permiso de acceso a la instalación, siguiendo los principios de reconocimiento facial que significa dar una imagen del código QR, requiriendo que el sistema determine si es el usuario autorizado o no para el acceso [9], se evaluó casos en donde la lectura no era óptima y se mejoró el algoritmo hasta conseguir una eficiencia de respuesta de lectura y activación del hardware para gestionar el acceso. La verificación de cada cadena cifrada de texto se comprobaba con la base de datos, aplicando otro filtro de seguridad encontrando correspondencias entre lo almacenado y lo que se recibía por el código QR [10]. Por último, se realizaron pruebas del sistema final, en busca de errores para ser corregidos antes de su implementación final en el espacio asignado.

Teniendo como contexto la metodología divida en etapas, cada una cuenta con subprocesos para garantizar la mayor eficiencia en relación entre el software y el hardware, en cada una de las etapas se implementaron pruebas las cuales consistían en la corrección de errores, bugs para realizar las adecuaciones pertinentes con la finalidad de que el software final no tuviera problemas de seguridad los cuales pueden ser explotados por el atacante para el robo de información o acceso no permitido. Una de las ventajas de separar la metodología en etapas radica en el mantenimiento del sistema total, con ello se puede detectar de manera más precisa la falla para ser atendida, sin afectar completamente el funcionamiento del sistema.

En cada etapa se considera un proceso de corrección de errores lo cual se traduce en conseguir la mayor eficiencia por módulo, con la finalidad de garantizar el cumplimiento puntual de las tareas gestionadas en cada etapa. En una segunda instancia se realiza las adecuaciones, labor que tiene como finalidad el detectar errores, poner el código en situaciones de riesgo y encontrar la solución más adecuadas sin afectar la funcionalidad ni el rendimiento. La metodología presentada en la figura 4 se puede escalar o en su defecto optimizar más, dependiendo del fin propuesto del sistema que se desea implementar.

5. Pruebas y resultados

Se realizaron pruebas y análisis en cada una de las etapas propuestas en la metodología, en la figura 5 se muestra un diagrama de flujo que plantea los pasos de desarrollo del sistema final. Cada proceso permitió depurar errores de compilación, así como verificar los recursos que se estaban ocupando en el procesamiento del algoritmo de encriptación final, dado que se buscaba una rápida respuesta para gestionar el acceso de manera rápida para los múltiples usuarios que requieren acceso a las instalaciones, cuidando un rendimiento entre la parte del software y el hardware.

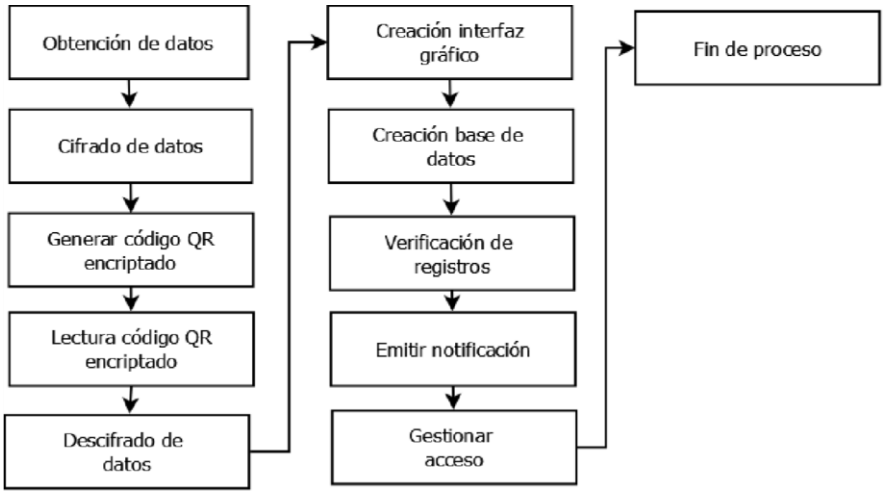


Figura 5. Secuencia de pasos del desarrollo del sistema final.

En la figura 6 se muestra el proceso de lectura del código QR, modificando las resoluciones de la cámara tomando tiempos de respuesta de la lectura del código cifrado, con ello se buscó la resolución más óptima para la lectura. El código QR toma la cadena de texto cifrado, la cámara lee los datos, aplicando filtros y el proceso de descifrado se obtiene una cadena de texto la cual se verifica en la base de datos su existencia, mostrando en la pantalla quién está intentando entrar a las instalaciones.

