



**UNIVERSIDAD
NACIONAL
DE LOJA**



**Facultad de la Energía, las Industrias y los Recursos Naturales No
Renovables**

CARRERA DE INGENIERÍA EN SISTEMAS

"Revisión Sistemática de Literatura: Vulnerabilidad de sistemas biométricos basados en huellas dactilares"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO
DE INGENIERA EN SISTEMAS

Autor:

Ximena Vanessa Tapia Jaramillo

Director

Ing. Jorge Tulio Carrión Gonzalez, Mg. Sc.

LOJA-ECUADOR

2017

Certificación del director

Ing. Jorge Tulio Carrión Gonzalez, Mg. Sc. en calidad de director del trabajo de titulación designado por disposición de la coordinación de la carrera de Ingeniería en Sistemas, certifico que el Egresada Ximena Vanessa Tapia Jaramillo, ha culminado el trabajo de titulación, con el tema **“REVISIÓN SISTEMÁTICA DE LITERATURA: VULNERABILIDAD DE SISTEMAS BIOMÉTRICOS BASADOS EN HUELLAS DACTILARES”**, quien ha cumplido con todos los requisitos legales exigidos por los que se aprueba la misma. Es todo cuanto puedo decir en honor a la verdad, facultando al interesado hacer uso de la presente, así como también se autoriza la presentación para la evaluación por parte del jurado respectivo.

05 de junio de 2017

Atentamente,



Ing. Jorge Tulio Carrión Gonzalez, Mg. Sc.

DIRECTOR DE TESIS

Autoría

Yo **XIMENA VANESSA TAPIA JARAMILLO** declaro ser autora del presente trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma: 

Cédula: 1104462856

31 de Agosto de 2017

**CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTORA,
PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y
PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.**

Yo **XIMENA VANESSA TAPIA JARAMILLO**, declaro ser autor de la tesis titulada:
**“REVISIÓN SISTEMÁTICA DE LITERATURA: VULNERABILIDAD DE SISTEMAS
BIOMÉTRICOS BASADOS EN HUELLAS DACTILARES”**; autorizo al Sistema
Bibliotecario de la Universidad Nacional de Loja para que con fines académicos,
muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad
de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de
información del país y del exterior, con las cuales tenga convenio con la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis
que realice un tercero.

Para constancia de esta autorización en la ciudad de Loja a los treintay un días del
mes de agosto del dos mil diez y siete.

Firma: 

Autor: Ximena Vanessa Tapia Jaramillo

Cédula: 1104462856

Dirección: Alamor (Río Amazonas y Guayaquil)

Correo Electrónico: ximena.tapia.cbpl@gmail.com

Teléfono: 073033267 **Celular:** 0959020466

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Jorge Tulio Carrión Gonzalez, Mg. Sc.

Tribunal de Grado: Ing. Jorge Iván Tocto, Mg. Sc.

Ing. Boris Marcel Díaz Pauta, MBA

Ing. Roberto Carlos Pineda López, Mg. Sc.

Dedicatoria

Dedico este trabajo al Niño Santo que me ha iluminado siempre en todo momento, ya que siempre ha escuchado mis suplicas para superarme en la vida estudiantil y diaria.

De manera muy especial a mi esposo que amo tanto Ing. Patricio Padilla quien me ha apoyado en todo momento dándome ánimos, fuerza, valor y alegría a mis días con su paciencia y dedicación para nuestras hijas Ashley Tamara y Danna Mishell Padilla Tapia que han tenido que soportar mi ausencia, viajes consecutivos, pero para ustedes este logro que nos llenará de emoción y tranquilidad para poder seguir adelante académicamente y así buscar un mejor futuro.

A mis padres Lic. Irma Jaramillo y Victor Tapia les dedico este trabajo ya que gracias a sus enseñanzas y ejemplo en valores, respeto, responsabilidad he podido culminar mi carrera ya que siempre me han apoyado para conseguir este logro tan anhelado.

Ximena Vanessa Tapia Jaramillo

Agradecimiento

Mi agradecimiento en primer lugar a Dios y al Niño Santo que iluminaron mi camino, mente y alma para poder realizar el presente Trabajo de Titulación.

Así mismo al director de tesis asignado para dirigir la tesis el Ing. Jorge Tulio Carrión Mg. mi más amplio agradecimiento por haberme recibido en las instalaciones de la Universidad Nacional de Loja, específicamente en el Área de Energía Industrias y Recursos Naturales no Renovables para compartir su conocimiento, ideas, criterios y sugerencias que lograban dirigirme de la mejor manera, dedicándome su tiempo y paciencia para la realización del presente Trabajo.

De manera muy especial le agradezco a mi esposo Ing. Patricio Padilla por apoyarme incondicionalmente siempre y en todo momento tanto emocional como económicamente, dándome la fuerza, consejos e ideas para continuar y lograr este objetivo tan anhelado, a mis hijas que han soportado y entendido mi ausencia para poder superarme cada día.

Todo esto no hubiera sido posible sin el amparo y cariño que me otorgaron mis padres, hermanas y hermano por darme ánimos, seguridad, ejemplo de perseverancia y dedicación, ya que de forma incondicional entendieron mi ausencia y malos momentos, que a pesar de la distancia siempre estuvieron a mi lado para saber cómo iba mi proceso, las palabras nunca serán suficientes para testimoniar mi aprecio y agradecimiento.

A todos ustedes, mi mayor reconocimiento y gratitud.

Índice

Certificación del director	ii
Autoría	iii
CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTORA.....	iv
Dedicatoria	v
Agradecimiento	vi
Índice.....	vii
Índice de Figuras	xi
Índice de Tablas.....	xii
A. TÍTULO	14
B. RESUMEN	15
Abstract.....	16
C. INTRODUCCIÓN	17
D. REVISIÓN DE LITERATURA	20
CAPÍTULO 1.- SISTEMA BIOMÉTRICO	20
1.1. Características y tipología de las Tecnologías Biométricas	20
1.2. Arquitectura de un Sistema Biométrico para Identificación Personal.....	22
CAPÍTULO 2.- TECNOLOGÍAS BIOMÉTRICAS	24
2.1. Tecnologías biométricas fisiológicas	24
2.1.1. Huella dactilar.....	24
2.1.2. Reconocimiento facial.....	26
2.1.3. Reconocimiento de iris.....	27
2.1.4. Reconocimiento de la geometría de la mano.....	29

2.1.5. Reconocimiento de retina	30
2.1.6. Reconocimiento vascular	31
2.2. Otras formas de biometría fisiológica	31
2.3. TECNOLOGÍAS BIOMÉTRICAS DE COMPORTAMIENTO	32
2.3.1. Reconocimiento de firma	32
2.3.2. Reconocimiento de escritor	33
2.3.3. Reconocimiento de voz.....	33
2.3.4. Reconocimiento de escritura de teclado	34
2.3.5. Reconocimiento de la forma de andar.....	35
CAPÍTULO 3.- BENEFICIOS DEL USO DE TECNOLOGÍAS BIOMÉTRICAS.....	37
3.1. Para las organizaciones y usuarios finales	37
3.2. USOS Y APLICACIONES	37
3.3. APLICACIONES ACTUALES DE LAS TECNOLOGÍAS BIOMÉTRICAS CON DETECCIÓN DE HUELLA DACTILAR	38
3.3.1. Control de accesos físicos y lógicos.....	38
3.3.2. Control de presencia	38
CAPÍTULO 4.- MÉTODOS DE ATAQUE	40
4.1. Métodos de ataque a la biometría de reconocimiento de Huellas Dactilares.....	40
4.1.2. Ataque al canal entre el sensor y el extractor de características	43
4.1.3. ATAQUES AL EXTRACTOR DE CARACTERÍSTICAS	43
4.1.4. Ataques al canal entre el extractor de características y el comparador	43
4.1.5. Ataques al comparador.....	44
4.1.6. ATAQUES A LA BASE DE DATOS.....	44
CAPÍTULO 5.- ALGORITMOS DE ATAQUE	46
5.1. Ataque mediante el algoritmo hill-climbing.....	46
5.2. ATAQUES MEDIANTE ALGORITMO SIDE-CHANNEL	49

5.2.1. <i>Basados en tiempo: Timing-Attacks</i>	50
CAPÍTULO 6.- REVISIONES BIBLIOGRÁFICAS	51
6.1. DEFINICIÓN	51
6.2. CLASIFICACIÓN DE LAS REVISIONES BIBLIOGRÁFICAS	51
6.3. SELECCIÓN DE LA REVISIÓN DEL ESTADO DEL ARTE	52
E. MATERIALES Y MÉTODOS	60
1.MATERIALES	60
2.MÉTODOS	62
1. <i>Planificación de la revisión.</i>	62
1.1. <i>Identificación de la necesidad de una revisión</i>	62
1.2. <i>Especificación de las preguntas de investigación</i>	62
1.3. <i>Desarrollo de un protocolo de revisión</i>	63
2. <i>Desarrollo de revisión.</i>	64
2.1. <i>Identificación de la investigación.</i>	64
2.2. <i>Selección de estudios primarios.</i>	65
2.3. <i>Extracción de datos y seguimiento.</i>	67
2.4. <i>Síntesis de datos.</i>	67
F. RESULTADOS	70
1. EXTRACCIÓN DE DATOS	70
2. SÍNTESIS DE DATOS.	87
G. DISCUSIÓN	89
1. DISCUSIÓN DE LA REVISIÓN SISTEMÁTICA	89
2. DESARROLLO DE LA PROPUESTA ALTERNATIVA	92
2.1. PLANIFICAR LA REVISIÓN BIBLIOGRÁFICA PARA OBTENER INFORMACIÓN PRIMARIA	92
2.2. REALIZAR UN PROCESO DE REVISIÓN SISTEMÁTICA PARA ESTUDIOS PRIMARIOS.	92

2.3. ANALIZAR LOS ALGORITMOS DE ATAQUE A LA VULNERABILIDAD DE LOS SISTEMAS BIOMÉTRICOS BASADOS EN HUELLAS DACTILARES.	93
2.4. SINTETIZAR LA INFORMACIÓN RECOPIADA EN LA REVISIÓN SISTEMÁTICA. ..	93
3. VALORACIÓN SOCIAL, TÉCNICA, ECONÓMICA Y CIENTÍFICA	94
3.1. VALORACIÓN SOCIAL	94
3.2. VALORACIÓN TÉCNICA	94
3.3. VALORACIÓN ECONÓMICA.....	94
3.4. VALORACIÓN CIENTÍFICA.....	94
H. CONCLUSIONES	95
I. RECOMENDACIONES	97
J. BIBLIOGRAFÍA.....	98
K. ANEXOS.....	101

