Criptosistema biométrico mediante la red vascular del dorso de la mano.

Trabajo Terminal No: 2020-A089

Alumnos: Antonio Cadena Genaro, Rodríguez Aguilar Kathia, Rodríguez Ron Daniel, Sánchez Aguilar Isaac.
Directores: Luna Benoso Benjamín, Silva García Víctor Manuel
**e-mail: daniel_rr08@icloud.com*

Resumen –
Se propone desarrollar un criptosistema biométrico mediante la red vascular del dorso de la mano para el cifrado de texto plano, utilizando los algoritmos de cifrado RSA y AES. Se obtendrá una imagen de la red vascular del dorso de la mano y será tratada mediante análisis de imágenes para obtener los rasgos de la misma. Con ellos se generará una llave criptográfica con RSA y después se usará junto con los principios de la teoría del caos para generar los parámetros que necesita el algoritmo de cifrado AES.

Palabras clave – AES, Criptosistema Biométrico, RSA, Teoría del caos.

1. Introducción

El reconocimiento biométrico como forma de autenticación e identificación se refiere al uso de características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como hablar, firmar o teclear). Estas características se denominan identificadores biométricos o rasgos biométricos, y sirven para reconocer automáticamente a los individuos [1]. El uso de los sistemas biométricos en la actualidad ha ido en aumento [10]. Algunos de estos son el reconocimiento de la huella digital, reconocimiento de la cara, reconocimiento de iris/retina, geometría de dedos/mano, autentificación de la voz y reconocimiento de la firma. Estos sistemas necesitan una base de datos en la que se guarda información por medio de un software especializado. La principal razón para tener una base de datos es poder comparar la información que se obtiene con la que está guardada. Una vez que se compare esta información se puede identificar a una persona.

Un criptosistema es una 5-tupla (P, C, K, E, D) que satisface las siguientes condiciones [11]:

1. P es un conjunto finito de posibles textos claros
2. C es un conjunto finito de posibles textos oscuros
3. K es el espacio de claves, es un conjunto finito de posibles claves
4. Para cada $K \in Q$, existe una regla de cifrado $eK \in E$ y una correspondiente regla de descifrado $R \in D$. Cada $eK : P \rightarrow C$ y $dK: C \rightarrow P$ son funciones tales que $dK(eK(x)) = x$ para todo texto claro $x \in P$.

Los criptosistemas biométricos son similares a los sistemas de generación de claves basados en contraseña, ya que se utilizan para asegurar o generar directamente la clave criptográfica a partir de características biométricas. Dado que las mediciones biométricas obtenidas durante la inscripción y las autenticaciones son diferentes, estas características no se pueden usar directamente para la generación de claves criptográficas. Para facilitar la generación de claves, los datos auxiliares o el boceto seguro de las características biométricas se almacenan durante la inscripción. Por lo tanto, los criptosistemas biométricos también se conocen como sistemas de datos auxiliares [2].

En este trabajo se planea crear un prototipo que, a partir de una imagen de la red vascular del dorso de la mano, trate la imagen para extraer patrones y crear una cadena de bits, la cual será cifrada utilizando el algoritmo RSA. Posteriormente la información cifrada será usada como parámetro en la Ecuación Mapa Logística (Principios de la Teoría del Caos) y generará once claves que utiliza el algoritmo AES. La finalidad de estas claves es cifrar texto plano con el algoritmo AES y con la llave única que se genera de cada persona. La llave será guardada y será de ayuda en el descifrado del texto plano.

A continuación, se presenta una tabla con ejemplos de sistemas similares.

Nombre	Características	Lugar	Año
Sistema de procesamiento de imágenes vasculares infrarrojas para aplicación en dispositivos biométricos de control de acceso [4]	-Utiliza análisis de patrones -Adquisición, preprocesamiento, reconocimiento y verificación de la imagen	Colombia	2014