En la figura 7 se muestra el diseño final del interfaz de usuario del sistema incorporando los algoritmos de cifrado, lectura de código QR, etc. El interfaz cuenta con una presentación sencilla pero funcional que facilita la interacción con el usuario, siendo un sistema abierto al cual se le pueden agregar más características o quitar según sean las necesidades del entorno donde se va instalar y la forma de gestionar el acceso. Se establecieron permisos de usuarios en el cual el administrador del sistema puede acceder a todas las características, como registrar usuarios nuevos, consultar registros o encriptar texto plano para pruebas o generar un nuevo acceso, los procesos del sistema se puede hacer de manera simultánea dado que la programación permite hacer varias tareas a la vez.

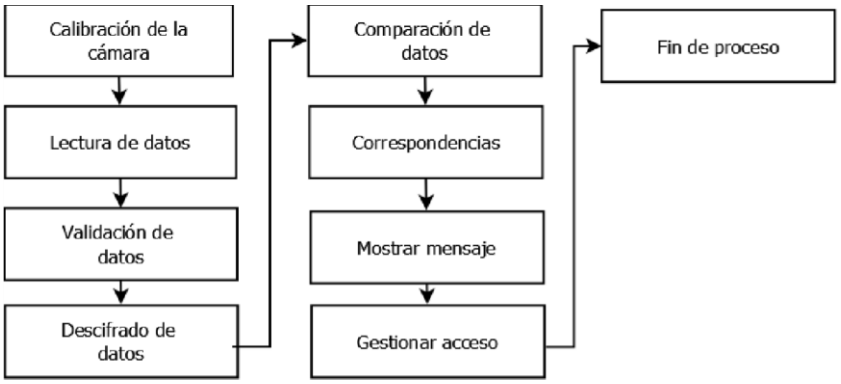
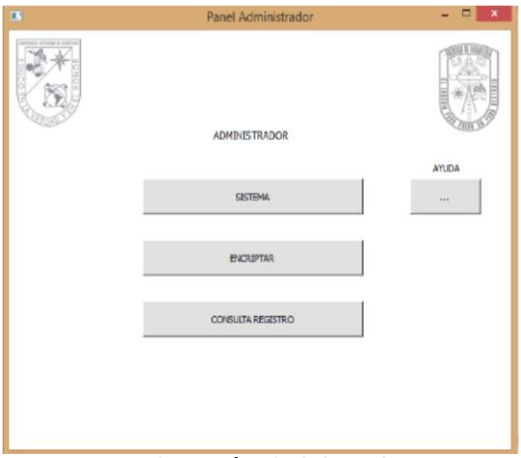


Figura 6. Lectura del código QR cifrado.

a) Pantalla de acceso b) Campos solicitados para registro



c) Menú administrador

Figura 7. Interfaz Gráfico.

En la figura 8 en el inciso a se aprecia la implementación de la mejora del algoritmo agregando nuevos arreglos a las combinaciones de los elementos. Destaca el uso de elementos que cumplen la función de agregar ruido a la información para que su lectura no sea tan intuitiva.

```
INGRESE SU OPCION:  1
ingresa clave numérica: 7
cadena a procesar: mayra azucena cintora garcia
0q0r020u0q0d0|0q0u0h0m0b0r020|0q0b0x020i070q0|0q0u0p0q0g
MENU

1-ENCRIPTAR

2-DESENCRIPTAR

3- ACCEDER

4- SALIR

INGRESE SU OPCION:  2
ingresa clave numérica: 7
cadena a procesar: 0q0r020u0q0d0|0q0u0h0m0b0r020|0q0b0x020i070q0|0q0u0p0q0g
mayra azucena cintora garcia
MENU

1-ENCRIPTAR

2-DESENCRIPTAR

3- ACCEDER

4- SALIR

INGRESE SU OPCION:  4
```

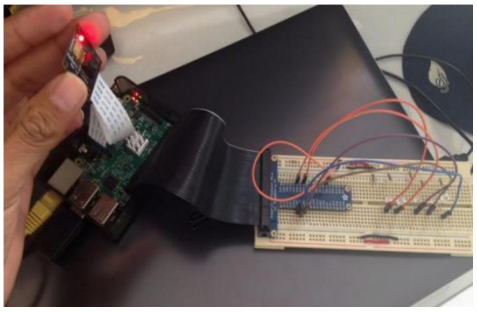
Figura 8. Código de mejora del algoritmo.