Índice de Figuras

Figura 1. Esquema de Trabajo de Titulación	18
Figura 2. Arquitectura de un Sistema Biométrico para identificación personal.	22
Figura 3. Huella Dactilar	24
<i>Figura 4. Patrones de huella dactilar</i>	<i>25</i>
Figura 5. Estructura de una Huella dactilar	25
Figura 6. Algunos tipos de crestas.....	26
Figura 7. Reconocimiento facial.....	26
Figura 8. Reconocimiento de iris.....	27
Figura 9. Geometría de la mano	29
Figura 10.Reconocimiento de retina	30
Figura 11.Reconocimiento vascular.....	31
Figura 12.Reconocimiento de firma	32
Figura 13.Reconocimiento de voz.....	33
Figura 14.Reconocimiento de escritura de teclado	34
Figura 15.Reconocimiento de la forma de andar.....	35
Figura 16.Potenciales puntos de ataque a un sistema de reconocimiento biométrico. 41	
Figura 17.Imágenes de huellas y caras sintéticas generadas con los programas.	42
Figura 18.Ataque hill-climbing tipo 4 basado en puntuación.....	46
Figura 19.Artículos por base de datos	67
Figura 20.Artículos seleccionados por año.....	87

Índice de Tablas

Tabla 1. Comparación de tecnología biométrica según sus características	36
Tabla 2. Nomenclatura algoritmo Hill-Climbing	46
Tabla 3. Protocolo de Barbara Kitchenham	55
Tabla 4. Materiales	60
Tabla 5. Preguntas de Investigación	63
Tabla 6. Bases de datos científicas	64
Tabla 7. Revisión preliminar y términos	65
Tabla 8. Resultados del fase de selección de artículos incluidos y excluidos.	66
Tabla 9. <i>Resultados del artículo A01</i>	70
Tabla 10. Resultados del artículo A02	71
Tabla 11. Resultados del artículo A03	72
Tabla 12. Resultados del artículo A04	73
Tabla 13. Resultados del artículo A05	74
Tabla 14. Resultados del artículo A06	75
Tabla 15. Resultados del artículo A07	77
Tabla 16. Resultados del artículo A08	77
Tabla 17. Resultados del artículo A09	79
Tabla 18. Resultados del artículo A10	80
Tabla 19. Resultados del artículo A11	81
Tabla 20. Resultados del artículo A12	82

Tabla 21. Resultados del artículo A13	83
Tabla 22. Resultados del artículo A14	85
Tabla 23. Resultados de selección de estudios primarios.....	87
Tabla 24. Artículos Revisados.....	101

a. Título

"Revisión Sistemática de Literatura: Vulnerabilidad de sistemas biométricos basados en huellas dactilares"

b. Resumen

Un sistema de autenticación biométrico utiliza las características fisiológicas (como huellas digitales, rostro, características de la mano, iris) y/o características conductuales (como la voz, la firma, el andar, la forma de escribir) de un individuo para identificar su identidad. Existen muchos métodos biométricos de identificación de individuos, el más usado es mediante la huella digital. Es por ello que el propósito del presente trabajo de titulación es analizar las vulnerabilidades que presentan los sistemas de reconocimiento biométrico basados en huella dactilar, ya que existen diferentes técnicas de ataque, que permiten el acceso mediante la falsificación de patrones dactilares. Para ello se desarrolló una Revisión Sistemática usando las bases de datos IEEE, Science Direct y Google Scholar encontrando bajo ciertos criterios de inclusión y exclusión artículos científicos así como de trabajos realizados, ya que en base al protocolo de Bárbara Kitchenham se lograron estudios que demuestran que existen formas de atacar a los diferentes niveles de procesamiento de identificación y verificación de las huellas dactilares, por lo que se abordará algoritmos de ataque de software como el Hill – Climbing y Side – Channel los cuales consisten en la generación de patrones de características para huellas dactilares aleatorios que son modificados iterativamente hasta alcanzar una similitud deseada con respecto a una huella real para lograr ser aceptado por un sistema de verificación.

Abstract

A biometric authentication system uses the physiological characteristics (such as fingerprints, face, hand features, iris) and / or behavioral characteristics (such as voice, signature, walking, writing) of an individual to identify their identity. There are many biometric methods of identifying individuals, the most used is through the fingerprint. This is why the purpose of the present titling work is to analyze the vulnerabilities of fingerprint based biometric recognition systems, since there are different attack techniques that allow access by means of the falsification of fingerprints. For this, a Systematic Review was developed using the IEEE, Science Direct and Google Scholar databases, finding, under certain criteria of inclusion and exclusion, scientific articles as well as of the work done, since, based on the protocol of Barbara Kitchenham, studies were obtained showing that There are ways to attack the different levels of processing of identification and verification of fingerprints, which will address software attack algorithms such as Hill - Climbing and Side - Channel which consist of the generation of pattern patterns for fingerprints Random fingerprints that are iteratively modified to achieve a desired similarity with respect to a real footprint in order to be accepted by a verification system.

c. Introducción

La identificación por huella dactilar es un método de identificación, además de ser el más usado en la actualidad por las organizaciones públicas y privadas a nivel mundial. La huella digital en los seres humanos se caracteriza por tener unos patrones que las hace diferentes a los demás, está basado en características particulares de cada ser humano las cuales no son cambiantes con el paso del tiempo, por lo anterior es que las empresas lo que buscan es entrar el mundo de la seguridad utilizando el método de identificación dactilar no solo para la protección de recursos tangibles e intangibles que son el activo vital para el buen funcionamiento de la organización y su competitividad en el mercado mundial[1].

La seguridad de la información es importante ya que es la esencia primordial de las compañías su cuidado y protección debe ser de manera adecuada, oportuna para evitar ser extraída de personas internas y externas que pueden utilizarla para causar daños irreparables o acaben con la continuidad de la organización. En las empresas son múltiples las vulnerabilidades a las que están expuestas es así, que las empresas están adquiriendo control de acceso biométricos cada vez más avanzados con características particulares para evitar suplantación, restringir el acceso a personas no autorizadas a zonas de carácter restringido por el tipo de actividades que allí se desarrollen, la información que se guarda, para prevenir y detectar cualquier situación que altere el normal funcionamiento de los procesos de la compañía.

Un complemento importante y alternativo en los controles de acceso biométricos dactilares es la utilización de hardware y software, lo que permiten verificar la identidad del usuario con un parámetro ya almacenado propio de esta persona en este caso la huella dactilar. Es por esto que en el presente Trabajo de Titulación se desarrolló una Revisión Sistemática sobre la Vulnerabilidad de sistemas biométricos basados en huellas dactilares, desde el punto de vista en seguridad, para la ejecución de esta se basó en las “Guidelines for performing Systematic Literature Reviews in Software Engineering” de Bárbara Kitchenham[2], el mismo que es un proceso desarrollado para identificar lo medular de una Revisión de la literatura de interés, realizando la búsqueda y extracción de lo más relevante acorde a criterios que han sido evaluados y respetados por otros[3].

El presente Trabajo de Titulación versa sobre el tema “Vulnerabilidad de sistemas biométricos basados en huellas dactilares”, el cual tiene como finalidad desarrollar una Revisión Sistemática de Literatura de acuerdo a:

- ✓ ¿Cuáles son las formas de falsificación de huellas digitales utilizadas para vulnerar sistemas biométricos?
- ✓ ¿En que se basan los algoritmos utilizados para identificación de falsificación de huellas dactilares en sistemas biométricos?
- ✓ ¿Qué algoritmos para identificación de falsificación de huellas dactilares en sistemas biométricos ha dado mejores resultados?

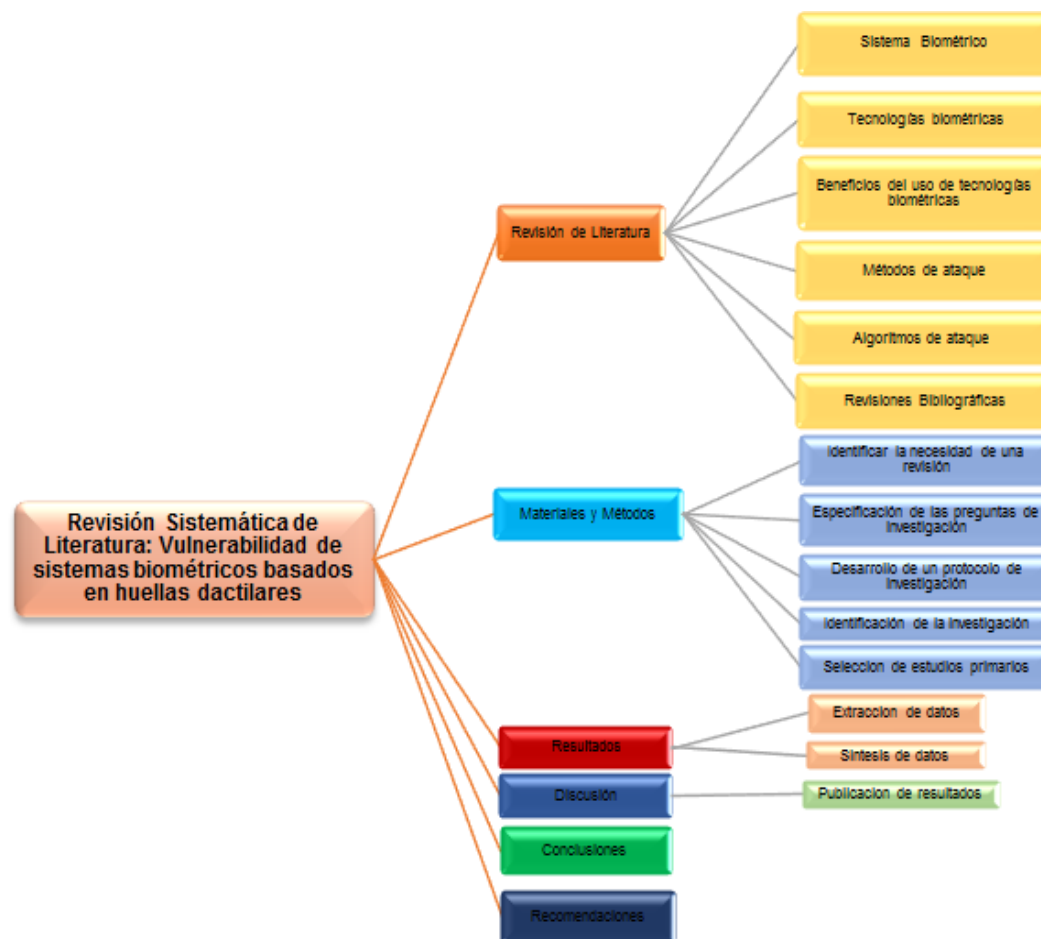


Figura 1. Esquema de Trabajo de Titulación

Como se puede observar en la Figura 1, en la Revisión de la Literatura se elaboró seis capítulos que ayudaron a sustentar los conocimientos de esta área de estudio, en el apartado de Materiales y Métodos se describió todas las herramientas utilizadas tanto

de Hardware, software y recursos de oficina, luego se desarrolló el método (Revisión Sistemática) para la selección de los estudios primarios, a continuación en el apartado de Resultados se presentó todos los datos relevantes obtenidos del análisis de los artículos seleccionados, en el apartado de Discusión se expresó un análisis de la Revisión Sistemática en base a los resultados y además presentó como se cumplió con los objetivos, en el apartado de Conclusiones se expresó las ideas más relevantes que se rescató luego de la revisión y por último en el apartado de Recomendaciones se planteó aspectos a considerar para el desarrollo de futuros trabajos.

d. Revisión de literatura

Capítulo 1.- Sistema Biométrico

La biometría es un término utilizado para referir a los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas[4]. Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar. En la actualidad, la tecnología ha permitido automatizar y perfeccionar estos procesos de reconocimiento biométrico, de forma que tienen multitud de aplicaciones y finalidades especialmente aquellas relacionadas con la seguridad[5].