Sistema de verificación biométrico vascular [5]	Registro y verificación de usuario utilizando el rasgo biométrico de la red vascular del dorso de la mano.	México, ESCOM	2012
Desarrollo de un Criptosistema Biométrico Basado en Firma Manuscrita [6]	Encriptación de rasgo biométrico de la firma usando AES como forma de autenticación.	España	2006
Implementación de un criptosistema de clave pública basado en una variedad algebraica y estudio de su espacio clave [7]	-Genera claves criptográficas, cifrar y descifrar archivos de texto utilizando el Criptosistema de Variedades Algebraicas. Conceptualización	Venezuela	2015
Criptosistema aplicado a la seguridad de cuentas bancarias basado en biometría del iris. [8]	- Un sistema que haga uso de la Encriptación Biométrica tomando como dato el iris de una persona.	México, ESCOM	2015
Criptosistema biométrico mediante la red vascular de la mano	Un criptosistema biométrico que utilice imágenes infrarrojas de la red vascular del dorso de la mano y genere una llave de acceso que se cifrará con ayuda de los principios de la teoría del caos y el algoritmo AES.	México, ESCOM	En proceso

2. Objetivo

Desarrollar un criptosistema biométrico mediante la red vascular del dorso de la mano.

Objetivos específicos:

-Obtener una imagen infrarroja del dorso de la mano.
-Diseñar un módulo de análisis y segmentación de las venas del dorso de la mano.
-Diseñar una metodología que genere una cadena a partir de la red vascular del dorso de la mano.
-Generar una llave criptográfica utilizando RSA a partir de la cadena de bits de las venas.
-Diseñar un módulo que encripte texto plano con AES, usando como llave secreta la generada en RSA y obteniendo las once claves que utiliza AES mediante la teoría del caos.
-Unificar todos los módulos anteriores para crear un criptosistema biométrico utilizando la red vascular del dorso de la mano.

3. Justificación

Actualmente el uso de sistemas biométricos es muy común en cualquier tipo de empresa, institución, etc., debido a que tiene muchas aplicaciones y proporciona un alto nivel de seguridad para restringir accesos, información, servicios o hasta dinero, permitiendo ingresar solo a personas que se encuentren registradas previamente. El desarrollo de nuevos sistemas que cumplan con la función de validación sigue en desarrollo y, además, se busca que represente un ahorro significativo y que sean seguros.

Los criptosistemas biométricos son una nueva tecnología que representa una poderosa herramienta en la seguridad de los sistemas de información, con esto también se han desarrollado sofisticados métodos de cifrado [3]. Dependiendo de la técnica biométrica empleada, los parámetros considerados son diferentes: los surcos de la huella dactilar, la geometría de la mano, la voz, la imagen facial, etc. De estos parámetros se extrae un patrón único de cada persona, que será el que se utilice para posteriores comparaciones.

Este tipo de tecnologías tiene muchas aplicaciones, como pueden ser: seguridad en movilidad y accesos, seguridad en transacciones (comercio electrónico y banca), seguridad en el acceso y firma de documentos electrónicos, seguridad en el acceso a equipos industriales, aplicaciones comerciales, reforzamiento de las infraestructuras de clave pública, así como aplicaciones gubernamentales. [2]

4. Productos o Resultados esperados

A continuación, se muestra el diagrama de arquitectura del sistema:

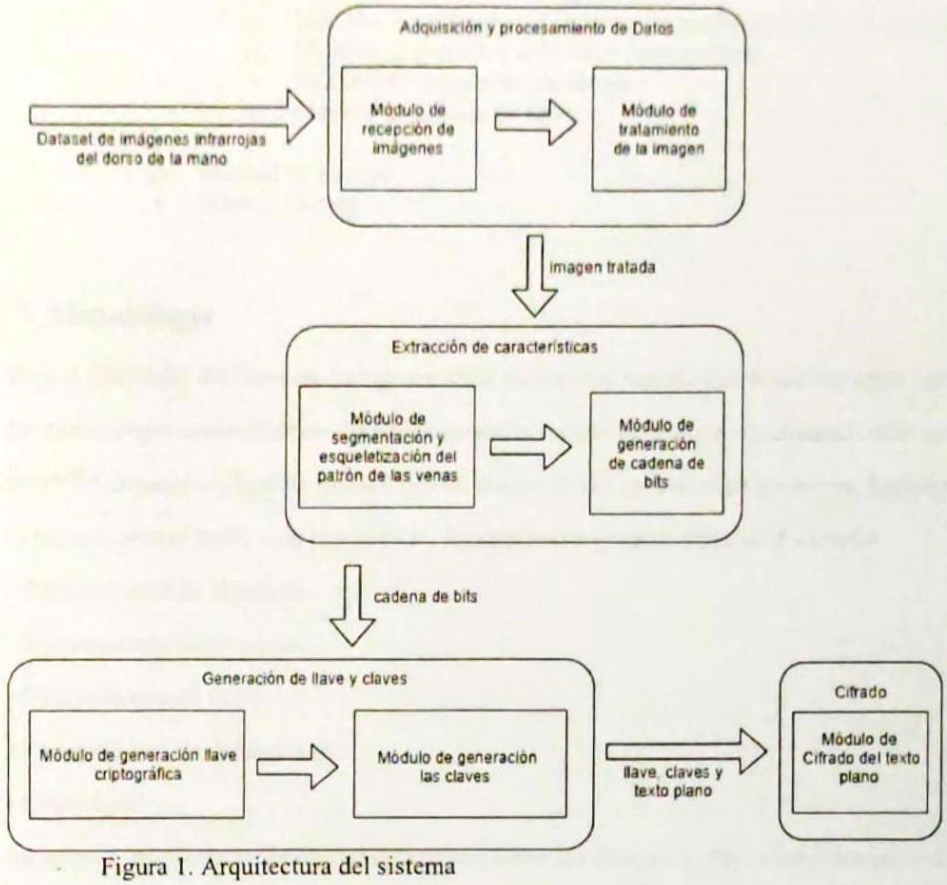

Figura 1. Arquitectura del sistema

Módulo de recepción de imágenes: Obtiene y recibe las imágenes infrarrojas de la red vascular del dorso de la mano.

Módulo de mejoramiento de imagen: Trata las imágenes tomadas para eliminar el ruido en ellas y obtener una imagen más estilizada y manejable para su posterior uso.

Módulo de segmentación y esqueletización del patrón de las venas: Obtiene las características que se reconocieron de las venas.

Módulo de generación de cadena de bits: Algoritmo que genera una llave a partir de las características y de la información que se obtuvieron en los módulos anteriores.

Módulo de generación de llave criptográfica: Genera una llave criptográfica a partir de la cadena de bits, con ayuda del algoritmo de cifrado RSA.

Módulo de generación de claves: Tomando en cuenta la llave criptográfica generada, crea claves con los principios de la teoría del caos, específicamente con la ecuación de mapa logístico.

Módulo de cifrado: Cifra el texto plano con ayuda de las claves y la llave criptográfica, utilizando el algoritmo de cifrado AES.

Tomando en cuenta el tiempo de desarrollo, a continuación, se presentan los productos esperados del presente trabajo terminal:

1. Prototipo de criptosistema biométrico generador de llave cifrada.

i. Módulo de visualización y captura de imágenes.
ii. Módulo de mejoramiento de imagen.
iii. Módulo de segmentación y esqueletización del patrón de las venas.
iv. Módulo de generación de llave criptográfica.
v. Módulo de generación de claves.
vi. Módulo de cifrado de llave.

2. Manual de usuario
3. Manual técnico

5. Metodología

Para el desarrollo del presente trabajo terminal se propone basarnos en la metodología ágil SCRUM.

La metodología constará de un desarrollo modular basado en historias de usuario como lo marca SCRUM, durante los Sprints (iteraciones de desarrollo del proyecto) se generarán ligeros prototipos como lo marca el modelo de prototipado, siguiendo el siguiente orden de desarrollo:

• Planteamiento de objetivos.

• Planteamiento de alcances.

• Planteamiento de valor.

• Planteamiento de dependencias

• Check List.

Los puntos anteriores serán discutidos en conjunto a los directores. Posteriormente procederemos a desarrollar un "prototipo" basado en el diseño anterior, bajo el siguiente esquema:

• Maquetado.

• Prueba de concepto.

• Validación.

• Desarrollo

• Codificación.

• Documentación.

• Pruebas

Posterior a esto se continuará de forma iterativa hasta cumplir con el proyecto.

6. Cronograma

Nombre del alumno(a): Antonio Cadena Genaro TT No.:
Título del TT: Prototipo de Criptosistema biométrico mediante la red vascular de la mano derecha.