Por otra parte, en la figura 9(a), se muestra las pruebas de la lectura del código QR, a una resolución de 400 por 304 pixeles, ideal para evitar problemas de lecturas. Se volvió a probar el generar el código desde un navegador para que este fuera leído a través de un dispositivo y se le aplicaran las pruebas pertinentes para evaluar su rápida lectura y sin perdidas de información, como se puede apreciar en la figura 9(b). En la figura 9(c) y 9(d), se muestra una prueba de lectura del código correcta incorporando un pequeño circuito de pruebas. Sin embargo, los primeros intentos la señal de activación no se alcanza a apreciar, lo cual fue corregido por mandar la señal y hacer que tuviera una duración de 20 segundos tiempo suficiente para poder acceder a las instalaciones. Los diferentes leds indican las primeras pruebas con 5 usuarios diferentes, quedando de la siguiente manera.

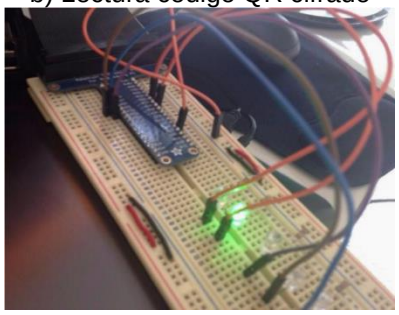
pins= { “Mayra Azucena Cintora García”: 18, “Jesús Carlos Pedraza Ortega”: 17, “Juan Manuel Ramos Arreguín”: 27, “Jonathan Armando Troncoso Ramos”: 22, “Juvenal Rodríguez Reséndiz” :23}, permitiendo obtener tiempos de respuestas, gestión de accesos y evaluar las capacidades de la lectura del código QR cifrado.

a) Pruebas código QR cifrado

b) Lectura código QR cifrado



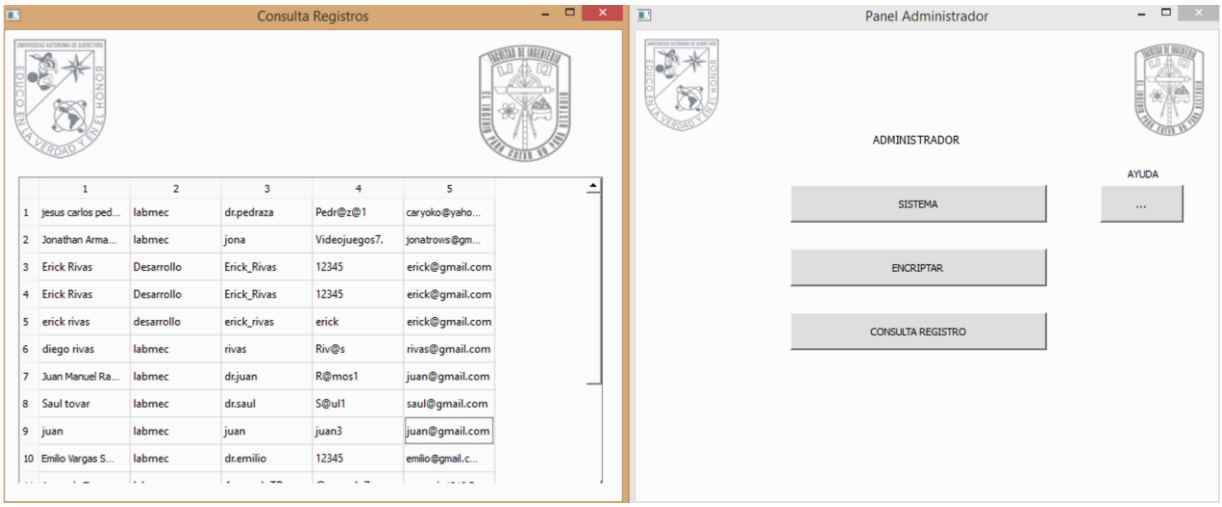
(c) Captura del código cifrado QR



(d) Señal de activación (acceso concedido)

Figura 9. Pruebas.

En la figura 10, se muestra la implementación de la base de datos utilizando sqlite3. Aquí se muestra los registros de la tabla de los usuarios registrados. LA tabla se inicia con una muestra de 30 participantes almacenando nombre, departamento, usuario, contraseña y correo. La ventaja de utilizar sqlite3 radica en la gran compatibilidad con el interfaz gráfico desarrollado con QT en Python, obteniendo una buena respuesta entre las peticiones de las consultas de los registros a verificar por parte del administrador. Para acceder a dicha información es necesario contar con permiso de administrador, permitiendo el manejo de datos más controlado. La distribución de la información que se muestra contempla los campos más significativos de los usuarios, dejando abierta la posibilidad a ingresar más campos según la necesidad del sistema, conservando la eficiencia en la respuesta entre consultas.