1.1. Características y tipología de las Tecnologías Biométricas

Para que las características físicas y conductuales sean utilizadas como elementos de identificación deben cumplir con los siguientes requisitos[5]:

- a) Universalidad:** Todas las personas tienen o presentan una característica.
- b) Singularidad:** Dos personas cualesquiera son distinguibles una de la otra en base de sus características.
- c) Estabilidad:** La característica tiene que ser lo suficientemente estable a lo largo del tiempo y en condiciones ambientales diversas.
- d) Cuantificable:** La característica tiene que ser medible cuantitativamente.
- e) Aceptabilidad:** El nivel de aceptación de la característica por parte de las personas debe ser suficiente como para ser considerada parte del sistema de identificación biométrico.
- f) Rendimiento:** El nivel de exactitud requerido debe ser elevado para que la característica sea aceptable.
- g) Usurpación:** Permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas.

El objetivo de usar características biométricas es poseer un conjunto de herramientas que permitan obtener la identificación y verificación de la identidad de una persona.

Y las tecnologías para medir estas características deben proporcionar:

- ✓ Rendimiento: nivel de exactitud
- ✓ Aceptación: por parte del usuario
- ✓ Resistencia al fraude y usurpación

Generalmente para poder ser usado los individuos deben registrar su identidad en el sistema por medio de la captura de una serie de parámetros biométricos. Este es el denominado proceso de registro, que se compone de tres fases distintas:

- ✓ Captura de los parámetros biométricos.
- ✓ Procesamiento en donde se crea una plantilla con las características personales de los parámetros capturados.
- ✓ Inscripción de la plantilla procesada guardándola en un medio de almacenamiento adecuado. Una vez que la inscripción está completa, el sistema puede autenticar a las personas mediante el uso de la plantilla.

Fundamentalmente se distinguen dos grupos de tecnologías biométricas en función de la metodología utilizada aquellas que analizan características fisiológicas de las personas y aquellas que analizan su comportamiento.

Por otra parte dependiendo de qué tecnologías utilizan los sistemas de identificación biométrica se dividen en:

- ✓ **Estática:** Es el estudio de las características físicas del ser humano, es decir utilizan tecnologías fisiológicas que miden y comparan rasgos físicos. A esta clasificación pertenecen las características de: huella dactilar, ojo, retina, iris, líneas de la mano, geometría de la mano, geometría facial, características de la cara, poros de la piel[4].
- ✓ **Dinámica:** Estudia las características de la conducta del ser humano, es decir utilizan tecnologías de comportamiento que comparan acciones o movimientos

como: pertenecen las características: manuscrito, firma, voz, tecleo, gestos o movimiento corporal[4].

- ✓ **Multimodales:** Combinan técnicas estáticas y dinámicas.

1.2. Arquitectura de un Sistema Biométrico para Identificación Personal

Los Dispositivos Biométricos poseen tres Componentes Básicos:

- ✓ El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner.
- ✓ El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos, Con los datos almacenados.
- ✓ El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema.



Figura 2. Arquitectura de un Sistema Biométrico para identificación personal[1].

En la Figura 2 puede entenderse conceptualmente como dos módulos[6]:

- ✓ **Módulo de inscripción** (enrollment module) Figura 2: se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al

sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características. El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u otro medio como una tarjeta magnética, recibirá el nombre de template (Plantillas).

En otras palabras un template es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

- ✓ **Módulo de identificación** (identification module) Figura 2: es el responsable del reconocimiento de individuos, ya que este módulo se encarga de establecer la identidad del individuo que accede al sistema. Para ello, tras la adquisición del rasgo biométrico del individuo, se extraen las características y se obtiene el patrón biométrico que posteriormente, es comparado con los patrones almacenados en la base de datos. Los resultados de dichas comparaciones son cuantificados y valorados, permitiendo así la toma de decisiones respecto a la identidad del individuo en función del grado de similitud obtenido. Por ejemplo en una aplicación de control de acceso.

Capítulo 2.- Tecnologías biométricas

2.1. Tecnologías biométricas fisiológicas

Las tecnologías biométricas se definen como métodos automáticos utilizados para reconocer a personas sobre la base del análisis de sus características físicas del usuario[7].

2.1.1. Huella dactilar



Figura 3. Huella Dactilar

Huella dactilar o fingerprint en inglés de la figura 3, es una característica biométrica de tipo morfológico, la huella dactilar se basa en la presencia de un conjunto de líneas genéricas llamadas crestas, son partes donde la piel se eleva sobre las zonas más bajas (valles), siendo el ancho de los valles de 2 a 5 décimas de milímetro.

La identificación basada en huella dactilar es la más antigua de las técnicas biométricas y ha sido utilizada en un gran número de aplicaciones debido a que se considera que las huellas dactilares son únicas e inalterables. El usuario sitúa la yema de un dedo normalmente el índice sobre un escáner de huella.

Es el rasgo biométrico más utilizado para autenticación. Se han desarrollado una amplia gama de tecnologías de captura, con distintas características de funcionamiento. Así mismo, tiene como ventajas su alta tasa de precisión y su facilidad de uso[8], en la figura 4, se muestra diferentes patrones de huellas dactilares, ya que todas las personas poseemos rasgos que identifican a cada una con solo una huella ya sea de un dedo o se toda la fisionomía de la mano.



Así mismo en la huella dactilar como la figura 5 se muestra su estructura en donde se encuentra el núcleo, delta, surcos, crestas papilares que es el relieve lineal que existe en la epidermis de ciertas zonas, que alternando con los surcos, forman el dibujo papilar. Son las rayas negras de una huella impresa en papel y valles es la hendidura entre las crestas de la huella digital.

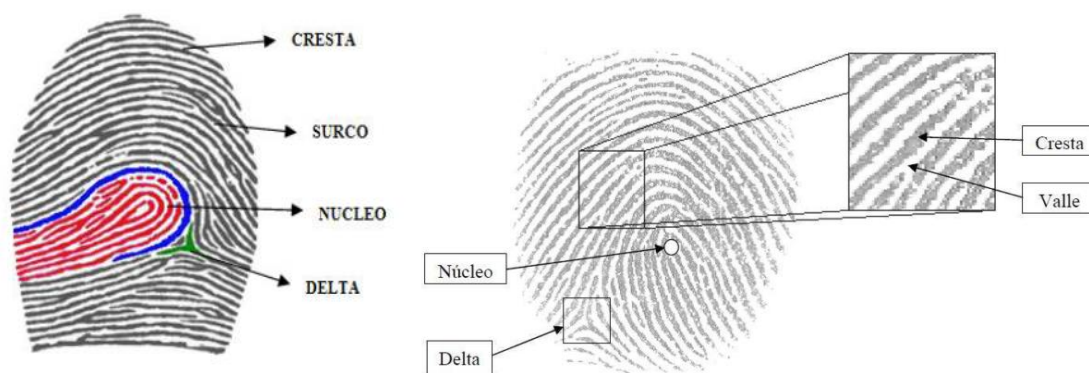


Figura 5. Estructura de una Huella dactilar[1][9]

Las crestas y los valles discurren en paralelo por la superficie de la huella. Las anomalías de las crestas se denominan **minucias** y pueden encontrarse en múltiples formas diferentes[10]. En la Figura 6, se muestran los ejemplos de minucias más típicos[9].

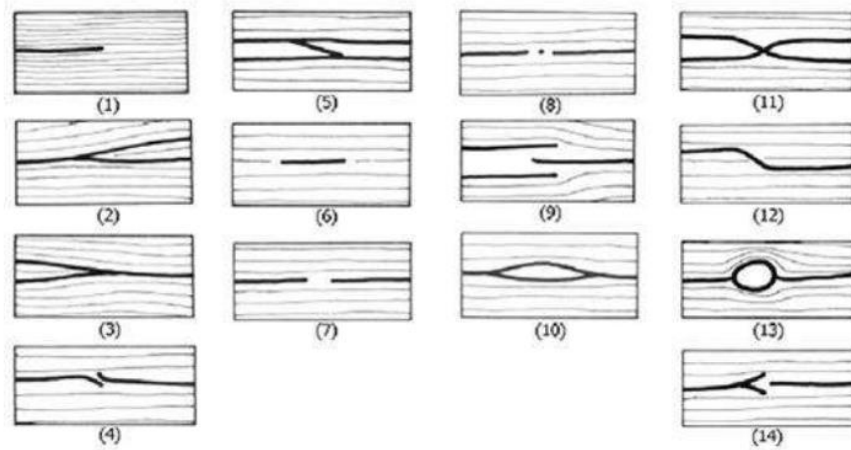


Figura 6. Algunos tipos de crestas: (1) Abrupta, (2) Bifurcación, (3) Convergencia, (4) Desviación, (5) Empalme, (6) Fragmento, (7) Interrupción, (8) Punto, (9) Ensemble, (10) Ojal, (11) Secante, (12) transversal, (13) Círculo, (14) Delta[9].

2.1.2. Reconocimiento facial



Figura 7. Reconocimiento facial

El reconocimiento facial de la figura 7, es una técnica mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Para ello, se utilizan programas de cálculo que analizan imágenes de rostros humanos[11].

Entre los aspectos clave empleados para la comparación se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.

A diferencia de otros sistemas biométricos, el reconocimiento facial puede ser utilizado para la vigilancia general, habitualmente mediante cámaras de video.

Mejoras en los sistemas de reconocimiento facial han podido discernir entre personas reales y fotografías, sin embargo, cualquier persona puede modificar visualmente su

cara de manera sencilla, como por ejemplo utilizando unas gafas de sol o dejándose crecer la barba[6].

Así mismo, debe considerarse que el rostro de las personas varía con la edad. Existen soluciones de software que utilizan esta tecnología para identificación de usuarios en dispositivos móviles y portátiles[12].

Se puede reconocer ciertas ventajas y desventajas de este sistema biométrico como a continuación[1]:

Ventajas:

- ✓ Sistema de reconocimiento es no invasivo por lo que no requiere contacto con el autenticador.
- ✓ Las personas pueden estar en movimiento cuando se encuentran frente al sistema biométrico.
- ✓ Alta aceptabilidad ya que los usuarios no ven interrumpido su flujo de acceso y trabajo.
- ✓ Es un sistema no invasivo ya que únicamente se trata de una fotografía.

Desventajas

- ✓ Variación en el ángulo de la cabeza lo que no permite realizar el proceso de verificación.
- ✓ Cambios de iluminación pueden llegar afectar el sistema biométrico.
- ✓ Los gestos expresivos pueden alterar el proceso de identificación.
- ✓ Unos de los mayores problemas es la utilización de máscaras, o que exista obstrucción debido a lentes, gafas o sombreros que puedan cubrir parte de la cara por lo que hace difícil ser detectado por el sistema de vigilancia.

2.1.3. Reconocimiento de iris



Figura 8. Reconocimiento de iris

Los patrones de iris de la figura 8, vienen marcados desde el nacimiento y rara vez cambian. Son extremadamente complejos, contienen una gran cantidad de información y tienen más de 200 propiedades únicas.