Actividad	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Sprint 1 Análisis del sistema											
Introducción y estado del arte											
Marco teórico											
Análisis de riesgos											
Estudios de factibilidad.											
Análisis de requerimientos y casos de usos											
Correcciones											
Sprint 2 Diseño y desarrollo											
Diagrama de bloques											
Diagrama de clases											
Diagrama de secuencia											
Descripción del desarrollo											
Correcciones											
Preparación de la presentación de TT1											
Presentación de TT 1											
Sprint 3 Programación de los módulos											
Módulo de visualización y captura de imágenes.											
Módulo de mejoramiento de imagen											
Módulo de segmentación y esqueletización del patrón de venas											
Módulo de generación de llave única de autentificación											
Módulo de generación de claves											
Módulo de cifrado											
Pruebas unitarias											
Corrección de incidencias											
Sprint 4 Pruebas y Resultados											
Manual de usuario											
Manual Técnico											
Pruebas de todos los módulos en conjunto											
Resultados y corrección de incidencias.											
Preparación de la presentación de TT2											
Presentación de TT 2											

Nombre del alumno(a): Rodríguez Aguilar Kathia TT No.:
Título del TT: Prototipo de Criptosistema biométrico mediante la red vascular de la mano derecha.

Actividad	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Sprint 1 Análisis del sistema											
Introducción y estado del arte											
Marco teórico											
Análisis de riesgos											
Estudios de factibilidad.											

Análisis de requerimientos y casos de usos											
Correcciones											
Sprint 2 Diseño y desarrollo											
Diagrama de bloques											
Diagrama de clases											
Diagrama de secuencia											
Descripción del desarrollo											
Correcciones											
Preparación de la presentación de TT1											
Presentación de TT 1											
Sprint 3 Programación de los módulos											
Módulo de visualización y captura de imágenes.											
Módulo de mejoramiento de imagen											
Módulo de segmentación y esqueletización del patrón de venas											
Módulo de generación de llave única de autentificación											
Módulo de generación de claves											
Módulo de cifrado											
Pruebas unitarias											
Corrección de incidencias											
Sprint 4 Pruebas y Resultados											
Manual de usuario											
Manual Técnico											
Pruebas de todos los módulos en conjunto											

Resultados y corrección de incidencias.											
Preparación de la presentación de TT2											
Presentación de TT 2											

Nombre del alumno(a): Rodríguez Romo Luis Daniel TT No.:
Título del TT: Prototipo de Criptosistema biométrico mediante la red vascular de la mano derecha.

Actividad	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Sprint 1 Análisis del sistema											
Introducción y estado del arte											
Marco teórico											
Análisis de riesgos											
Estudios de factibilidad.											
Análisis de requerimientos y casos de usos											
Correcciones											
Sprint 2 Diseño y desarrollo											
Diagrama de bloques											
Diagrama de clases											
Diagrama de secuencia											
Descripción del desarrollo											
Correcciones											
Preparación de la presentación de TT1											
Presentación de TT 1											
Sprint 3 Programación de los módulos											
Módulo de visualización y captura de imágenes.											
Módulo de mejoramiento de imagen											
Módulo de segmentación y esqueletización del patrón de venas											
Módulo de generación de llave única de autentificación											
Módulo de generación de claves											
Módulo de cifrado											
Pruebas unitarias											

Corrección de incidencias											
Sprint 4 Pruebas y Resultados											
Manual de usuario											
Manual Técnico											
Pruebas de todos los módulos en conjunto											
Resultados y corrección de incidencias.											
Preparación de la presentación de TT2											
Presentación de TT 2											

Nombre del alumno(a): Sánchez Aguilar Isaac TT No.:
Título del TT: Prototipo de Criptosistema biométrico mediante la red vascular de la mano derecha.