	1	2	3	4	5
1	jesus carlos ped...	labmec	dr.pedraza	Pedr@z@1	caryoko@yaho...
2	Jonathan Arma...	labmec	jona	Videojuegos7.	jonatrows@gm...
3	Erick Rivas	Desarrollo	Erick_Rivas	12345	erick@gmail.com
4	Erick Rivas	Desarrollo	Erick_Rivas	12345	erick@gmail.com
5	erick rivas	desarrollo	erick_rivas	erick	erick@gmail.com
6	diego rivas	labmec	rivas	Riv@s	rivas@gmail.com
7	Juan Manuel Ra...	labmec	dr.juan	R@mos1	juan@gmail.com
8	Saul tovar	labmec	dr.saul	S@ul1	saul@gmail.com
9	juan	labmec	juan	juan3	juan@gmail.com
10	Emilio Vargas S...	labmec	dr.emilio	12345	emilio@gmail.c...

Figura 10. Pruebas base de datos.

6. Conclusiones

Se diseñó un prototipo de plataforma electrónica que contiene una cámara, un módulo de pines, que tiene el potencial de ser escalable en hardware y en programación, permitiendo abarcar más lugares en donde se requiera implementar seguridad y llevar una gestión centralizada del acceso, cabe mencionar que el sistema cuenta con un interfaz gráfico sencillo lo cual permite que sea más fácil la administración de la plataforma electrónica. Los sistemas de seguridad son costosos, y en muchos casos es difícil encontrar una opción que se adecue completamente a las necesidades, es por esto que se desarrolló una plataforma electrónica la cual servirá de base para implementar sistemas de seguridad robustos, utilizando solamente lo requerido y con la ventaja de ser escalabre a un futuro.

El prototipo de plataforma electrónica queda abierto a posibles modificaciones de capacidad del sistema, con la finalidad de siempre mejorar su funcionamiento y rendimiento. Una de sus posibles aplicaciones puede ser en el hogar, escuelas o en entornos corporativos; lugares en los que son frecuentados por muchas personas día con día, la plataforma electrónica brinda una base sólida la cual puede ayudar de soporte a sistemas de seguridad complementarios o ser adaptado a las necesidades del entorno que se desee instalar.

La mejora significativa permitirá agregar un grado más de seguridad, elevando considerablemente el grado de combinaciones posibles antes de llegar a la información original. La plataforma electrónica conserva la robustez de procesamiento y una alta respuesta en cuanto a la lectura a través de la cámara, todo lo anterior se traduce en eficiencia significativa en la gestión de acceso al personal e integridad de los datos almacenados para su posterior monitoreo. Cumpliendo

con la planeación esperada como unos de los objetivos principales del desarrollo tecnológico de la plataforma, que cada vez que se encontrará una falla o un área de oportunidad, se pudiera mejorar sin perder la esencia con la cual fue pensada.

Referencias

[1] Duc N. y Minh B. "*Your face is not your password face authentication by passing lenovo-asustoshiba*". Black Hat Briefings. Ha Noi University of Technology, Vietnam. (2009)
[2] Bhattacharyya D., Ranjan R., Alisherov F. y Choi M. "*Biometric Authentication: A Review*". In International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, p. 13–28. (2009)
[3] Murillo M., Cruz C., Abundiz F. y López R. "*Cifrado caótico de plantilla de huella dactilar en sistemas biométricos"*. Congreso Latinoamericano de Control Automático, pp. 18-23. (2014)
[4] Arboledas D. "*Criptografía sin secretos con Python".* Ra-Ma, Madrid, 1ra Edición. (2017)
[5] Kumar S.,y Kaur H. "*Face recognition techniques: Classification and comparisons*". In International Journal of Information Technology and Knowledge Management, 5(2), p. 361–363. (2012)
[6] Aceves M. y Ramos J. "*Fundamentos de Sistemas Embebidos –Mediante Lenguajes Descriptivos de Hardware*". Asociación Mexicana de Mecatrónica A.C., México, 1ra Edición. (2012)
[7] Zuriaga A. "*Estudio comparativo de las capacidades de Intel y ARM*". Tesis de Maestría, Universidad Carlos III de Madrid, España. (2014)
[8] Bay H., Ess A., Tuytelaars T. y Van Gool L. "*Speeded-up robust features (SURF)*". In Computer vision and image understanding, 110(3), p. 346–359. (2008)
[9] Junered M." *Face Recognition in Mobile Devices*". Master Thesis. Luleå University of Technology, Luleå, Suecia. (2010)
[10] Chao W." *Face Recognition*". GICE, National Taiwan University, Taiwan. (2010)