El escaneado del iris se lleva a cabo con una cámara de infrarrojos especializada situada por lo general muy cerca de la persona que ilumina el ojo realizando una fotografía de alta resolución. Este proceso dura sólo uno o dos segundos y proporciona los detalles del iris que se localizan, registran y almacenan para realizar futuras verificaciones[13].

A continuación se presenta ciertas ventajas y desventajas que presta el sistema biométrico de reconocimiento de iris[1]:

Ventajas

- ✓ El iris tiene características únicas que no cambian con el tiempo.
- ✓ El reconocimiento de Iris es una Técnica donde el usuario puede realizar la verificación desde una distancia cómoda del escáner.
- ✓ El patrón de los vasos sanguíneos en la retina no cambia con el tiempo.
- ✓ El tiempo de verificación de retina es rápido.
- ✓ El sistema de análisis de retina es difícil de engañar, no existe la manera de hacer una réplica igual y cuando la persona fallece la retina se deteriora.

Desventajas

- ✓ Para obtener la medida exacta el patrón debe estar ubicado a una distancia considerable del escáner, lo cual significa incomodidad para los usuarios, porque no siempre será con exactitud la distancia.
- ✓ Este sistema es poco utilizado en el mercado por lo que no es de fácil adquisición y es muy costoso.
- ✓ No tiene la facilidad de realizar búsqueda de un patrón con varios patrones ya almacenados.
- ✓ Necesidad del desarrollo del algoritmo. El reconocimiento de retina puede revelar enfermedades y afecciones la cuales pueden vulnerar el derecho a intimidad de los usuarios como hipertensión.

- ✓ El reconocimiento de retina la captura de este rango biométrico es compleja ya que se necesita voluntad y cooperación por parte del usuario ya que se requiere contacto con el sensor y su gran aceptabilidad es muy importante.

2.1.4. Reconocimiento de la geometría de la mano



Figura 9. Geometría de la mano

La geometría de la mano de la figura 9, se basa en la estructura de la palma y de los dedos, incluyendo el ancho y la longitud de los dedos o el grosor de la palma.

Esta tecnología utiliza la forma de la mano para confirmar la identidad del individuo. Para la captura de la muestra se emplean una serie de cámaras que toman imágenes en 3-D de la mano desde diferentes ángulos.

Las características extraídas incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea en general. No se tienen en cuenta detalles superficiales, tales como huellas dactilares, líneas, cicatrices o suciedad, así como las uñas, que pueden variar de tamaño en un breve período de tiempo.

Si bien es cierto que la estructura de los huesos y las articulaciones de la mano son rasgos relativamente constantes, no obstante otras circunstancias, como una inflamación o una lesión, pueden variar la estructura básica de la mano dificultando la autenticación[14].

Se presenta algunas ventajas y desventajas del sistema biométrico de reconocimiento de la geometría de la mano[1]:

Ventajas

- ✓ Plantillas ocupan pequeñas cantidades de bytes.

- ✓ Es un sistema no intrusivo.
- ✓ Gran exactitud.
- ✓ Sencillo, no es costoso y no requiere de luz especial para ser utilizado.

Desventajas

- ✓ Lectores son de relativo gran tamaño, lo que los hace fáciles de ser dañados.
- ✓ Lectores son costosos.
- ✓ Variación de la morfología y geometría de la mano a lo largo de la vida.
- ✓ Toma mucho espacio para registrar y se puede alterar con facilidad con la utilización de joyas o problemas de salud como artritis.

2.1.5. Reconocimiento de retina



Figura 10. Reconocimiento de retina

El escáner biométrico de la retina de la figura 10, se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma. El hecho de que cada patrón sea único (incluso en gemelos idénticos al ser independiente de factores genéticos) y que se mantenga invariable a lo largo del tiempo, la convierten en una técnica idónea para entornos de alta seguridad.

Pese a que su tasa de falsos positivos sea prácticamente nula, esta tecnología tiene un inconveniente considerable ya que es necesaria la total colaboración por parte del usuario al tratarse de un proceso que puede resultar incómodo. La toma de la muestra se realiza a partir de la pupila, lo que requiere que el usuario permanezca inmóvil y muy cerca del sensor durante la captura de la imagen. No obstante, el uso de una cámara de infrarrojos para la captura evita el riesgo de que el ojo pueda resultar dañado en el proceso[15].

2.1.6. Reconocimiento vascular



Figura 11. Reconocimiento vascular

En la biometría vascular de la figura 11, se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo (o de las muñecas). A diferencia de la huella dactilar el patrón biométrico es interno, por esta razón no deja rastro y sólo se puede conseguir en presencia de la persona. Es por tanto muy difícil el robo de identidad.

Debido a estas características es especialmente indicado para entornos de alta seguridad, así como en situaciones en que la superficie del dedo pueda estar en mal estado, erosionada o poco limpia[6].

2.2. Otras formas de biometría fisiológica

Existen además otras técnicas que analizan:

- ✓ Líneas de la palma de la mano
- ✓ Forma de las orejas
- ✓ Piel, textura de la superficie dérmica
- ✓ Adn, patrones personales en el genoma humano
- ✓ Composición química del olor corporal.

Estas técnicas son todavía novedosas y su uso es muy reducido. Su implantación presenta mayores problemas que en el resto de los casos, ya sea por menor eficacia o por necesitar mayores esfuerzos en el procesamiento de la información.

2.3. Tecnologías biométricas de comportamiento

Las tecnologías biométricas de comportamiento se caracterizan por considerar en el proceso de identificación rasgos derivados de una acción (al escribir, al caminar, etc.) realizada por una persona. Por tanto, incluyen la variable tiempo, ya que toda acción tiene un comienzo, un desarrollo y un final.

2.3.1. Reconocimiento de firma



Figura 12. Reconocimiento de firma

Esta técnica analiza la firma manuscrita de la figura 12, para confirmar la identidad del usuario firmante.

Existen dos variantes a la hora de identificar a las personas según su firma:

- ✓ **Comparación simple:** se considera el grado de parecido entre dos firmas, la original y la que está siendo verificada.
- ✓ **Verificación dinámica:** se hace un análisis de la forma, la velocidad, la presión de la pluma/bolígrafo y la duración del proceso de firma. No se considera significativa la forma o el aspecto de la firma, sino los cambios en la velocidad y la presión que ocurren durante el proceso, ya que sólo el firmante original puede reproducir estas características[16].

El reconocimiento de firma tiene así mismo ventajas y desventajas como las señaladas a continuación[1]:

Ventajas

- ✓ La firma es una sola para cada persona.

- ✓ Es Hardware que se utiliza es bastante sencillo.
- ✓ Costo de implementación es bajo.
- ✓ Es un sistema con gran aceptabilidad y ha sido utilizado desde el pasado.

Desventajas

- ✓ No es confiable debido a que la persona puede variar su firma dependiendo de la ocasión, por lo que al realizar la verificación con el sistema se debe firmar más de una vez.
- ✓ Tiene un alto índice de falsificación.
- ✓ Bajo nivel de precisión.
- ✓ La firma tiene una variación para una misma persona con el pasar de los años por lo que hace difícil su identificación.

2.3.2. Reconocimiento de escritor

El objetivo del reconocimiento de escritor es averiguar o confirmar la identidad del autor de un determinado texto manuscrito valiéndose de un software OCR (o reconocimiento óptico de caracteres). Cada persona tiene una forma de escribir diferente, teniendo rasgos propios e inconfundibles para cada letra. Asimismo, cada persona tiene un grado de inclinación en la escritura y nivel de presión al escribir.

Uniendo todos estos datos, un software de reconocimiento de escritor puede ser capaz de detectar la persona que está escribiendo un texto manuscrito.

2.3.3. Reconocimiento de voz

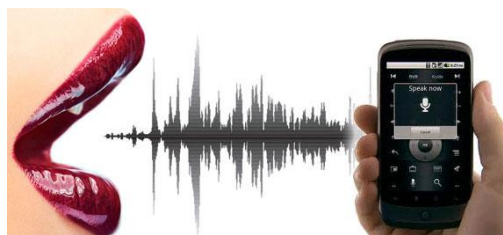


Figura 13. Reconocimiento de voz

Este tipo de dispositivos biométricos de la figura 13, están basados en un entrenamiento de las variaciones de la voz donde se implementa un micrófono y las aplicaciones de reconocimiento de voz usan redes neuronales para aprender a identificar voces. Existen factores como el ruido de fondo que pueden generar un margen de error.

A pesar de que siguen existiendo dificultades para reconocer la forma natural de hablar de ciertos individuos, esta tecnología cuenta con la ventaja de que el dispositivo de adquisición es simplemente un micrófono por lo que no requiere de inversiones adicionales[17].

La utilización de este método está más extendida en sistemas de respuesta por voz y en centros de atención de llamadas telefónicas (call centers) que en el control de acceso físico a edificios o a redes y equipos informáticos[15].

Se puede observar algunas ventajas y desventajas del sistema de reconocimiento de voz[1]:

Ventajas

- ✓ Puede ser confiable es una marca individual de una persona.
- ✓ Es un sistema biométrico aceptado.

Desventajas

- ✓ La voz puede ser grabada y reproducida después para engañar al sistema.
- ✓ Puede ser alterada por la edad o enfermedades o afecciones como resfriado o en algunos casos el estado de ánimo hace que varía.
- ✓ Su baja distintividad y es muy fácil de ser imitada.

2.3.4. Reconocimiento de escritura de teclado



Figura 14. Reconocimiento de escritura de teclado

Métodos como key-stroke, código morse y tiempo entre pulsaciones son algunas técnicas como la figura 14, que se basan en el hecho de la existencia de un patrón de escritura en teclado que es permanente y propio de cada individuo. Este elemento biométrico solo requiere de un teclado y la aplicación que controla la velocidad de tecleo la desventaja es que puede estar sujeto a alteraciones de los usuarios por lesiones sufridas en las manos.

2.3.5. Reconocimiento de la forma de andar

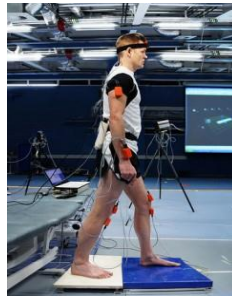


Figura 15. Reconocimiento de la forma de andar

La forma de caminar de la figura 15, es que cada sujeto permite su identificación aunque no requiere proximidad existen muchas dificultades para el reconocimiento rápido del mismo ya que lo que se necesita son procesos de poca duración para el análisis del modo de andar[9].

Esta tecnología está todavía en desarrollo y no ha alcanzado aún los niveles de rendimiento necesarios para ser implantada de manera similar al resto de tecnologías biométricas.

2.4. Comparación de tecnologías biométricas

En la Tabla 1, se muestra una comparación entre las tecnologías biométricas según las características que posee cada uno, calificándolas en niveles de seguridad como: Alta (A), Media (M) y Baja (B)[18]. La cual fue modificada de acuerdo a las tecnologías requeridas para el presente trabajo.