Actividad	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Sprint 1 Análisis del sistema											
Introducción y estado del arte											
Marco teórico											
Análisis de riesgos											
Estudios de factibilidad.											
Análisis de requerimientos y casos de usos											
Correcciones											
Sprint 2 Diseño y desarrollo											
Diagrama de bloques											
Diagrama de clases											
Diagrama de secuencia											
Descripción del desarrollo											
Correcciones											
Preparación de la presentación de TT1											
Presentación de TT 1											
Sprint 3 Programación de los módulos											
Módulo de visualización y captura de imágenes.											
Módulo de mejoramiento de imagen											
Módulo de segmentación y esqueletización del patrón de venas											

Módulo de generación de llave única de autentificación											
Módulo de generación de claves											
Módulo de cifrado											
Pruebas unitarias											
Corrección de incidencias											
Sprint 4 Pruebas y Resultados											
Manual de usuario											
Manual Técnico											
Pruebas de todos los módulos en conjunto											
Resultados y corrección de incidencias.											
Preparación de la presentación de TT2											
Presentación de TT 2											

7. Referencias

[1] F. Serratosa. "La biometría para la identificación de las personas". Universitat Oberta de Catalunya. PID_00195448

[2] León P., Susan K. "Avances en ténicas biométricas y sus aplicaciones en seguridad". Universidad de Caraboro, Venezuela, 2011.

[3] J. Nair.B.J. "A Review on Biometric Cryptosystems". IJLTET, vol. 6, 2015.

[4] C. Cortés. "Sistema de procesamiento de imágenes vasculares infrarrojas para aplicación en dispositivos biométricos de control de acceso". Tekhne, vol. 12, pp. 13-22, 2015.

[5] E. Carrasco, D. Fuentes, C. Benitez, F. Hernández."Sistema de verificación biométrico vascular". Trabajo Terminal. Escom, IPN. CDMX, 2012.

[6] M. Freire. "Desarrollo de un sistema criptobiométrico basado en firma manuscrita". Universidad Antonio de Nebrija, España, 2006.

[7] J. Contreras. "Implementación de un criptosistema de clave pública basado en una variedad algebraica y estudio de su espacio clave".2015

[8] J. Fuentes, G. Moreno. "Criptosistema aplicado a la seguridad de cuentas bancarias basado en biometría del iris". Tesis. ESCOM, Instituto Politécnico Nacional. 2015.

[9] Instituto nacional de ciberseguridad (2016). Tecnologías biométricas aplicadas a la ciberseguridad[Online] Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

[10] Saeed, K. (2017). New directions in behavioral biometrics. CRC Press

[11] L Ayestarán."Introducción a la criptografía". Trabajo de fin de grado. Facultad de Ciencia y Tecnología, Universidad de la Rioja. Logroño, 2016.

[12] R. Álvarez."Aplicación de las matrices por bloques a los criptosistemas de cifrado por flujo". Tesis Doctoral. Universidad de Alicante. España, 2005.

[13] A. Hernández."Teoría del caos y criptografía". Tesis . Facultad de matemática y computación, Universidad de La Habana. Cuba, 2014.

8. Alumnos y Directores

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Art. 3, fracc. II, Art. 18, fracc. II y Art. 21, lineamiento 32, fracc. XVII de la L.F.T.A.I.P.G.
PARTES CONFIDENCIALES: No. de boleta y Teléfono.

Genaro Antonio Cadena. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2015630029, Tel.5545111896, email genaroantonioc@hotmail.com

Firma:_____

Rodríguez Aguilar Kathia. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2013630372, Tel.5518654468, email: kath_rodagui@outlook.com

Firma:_____

Rodríguez Romo Luis Daniel. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2014071385, Tel.5544939084, email: daniel_rr08@icloud.com

Firma:_____

Sánchez Aguilar Isaac. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2016630523, Tel.5612979803, email saais31@gmail.com

Firma:_____

Luna Benoso Benjamín. - Licenciado en Física y Matemáticas, egresado de la ESFM, IPN. Maestro en Ciencias de la Computación. Doctor en Ciencias de la Computación, egresado del Centro de Investigación en Computación del IPN. Profesor de tiempo completo en ESCOM/IPN. Áreas de Interés: Bases de Datos, Big Data, minería de datos, desarrollo de sistemas Web. Email: mobius_95@hotmail.com

Firma:_____

Silva García Víctor Manuel. - Doctor en Ciencias de la Computación. ESFM Licenciado en Física y Matemáticas. Maestría en Computación y Estadística en el Colegio de Postgraduados, Universidad Autónoma de Chapingo. Egresado de ESFM, IPN. Áreas de Interés: Criptografía y seguridad informática. Email: vsilvag@ipn.mx

Firma:_____