Tabla 1. Comparación de tecnología biométrica según sus características

Identificado or Biométrico	Característica	Universalidad	Singularidad	Estabilidad	Cuantificable	Aceptabilidad	Rendimiento	Usurpación
Huella Dactilar		M	A	A	M	M	A	M
Reconocimiento facial		A	B	M	A	A	B	A
Reconocimiento de iris		A	A	A	M	M	A	M
Reconocimiento de la geometría de la mano		M	M	M	A	M	M	M
Reconocimiento de retina		A	A	M	B	B	A	B
Reconocimiento vascular		M	M	M	M	M	M	B
Reconocimiento de firma		B	B	B	A	A	B	A
Reconocimiento de voz		M	B	B	M	A	B	A
Reconocimiento de escritura de teclado		B	B	B	M	M	A	M
Reconocimiento de la forma de andar		M	B	B	A	A	B	M

Capítulo 3.- Beneficios del uso de tecnologías biométricas

La implantación de tecnologías biométricas conlleva un conjunto de ventajas tanto para entidades públicas y privadas como para los usuarios finales.

Aunque las medidas biométricas están relacionadas con la ciberseguridad, gran parte de sus beneficios afectan a la vida diaria de usuarios y empleados:

- ✓ Reducción de costes de mantenimiento de los sistemas de autenticación
- ✓ Aumento de la eficiencia
- ✓ Control horario
- ✓ Mejora de la imagen corporativa

3.1. Para las organizaciones y usuarios finales

Las organizaciones deben ser el principal motor que promueva e invierta en el desarrollo de las tecnologías biométricas. Para que esto ocurra, los beneficios potenciales a obtener con su implantación han de ser claros y relevantes. A continuación se describen los más destacados.

3.2. Usos y aplicaciones

Usada como forma única de autenticación o combinada con otras medidas (como tarjetas inteligentes, claves de cifrado o firmas digitales), la biometría está destinada a extenderse en muchos aspectos de nuestra vida diaria.

Los puntos fuertes de la biometría son:

- ✓ Puede asociarse a un individuo en concreto
- ✓ Su comodidad, ya que no es necesario tener o recordar algo.
- ✓ Es altamente resistente al fraude.

3.3. Aplicaciones actuales de las tecnologías biométricas con detección de huella dactilar

3.3.1. Control de accesos físicos y lógicos

Una de las aplicaciones en las que más extendido está el uso de la biometría es el control de accesos, ya sea éste físico (por ejemplo acceso a edificios o espacios restringidos) o lógico (acceso a sistemas, programas o equipos informáticos, móviles, tabletas).

Actualmente, la huella dactilar es la solución mayoritaria para este uso debido a su alto grado de madurez, que permite el establecimiento de precios competitivos, y a la usabilidad que ofrece.

No obstante, y aunque su presencia sea menor, el reconocimiento facial se presenta como alternativa a la huella dactilar en este tipo de aplicaciones.

En ocasiones, para el control de acceso a zonas de alta seguridad, se hace uso de una combinación de técnicas. Un ejemplo es el uso de una contraseña o tarjeta de identificación adicional a la huella dactilar, o la combinación de dos tecnologías biométricas, denominada biometría bimodal. Así, se pueden combinar dos factores de identificación: por un lado quién o cómo se es (biometría) y por otro, lo que se sabe o se tiene por ejemplo, contraseñas y tarjetas.

Del mismo modo que se pueden instalar sensores en la entrada de edificios y salas de acceso restringido, cada vez más se integran sensores biométricos en los ordenadores corporativos de cara a gestionar la autenticación en sistemas y aplicaciones mediante tecnologías biométricas.

3.3.2. Control de presencia

Los métodos utilizados tradicionalmente para registrar a diario los horarios en los que los empleados acceden y abandonan sus respectivos puestos de trabajo suelen estar basados en el uso de un sistema biométrico de reconocimiento dactilar, ya que esto ayuda a evitar que se puedan cometer irregularidades debido a que el acceso es personal.

El uso de cualquier técnica biométrica supone una forma eficaz de mitigar este riesgo por la imposibilidad de compartir los rasgos biométricos entre empleados.

Para este tipo de aplicaciones se utiliza habitualmente la huella dactilar, aunque también técnicas menos extendidas en el mercado como la geometría de la mano.

3.3.3. Medio de pago

El uso de la biometría en terminales de punto de venta (TPV) ha reducido el tiempo empleado en transacciones y ha reducido las posibilidades de errores o confusiones. Como ejemplo, es posible implantar el uso de la huella dactilar para el pago (pre-asociado a una cuenta bancaria), eliminando problemas relacionados con la pérdida de tarjetas, olvido de números de identificación, transacciones manuales y cargos a cuentas erróneas.

3.3.4. Control de navegación

Se pueden usar controles mediante huella dactilar aplicados al acceso a redes sociales y a determinados sitios web, incluyendo las restricciones que la empresa haya determinado, por ejemplo, el filtrado de contenidos, la búsqueda de páginas o el uso ciertos servicios.

Capítulo 4.- Métodos de ataque

Se refiere a un acceso falso de un usuario ilegal en el sistema biométrico de huellas digitales mediante el uso de una huella dactilar falsa que reproduce la de un usuario no autorizado. Estos artefactos están hechos de diversos materiales como plastilina, arcilla, gelatina, goma. Todo el proceso de creación de huellas dactilares falsas se puede hacer con o sin cooperación y obtener un acceso fácil a la sociedad altamente autenticada[19].

Así también según[20], un ataque de suplantación consiste en robar, copiar y replicar sintéticamente un biométrico ras, para obtener acceso no autorizado, derrotando la seguridad del sistema. La factibilidad de un ataque de suplantación es mucho mayor que otros tipos de ataques contra sistemas de biometría, ya que no requiere ningún conocimiento de sistema.

Se pueden clasificar en tres categorías[21]:

- ✓ **Administrativos:** El ataque se realiza por gente de dentro (*insiders*), como administradores de sistemas, o alguien que amenaza a otra persona para que le de las credenciales de acceso.
- ✓ **Infraestructura no segura:** El atacante fija como objetivo componentes vulnerables del sistema. Una vez dentro, puede modificar datos, robarlos etc.
- ✓ **Biometric overtress:** En este tipo de ataque se crean biometrías artificiales para intentar engañar al sistema y obtener acceso. La generación de la biometría falsa está basada en la de algún usuario genuino del que se ha ido recabando información de forma secreta. Por ejemplo recolectando muestras de sus huellas dactilares.

4.1. Métodos de ataque a la biometría de reconocimiento de Huellas Dactilares

En los sistemas biométricos de reconocimiento dactilar existen diferentes tipos de ataques a los que puede ser sometido un sistema de reconocimiento biométrico basado en huella dactilar. En concreto, se han analizado los posibles puntos de ataque clasificándolos en ocho categorías[22]. En la Figura 16 se pueden ver estos puntos de

ataque junto a los componentes básicos de un sistema biométrico. Los puntos potenciales son los siguientes:

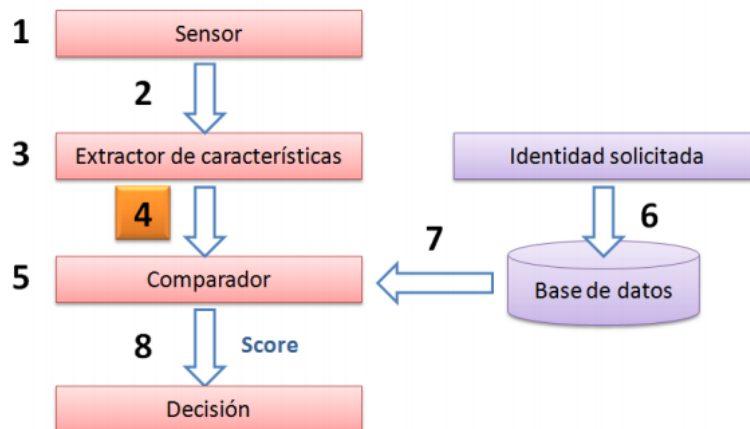


Figura 16. Potenciales puntos de ataque a un sistema de reconocimiento biométrico[9].

- ✓ Ataques al sensor o escáner (punto 1 en la Figura 16).
- ✓ Ataques al módulo extractor de características (punto 3 en la Figura 16).
- ✓ Ataques al módulo comparador (punto 5 en la Figura 16).
- ✓ Ataques a la base de datos del sistema (punto 6 en la Figura 16).
- ✓ Ataques a los distintos canales de comunicación entre los módulos existentes en el sistema (puntos 2, 4, 7 y 8 en la Figura 16).

El ataque al sensor o escáner es un tipo de ataque directo al sistema, y en él, el atacante no tiene ningún conocimiento sobre el funcionamiento de dicho sistema. El resto de ataques se denominan indirectos y van dirigidos a alguno de los módulos internos del sistema. En ellos el impostor necesita de algún tipo de conocimiento sobre el funcionamiento o estructura interna del sistema.

Los ataques lanzados directamente sobre los módulos del sistema (1, 3, 5 y 6 de la Figura 16) se denominan ataques Troyanos. En cambio, los que se lanzan sobre los canales de comunicación entre los módulos del sistema (2, 4, 7 y 8 de la Figura 16) son referenciados como ataques de repetición.

4.1.1. Ataques al sensor

Estos ataques han demostrado ser muy exitosos ya que sólo necesitan generar el rasgo biométrico sin tener que conocer el funcionamiento del módulo comparador o las especificaciones de las plantillas. En consecuencia, en el caso concreto de la huella dactilar, para poder llevar a cabo este tipo de ataques sólo se requiere un dedo falso del usuario a suplantar. Además, al operar en el dominio analógico, los mecanismos de protección digitales como encriptación, hashing (técnicas de transformación no invertible), firma digital, no son aplicables. Normalmente se había pensado que la plantilla de minucias constituía una representación compacta de las características de la imagen original sin suficiente información como para poder reconstruir dicha imagen. Dichos ataques, se basan en la utilización de huellas falsas creadas a partir de plantillas estándar de minucias[18].

La creación de dedos de goma como huella artificial para este tipo de ataques, se puede realizar con o sin la colaboración del dueño del rasgo biométrico. Cabe esperar, que los ataques al sistema serán más exitosos si el dedo artificial se crea con la colaboración del usuario por tener una calidad de imitación mayor. Además según[23] existen dos programas de libre distribución para generar imágenes sintéticas de huellas y caras llamados SFINGE y FACES respectivamente como la figura 17. El programa de huellas sintéticas fue creado para facilitar la creación de bases de datos (una base de datos sintética es menos laboriosa que la captura de donantes).



Figura 17. Imágenes de huellas y caras sintéticas generadas con los programas SFINGE y FACES respectivamente[23].

4.1.2. Ataque al canal entre el sensor y el extractor de características

Se trata de un ataque tipo 2 mostrados en la figura 16. Los ataques en este nivel consisten en inyectar datos biométricos almacenados previamente. Esta posibilidad es especialmente importante en aplicaciones remotas, en las que un ordenador cliente proporciona datos biométricos a un host remoto que lleva a cabo el reconocimiento. Esta situación es especialmente delicada en aplicaciones de Internet[23].

El canal de comunicación puede ser interceptado y se puede introducir otra información que sustituya a la enviada por el sensor o bien guardar la imagen de la huella digital del usuario legítimo para ser replicada posteriormente y presentada al extractor de características.

4.1.3. Ataques al extractor de características

En los ataques de este nivel, se fuerza al extractor de características a proporcionar valores escogidos por el impostor, en vez de las medidas reales extraídas a partir de la señal original capturada por el sensor biométrico. Este ataque suele consistir en insertar un programa que reemplaza al verdadero extractor de características[23], es decir que es un programa tipo Troyano (código ejecutable que no es directamente la traducción original del programa, sino que ha sido añadido con posterioridad y que entra simulando ser el original) puede suplantar al extractor de características y enviar características generadas a voluntad del atacante (generadas artificialmente) al comparador[20].

4.1.4. Ataques al canal entre el extractor de características y el comparador

Este ataque consiste en reemplazar las características extraídas por otras de falsas, o por un conjunto de características que han sido adquiridas previamente de forma ilegal. Es parecido al ataque del punto 2 de la figura 16. De hecho, los sistemas remotos se pueden diseñar para enviar las medidas biométricas (señal de voz, imagen capturada, etc.) o para enviar únicamente la transmisión de las medidas de interés (coeficientes cepstrales, minucias, coeficientes de las eigenfaces, etc.). La ventaja de esta segunda solución es que elimina el envío de información no relevante y además impide que a partir de la información enviada se pueda regenerar la señal biométrica

original (a partir de las minucias, no se puede restaurar el bmp de la huella dactilar de la que fueron extraídas)[23].

4.1.5. Ataques al comparador

Al igual que en los ataques de tipo 3, se trata de introducir un programa Troyano que suplante al comparador modificando las puntuaciones (scores) o la decisión final (sí o no) que se envía a la aplicación de autenticación. Si el programa Troyano envía siempre respuestas afirmativas, se dice que estamos ante un puenteo del sistema[24]. Si, por el contrario, la respuesta es siempre negativa o las puntuaciones son bajas, se habla de una negación del servicio.

4.1.6. Ataques a la base de datos

Este ataque puede lanzarse durante el proceso de registro, etapa de verificación o directamente sobre la base de datos en cualquier momento mediante un programa Troyano que suplante a la base de datos enviando información generada artificialmente (plantillas, nombres de usuarios, etc.) Para el caso de una aplicación sobre tarjeta inteligente, es importante que esté protegida correctamente mediante por ejemplo, técnicas de encriptación[22], porque la pérdida de la tarjeta permite el acceso directo al impostor a la plantilla (template). Otro método de protección de plantillas biométricas supone la utilización de una versión distorsionada de la señal biométrica no invertible o el vector de características[25]. Esto permite cambiar la transformación de distorsión en el momento en que la plantilla se vea comprometida.

El resultado de la autenticación depende de la comparación entre las plantillas o modelos almacenados en la base de datos y las características extraídas de la muestra de entrada. Si se altera la base de datos de alguna forma, el sistema será craqueado de forma permanente. De forma alternativa, en vez de alterar la base de datos, es posible almacenar modelos que pertenezcan a un usuario no autorizado. En el primer caso, debe asegurarse la integridad de la base de datos y que ésta no es manipulada desde el exterior[23]. Esto implica backups frecuentes, suprimir los permisos de escritura salvo para nuevas entradas, etc. En el segundo caso, debe ponerse especial atención durante el entrenamiento (enrollment) de los usuarios mediante la supervisión de un gestor durante todo el proceso. Obviamente antes de

aceptar un nuevo usuario, debe comprobarse que realmente es quien dice ser y que está autorizado a acceder al sistema.

4.1.7. Ataques al canal entre la base de datos y el comparador

Este nivel es análogo a los niveles 2 y 4 de la Figura 16. Sin embargo, aquí la suplantación de los datos reales afecta a la comunicación de los modelos (o plantillas) almacenados en la base de datos hacia el clasificador. Puede ser importante cuando la base de datos sea remota y, por ejemplo, compartida por varios sistemas de acceso que trabajan sobre una misma base de datos común a todos ellos[23].

4.1.8. Ataques al canal entre el comparador y la aplicación

El último nivel consiste en saltarse todo el sistema biométrico y reemplazar su decisión. Por ejemplo, en un sistema de control de accesos basado en reconocimiento biométrico, seguramente habrá un par de terminales que enviarán el resultado del sistema biométrico hacia un actuador. El actuador puede ser tan simple como un relé que abre o cierra un circuito en función de la tensión aplicada. Actuar sobre estos cables e inyectarles una tensión de activación sería suficiente para burlar todo el sistema biométrico[23].

La información que circula por el canal entre la aplicación que solicita una verificación y el comparador puede ser interceptada y guardada para ser utilizada más adelante. Es decir, la decisión final del sistema (sí o no) queda en manos de la voluntad del intruso.

Capítulo 5.- Algoritmos de ataque

5.1. Ataque mediante el algoritmo hill-climbing

Los ataques hill-climbing a sistemas de reconocimiento biométrico consisten en la sucesiva modificación de un patrón de características obtenido sintéticamente hasta conseguir que el sistema acepte dicho patrón. Pueden realizarse ataques hill-climbing de tipo 2 (según la clasificación de la Figura 16), es decir, atacar al canal de comunicaciones que existe entre el sensor y el extractor de características; o bien se pueden realizar ataques de tipo 4 que consisten en atacar al sistema en el canal de comunicación entre el extractor de características y el módulo comparador. La Figura 18 muestra un esquema general de ataques hill-climbing tipo 4 basado en puntuación o score. Para este tipo de ataque se requiere conocer el formato de la plantilla.

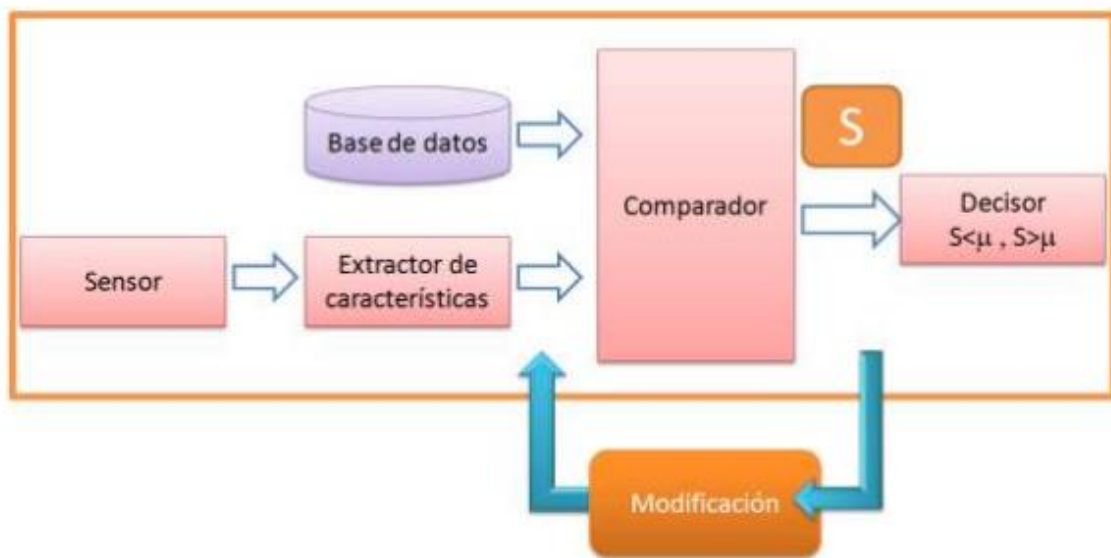


Figura 18. Ataque hill-climbing tipo 4 basado en puntuación

Emplearemos la siguiente tabla 2. la nomenclatura basada en [26]:

Tabla 2. Nomenclatura algoritmo Hill-Climbing

Di :	la plantilla del usuario de la base de datos, $i = \dots$, donde 1,2,3, ,N y N es el número de usuarios en la base de datos.
------	---

n_i :	número de minucias de la huella. El sistema atacante desconoce este valor.
T_i^j :	la j-ésima plantilla sintética generada por el sistema de ataque para la huella de la base de datos del usuario i.

El formato de las plantillas es el siguiente:

$$T_i^j = \begin{bmatrix} {}^1x_i^j & {}^1y_i^j & {}^1\theta_i^j \\ {}^2x_i^j & {}^2y_i^j & {}^2\theta_i^j \\ \vdots & \vdots & \vdots \\ {}^nx_i^j & {}^ny_i^j & {}^n\theta_i^j \end{bmatrix}$$

Donde x e y representan la fila y columna respectivamente de cada minucia y θ es el ángulo de la orientación de la minucia.

- ✓ $S(D_i, T_i^j)$: es la puntuación o score resultante de la comparación entre las plantillas D_i y T_i^j .
- ✓ S_{umbral} : es la mínima puntuación necesaria para que dos huellas sean consideradas correspondientes y por tanto la huella T_i^j sea aceptada como correspondiente a la huella D_i del usuario i.

Se emplean únicamente las coordenadas de cada minucia y su orientación, por ser estos datos comunes a la mayoría de los sistemas de reconocimiento actuales basados en minucias.

El ataque descrito en [26] efectúa las siguientes operaciones:

1. Crear 100 patrones de minucias $T_i^1, T_i^2, T_i^3, \dots, T_i^{100}$ completamente aleatorios del mismo tamaño que las imágenes de la huella. Para que estos patrones sean más realistas, se crean minucias separadas al menos la distancia equivalente a una cresta. Para el caso de 500 ppp, esta distancia es de 9 píxeles aproximadamente. El número de minucias iniciales en el ataque descrito es de 25.

2. Atacar con los 100 patrones la huella objetivo y almacenar todas las puntuaciones devueltas por el matcher. Se escogerá como patrón ganador $T_i^{Ganador}$ aquél que haya generado la puntuación más alta $S_{ganadora}(D_i, T_i^j)$:
3. Realizar las siguientes iteraciones:
 - a) Desplazar con probabilidad 0.5 una minucia de ganador $T_i^{Ganador}$, a una celda adyacente o modificar su ángulo con probabilidad 0.5. Si la puntuación en el matcher mejora, almacenar esta modificación en el patrón, si no, se desecha.
 - b) Añadir una nueva minucia. Si la puntuación aumenta, almacenarla, si no, eliminarla.
 - c) Reemplazar una minucia por otra aleatoria. De nuevo, si se mejora, almacenar el cambio, si no, ignorarlo.
 - d) Eliminar una minucia y operar del mismo modo.
4. Si en algún momento se supera la puntuación umbral, el ataque habrá tenido éxito y por lo tanto se detiene.

✓ Protección frente a ataques hill-climbing

Dado que un ataque hill-climbing requiere para su funcionamiento la puntuación obtenida en el matcher o comparador como lo muestra la figura 18, la solución más trivial para proteger un sistema de esta clase de ataques sería la de que el matcher no revelase la puntuación sino simplemente la indicación de aceptación o rechazo por parte del sistema. Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que empleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible.

En [26] se propone cuantificar las puntuaciones devueltas por el matcher como una método de protección ante ataques hill-climbing. La ventaja de esta medida es clara, puesto que al basarse el ataque en pequeñas modificaciones de la plantilla inicial, una leve mejora o un leve empeoramiento no podrán, en general, ser detectados al permanecer la mejoría dentro del mismo paso de cuantificación y mantenerse por lo tanto invariable la puntuación de salida. Nótese que cualquier matcher puede ser considerado como cuantificado.

Una sencilla pero eficaz solución es bloquear los intentos de coincidencia si hay demasiadas falsas coincidencias en un período de tiempo determinado (por ejemplo, es muy poco probable que un usuario legítimo puede proporcionar más de, digamos, 20 falsos ataques por día). Los sucesivos intentos pueden indicar un ataque por un programa informático, para una plantilla específica. Si el atacante tiene tiempo suficiente, incluso esta medida no puede ser muy eficaz. Por ejemplo, el atacante puede acumular los resultados de varios días: si 1.000 iteraciones son necesarias para romper en una cuenta, el atacante puede montar un ataque que dura 50 días (con 20 iteraciones/día) y todavía se las arreglan para irrumpir en la cuenta[27].

5.2. Ataques mediante algoritmo side-channel

Un ataque side-channel se produce cuando un atacante es capaz de utilizar información adicional obtenida de la implementación física de un sistema criptográfico[25]. Si la información side-channel es suficiente, permitirá romper un sistema cifrado. No se trata de ataques por fuerza bruta que aprovechan la existencia de una tasa de falsa aceptación, sino que utilizan información de la implementación del sistema como puede ser el tiempo (timing-attacks)[28], el consumo de energía (powerattacks), las pérdidas electromagnéticas o el ruido del sistema. Existen varios tipos de ataques side-channel, dentro de los cuales, aquellos basados en la información temporal han demostrado tener una gran eficiencia. Estos ataques denominados timing-attacks se han convertido en una amenaza real a tener en cuenta a la hora de implementar sistemas de seguridad, por lo que profundizaremos a continuación en su funcionamiento.

Algoritmo de ataque:

1. Crear 100 patrones sintéticos con un número determinado de minucias del tamaño de la imagen de la huella a estudiar.
2. Atacar la huella objetivo con los 100 patrones sintéticos y guardar los tiempos que tarda el comparador en generar una puntuación. Se elige el mejor patrón en función del tiempo T_m .
3. Modificamos el patrón ganador permitiendo uno de los siguientes cambios: B. Añadir una nueva minucia. C. Sustituir una minucia existente por otra aleatoria.
4. Para que los patrones sean realistas las minucias deben estar separadas el equivalente a una cresta que para la resolución de la imagen con la que se

trabaja es de 9 píxeles. En general, se permiten M cambios antes de realizar una nueva comparación.

5. Se realiza una nueva comparación y se calcula el nuevo tiempo T_m tras los M cambios realizados. Si el tiempo T_m indica que la puntuación ha aumentado, se conserva el cambio, si no, se desecha y se vuelve a modificar la huella (paso 3).
6. El algoritmo deja de ejecutarse si el sistema devuelve una respuesta positiva (el ataque finaliza con éxito) o se supera el número máximo de iteraciones (el ataque no ha tenido éxito).

5.2.1. Basados en tiempo: Timing-Attacks

Estos ataques fueron desarrollados para romper sistemas criptográficos. En principio, las características temporales sólo revelan una pequeña cantidad de información sobre un sistema criptográfico como puede ser la longitud de una clave, pero está demostrado que algunos ataques son capaces de encontrar la clave secreta en sí. Los sistemas criptográficos suelen utilizar tiempos diferentes según la entrada que estén procesando. Para que esto no ocurra se suele optimizar el código del algoritmo evitando operaciones innecesarias o aquellas que no se ejecuten en un tiempo fijo. El funcionamiento de los ataques side-channel basados en tiempo consiste en monitorizar el movimiento de datos que entra y sale de la CPU o la memoria. Sabiendo el tiempo que tarda en mover cierta información es posible saber la longitud que puede tener una clave, o de manera más clara, la longitud que seguro no va a tener [25], [28].

Capítulo 6.- Revisiones Bibliográficas

6.1. Definición

Según [29] la revisión sistemática es un “método que permite a los especialistas obtener resultados relevantes y cuantificables, esto lleva a la identificación, selección y producción de evidencias basadas en la investigación de un tópico en particular”. Para [30] “las revisiones de literatura tienen como fin resumir, compilar, criticar y sintetizar la investigación existente sobre un área temática o fenómeno de interés usando un proceso de búsqueda, catalogación, ordenamiento, análisis, crítica y síntesis”.

Las revisiones de literatura son contribuciones al conocimiento actual ya que sus hallazgos son únicamente obtenidos cuando la literatura más relevante es analizada como un todo y no como la simple lectura de documentos aislados[30].

6.2. Clasificación de las Revisiones Bibliográficas

Considerando la definición que dan los distintos autores para los diferentes tipos de revisión, se pueden observar las diferentes clasificaciones y la denominación que reciben las revisiones a continuación:

✓ **Clasificación 1.-** Pertenecen a Cronin [31][32]

Revisión tradicional o Narrativa, Revisión Sistemática, Meta-Análisis, Meta-síntesis.

✓ **Clasificación 2.-** Pertenecen a Grant [33]

Revisión Crítica, Revisión de Literatura, Revisión Sistemática, Meta-Análisis, Revisión Sistemática Cualitativa, Revisión Panorámica, Revisión Paraguas, Revisión de Estudios Mixtos, Revisión de Mapeo Sistemático, Revisión Rápida, Revisión Sistematizada.

✓ **Clasificación 3.-** Pertenecen a Whittemore

Revisión de Integradora, Revisión Sistemática, Meta-Análisis, Síntesis Cualitativa, Revisión Panorámica, Revisión Paraguas, Revisión de Estudios Mixtos, Revisión RE-AIM.

✓ **Clasificación 4.-** Pertenecen a Goris [34].

Revisión de Narrativa, Revisión de Integradora, Revisión Panorámica, Análisis Conceptual, Revisión Sistemática, Revisión Paraguas, Revisión Realista.

6.3. Selección de la Revisión del Estado del arte

Primeramente se realizó una descripción de cada uno de los tipos de revisión bibliográfica existentes, con el fin de identificar sus propósitos y elegir el tipo de revisión adecuada para desarrollar el Trabajo de Titulación. Los tipos de revisiones bibliográficas son:

- ✓ **Narrativa:** Conocida como tradicional o crítica. Su objetivo es identificar, analizar, valorar e interpretar el cuerpo de conocimientos sobre un tema específico. El enfoque y profundidad de la revisión está en función del contexto para el que se realice. Sin embargo, la característica común en la revisión narrativa es que se revisa la literatura publicada, y ello implica que los materiales incluidos poseen cierto grado de permanencia. Ocasionalmente este proceso puede haber sido realizado por pares (dos autores de forma independiente realizan la revisión, y después ponen en común sus conclusiones, realizando un proceso de contrastación), aunque no siempre es una condición imprescindible[32].
- ✓ **Integradora:** Este tipo de revisión fundamentalmente se centra en sintetizar el conocimiento sobre metodología, conocimientos teóricos o sobre la investigación realizada esbozando una conclusión sobre un tema específico esta propuesta puede ser confusa porque en cierto modo es parecida a la revisión narrativa, sin embargo el propósito de la revisión integradora puede ser aportar una comprensión más profunda o incluso crear una nueva conceptualización del tema. Tiene como objetivo demostrar que el autor ha investigado ampliamente la literatura y evaluado críticamente su calidad [33].
- ✓ **Sistemática:** Una revisión sistemática es definida como un resumen de evidencias, La diferencia más importante entre las revisión sistemática y otro tipo de revisiones es que fundamentalmente la metodología utilizada es explícita y precisa, y además se sigue un protocolo claramente delineado, estandarizado y replicable que asegura la calidad, consistencia y transparencia del proceso de revisión [33].

- ✓ **Meta-Análisis:** El meta-análisis es la combinación cuantitativa, mediante las técnicas estadísticas adecuadas, de los resultados de investigaciones anteriores (por lo general publicadas como artículos originales). Es un tipo de diseño metodológico en sí mismo, por lo que podría considerarse investigación original, en el que las unidades de análisis son estudios originales publicados previamente sobre el tema de interés. Últimamente el meta-análisis por la magnitud que está adquiriendo es considerada en sí como un tipo de revisión [35].
- ✓ **Panorámica:** pretende identificar los conceptos clave que sustentan un área de investigación, las principales fuentes y tipos de evidencias disponibles sobre todo cuando un área es compleja o no ha sido revisado exhaustivamente antes. Una de sus características es que no son una revisión sistemática que sea llevada a cabo con un protocolo preestablecido por la amplia variedad de estudios que se incluyen. Otro elemento que caracteriza a este tipo de revisión es que se utiliza la técnica de mapeo conceptual, de mapeo de la bibliografía y la opinión de los usuarios (2, 16). Esta metodología contribuye a identificar vacíos y carencias en el conocimiento sobre un tema [33]
- ✓ **Análisis conceptual:** Un tipo de revisión emergente en ciencias de la salud. El análisis conceptual es un método por el cual los conceptos que son de interés para una disciplina se examinan con el fin de aclarar sus características y conseguir una mejor comprensión del significado de ese concepto. Muchos de los conceptos que se usan en las ciencias de la salud son conceptos conductuales que se encuentran imbuidos de la forma en que se comprende el proceso de salud y enfermedad. Cuando se inicia un análisis conceptual se debe tener en cuenta que el concepto que se analiza debe Cuando se inicia un análisis conceptual se debe tener en cuenta que el concepto que se analiza debe ser relevante para la práctica y la disciplinarse relevante para la práctica y la disciplina [36]
- ✓ **Sistematizada:** Las revisiones sistematizadas o revisiones estructuradas intentan incluir uno o más elementos del proceso de revisión sistemática, sin llegar a afirmar que la producto resultante es una revisión sistemática. Podría catalogarse como una "revisión sistemática" pero en muchas ocasiones carecen de algún elemento que no permite etiquetarlas como tales. Un ejemplo

puede ser los trabajos de revisión que pueden realizar los estudiantes de postgrado que aun siguiendo toda la metodología de una revisión sistemática, carecen de recursos suficientes para realizarla (por ejemplo disponer de dos revisores que evalúen los documentos sometidos a análisis) [37].

- ✓ **Revisión de revisiones o paraguas:** Las revisiones paraguas o revisión de revisiones son un nuevo tipo de revisiones que están ganando un creciente interés, de manera que el número de reseñas publicadas es cada vez mayor. Estas revisiones se centran fundamentalmente en resumir la evidencia disponible. Pueden ser utilizadas para evaluar las similitudes y diferencias en las revisiones publicadas, para resumir lo que se sabe sobre un tema y normalmente implican un amplio número de diferentes tipos de revisiones. Este tipo de revisiones tienen limitaciones por la calidad metodológica utilizada al realizar este tipo de revisiones y que deberían establecerse normas metodológicas y directrices para mejorar la calidad de este nuevo tipo de publicación.
- ✓ **Realista:** Este tipo de revisiones han surgido como respuesta a la complejidad que tiene el diseño de políticas de intervención en salud. Los métodos tradicionales de análisis de las políticas de salud se centran en la medición y Muy frecuentemente estos informes encuentran que la evidencia es confusa, y ofrecen poca o ninguna idea de por qué la intervención funcionó o no funcionó cuando se aplica en diferentes contextos o circunstancias. La revisión realista está diseñada para trabajar con las intervenciones o programas sociales complejos, de modo que en el enfoque emerge una evaluación "realista". Este tipo de revisiones proporciona un análisis explicativo dirigido a discernir lo que funciona, en quién, en qué circunstancias, y en qué aspectos y cómo funciona [34].

6.4. Revisión Sistemática de Bárbara Kitchenham

6.4.1. Definición

Una revisión sistemática de la literatura es un medio para identificar, evaluar e interpretar todas las investigaciones disponibles acerca de una pregunta en particular

la investigación, o área temática, o fenómeno de interés. Los estudios individuales que contribuyen a una revisión sistemática se denominan primario estudios.

6.4.2. Importancia

La mayoría de la investigación se inicia con una revisión de la literatura de algún tipo. Sin embargo, a menos que una revisión de la literatura es exhaustiva y justa, es de poco valor científico. Esta es la principal razón para la realización de revisiones sistemáticas. Una revisión sistemática sintetiza el trabajo existente de una manera que sea justa y visto para ser justos. Por ejemplo, las revisiones sistemáticas deben llevarse a cabo de acuerdo con una estrategia de búsqueda predefinida. La estrategia de búsqueda debe permitir que la exhaustividad de la búsqueda para ser evaluado. En particular, los investigadores que realizan una revisión sistemática deben hacer todos los esfuerzos para identificar y reportar investigación que no apoyan su hipótesis de investigación preferente, así como la identificación y presentación de informes de investigación que lo soporta.

6.4.3. Proceso de Revisión

Una revisión sistemática de la literatura implica varias actividades. Las directrices existentes para las revisiones sistemáticas tienen ligeramente diferentes sugerencias sobre el número y el orden de las actividades. Sin embargo Barbara Kitchenham las plantea como se muestra en la Tabla 3.

Tabla 3. Protocolo de Barbara Kitchenham

REVISIÓN SISTEMÁTICA	
PLANIFICACIÓN DE LA REVISIÓN.	
	<ul style="list-style-type: none"> • Identificación de la necesidad de una revisión.
	<ul style="list-style-type: none"> • Especificación de la pregunta(s) de investigación.

ETAPA 1	<ul style="list-style-type: none"> • El desarrollo de un protocolo de revisión.
EJECUCIÓN DE LA REVISIÓN.	
ETAPA 2	<ul style="list-style-type: none"> • Identificación de la investigación.
	<ul style="list-style-type: none"> • Selección de los estudios primarios.
	<ul style="list-style-type: none"> • La extracción de datos y el seguimiento.
	<ul style="list-style-type: none"> • Síntesis de los datos.
ETAPA 3	INFORME DE LOS RESULTADOS.

6.4.4. Planificación

Antes de llevar a cabo una revisión sistemática es necesario para confirmar la necesidad de un examen. Las actividades más importantes antes de la revisión son la definición de la pregunta de investigación, se define los procedimientos básicos de revisión. El protocolo de examen debe estar sujeta a un proceso de evaluación independiente. Esto es particularmente importante para un estudio encargado.

✓ **Identificación de la necesidad de una revisión.**

La necesidad de una revisión sistemática surge de la exigencia de los investigadores para resumir toda la información existente sobre algún fenómeno de manera exhaustiva e imparcial. Esto puede ser con el fin de sacar conclusiones más generales sobre algún fenómeno que es posible a partir de los estudios individuales, o puede llevarse a cabo como preludeo a otras actividades de investigación.

✓ **Especificación de la pregunta(s) de investigación.**

Las preguntas de la investigación es la parte más importante de cualquier revisión sistemática. Las preguntas ponen en marcha toda la metodología de revisión sistemática por lo tanto la elaboración debe considerar que:

- El proceso de búsqueda debe identificar los estudios primarios que abordan las cuestiones de investigación.
- El proceso de extracción de datos debe extraer los elementos de datos necesarios para responder a las preguntas.
- El proceso de análisis de datos debe sintetizar los datos de tal manera que las preguntas pueden ser contestadas.

✓ **El desarrollo de un protocolo de revisión.**

Un protocolo de revisión especifica los métodos que se utilizarán para llevar a cabo una revisión sistemática específica. Un protocolo predefinido es necesario reducir la posibilidad de sesgo investigador. Por ejemplo, sin un protocolo, es posible que la selección de los estudios individuales o el análisis puedan ser impulsados por las expectativas del investigador.

6.4.5. Ejecución

Una vez que el protocolo ha sido acordado, el examen adecuado puede comenzar. Sin embargo, como se señaló anteriormente, los investigadores deben esperar a probar cada uno de los pasos que se describen en esta sección cuando construyen su protocolo de investigación.

✓ **Identificación de la investigación**

El objetivo de una revisión sistemática es encontrar el mayor número de estudios primarios relacionados con la pregunta de investigación como sea posible utilizando una estrategia de búsqueda imparcial. El rigor del proceso de búsqueda es un factor que distingue a las revisiones sistemáticas de las revisiones tradicionales.

Es necesario determinar y seguir una estrategia de búsqueda. A continuación, elaborar una lista de palabras clave que van a servir construir sofisticadas cadenas de

búsqueda a continuación, se pueden construir utilizando AND y OR. Paso seguido se especifica las fuentes de búsqueda y se procede a realizar las consultas

Como punto final a este paso se identifica los criterios de inclusión y exclusión que se va aplicar a los estudios encontrados.

✓ **Selección de los estudios primarios**

Una vez que se han obtenido los estudios primarios potencialmente relevantes, que deben ser evaluados por su importancia real. Para esto se describe los criterios de selección que se utilizan para identificar los estudios primarios que proporcionan evidencia directa acerca de la pregunta de investigación. Con el fin de reducir la probabilidad de sesgo, los criterios de selección se decidirán durante la definición del protocolo, aunque pueden ser refinados durante el proceso de búsqueda.

✓ **La extracción de datos y el seguimiento.**

El objetivo de esta etapa es el diseño de formularios de extracción de datos para registrar con precisión la información de los investigadores obtienen a partir de los estudios primarios. Para reducir la posibilidad de sesgo, los formularios de extracción de datos deben ser definidos y pusieron a prueba cuando se define el protocolo de revisión.

✓ **Síntesis de los datos.**

La síntesis de los datos consiste en recopilar y resumir los resultados de los estudios primarios incluidos. Síntesis puede ser descriptivo (no cuantitativa). Sin embargo, a veces es posible complementar una síntesis descriptiva con un resumen cuantitativo utilizando técnica estadísticas.

6.4.6. Publicación de resultados.

La fase final de una revisión sistemática consiste en la redacción de los resultados de la revisión y difusión de los resultados a las partes potencialmente interesadas. Es importante comunicar los resultados de una revisión sistemática de manera efectiva. Por esta razón la mayoría de las guías recomiendan la planificación de la estrategia de difusión durante la etapa de puesta en marcha (si existe) o la hora de preparar el protocolo de revisión sistemática.

Por lo general, las revisiones sistemáticas serán notificadas en al menos dos formatos:

- ✓ En un informe técnico o en una sección de una tesis doctoral.
- ✓ En un artículo de revista o conferencia.

e. Materiales y métodos

1. Materiales

En la Tabla 4 se detalla algunos materiales, que fueron necesarios para el desarrollo del presente trabajo de titulación.

Tabla 4. Materiales

Hardware	
Material	Detalle
Computadora	Para realizar la digitación de todo el proceso
Impresora	Se utilizó en la impresión del trabajo cada que fue necesario.
Dispositivos de almacenamiento	Se utilizó una memoria USB y distintas herramientas de la nube como Dropbox, Mendeley.
Software	
Material	Detalle
Licencia Windows	Contribuyó en el funcionamiento del sistema operativo de la computadora.
Mendeley Desktop	Permitió la gestión bibliográfica para citar o referenciar desde el procesador de texto.
Procesador texto	Facilito la edición del texto y revisión online.

Materiales Varios	
Material	Detalle
Papel	Para la impresión de avances y presentación del trabajo de titulación.
Internet	La principal herramienta pues permitió el acceso a diferentes herramientas utilizadas en la elaboración del presente trabajo.
Transporte	Ayudó a trasladarme y acudir al sitio necesario para culminar el proyecto.
Accesorios de oficina	Necesario para el desarrollo y culminación del trabajo de titulación.
Fuentes de búsqueda	
Material	Detalle
IEEE	Base de datos científica que se utilizó para obtener documentos para el desarrollo de la investigación.
Google Scholar	Base de datos científica que se utilizó para obtener documentos para el desarrollo de la investigación.
ScienceDirect	Base de datos científica que se utilizó para obtener documentos para el desarrollo de la investigación.

2. Métodos

Para el desarrollo del presente trabajo de titulación se utilizará la metodología de acuerdo a la definición de Barbara Kitchenham[3], ya que este es un medio para evaluar e interpretar todas las investigaciones disponibles acerca de tres preguntas en particular de la presente investigación, área temática, o fenómeno de interés, constituyéndose en el más conveniente para el desarrollo de este trabajo de titulación. Al realizar una revisión sistemática debemos cumplir tres etapas: la planificación de la revisión, desarrollo de la revisión e informe de resultados.

1. Planificación de la revisión.

Para el desarrollo de esta investigación se realizan tres actividades como las descritas a continuación.

1.1. Identificación de la necesidad de una revisión

En la actualidad la vulnerabilidad de los sistemas biométricos basados en huellas dactilares, se ha convertido en una amenaza para la seguridad de los sistemas informáticos que permiten el acceso a información o datos dentro de una entidad de índole financiero, militar, incluso en la domótica, instituciones públicas o privadas, ya que hoy en día la huella dactilar es una forma de mantener la identidad de una persona de manera única, lo que permite que se pueda llevar a cabo un sin número de actividades personales como transacciones bancarias, medio de pago, acceso a correos electrónicos, entrada y salida del lugar de trabajo, entre otros, es por ello que surge la necesidad de realizar una revisión sistemática de literatura: Vulnerabilidad de sistemas biométricos basados en huellas dactilares, ya que han sido quebrantadas sus seguridades debido a que el ser humano ha encontrado diferentes algoritmos de suplantación y así acceder con fines maliciosos, lo que permitirá contribuir con información que pueda servir y aportar con este tema.

1.2. Especificación de las preguntas de investigación

Se planteó como objetivo “Realizar una revisión sistemática de Vulnerabilidad de sistemas biométricos basados en huellas dactilares” sobre artículos relacionados al ataque de sistemas biométricos basados en detección dactilar mediante algoritmos

como Hill-Climbing y Side-Channel. En base a esto se proyecta las preguntas de investigación mencionadas en la Tabla 5:

Tabla 5. Preguntas de Investigación

Preguntas de Investigación	
PI01	¿Cuáles son las formas de falsificación de huellas digitales utilizadas para vulnerar sistemas biométricos?
PI02	¿En que se basan los algoritmos utilizados para identificación de falsificación de huellas dactilares en sistemas biométricos?
PI03	¿Qué algoritmos para identificación de falsificación de huellas dactilares en sistemas biométricos ha dado mejores resultados?

1.3. Desarrollo de un protocolo de revisión

El protocolo a seguir es planteado por Barbara Kitchenham que se compone de tres fases y cada fase tiene sus respectivas actividades.

2. Desarrollo de revisión.

2.1. Identificación de la investigación.

Para obtener artículos de calidad que permitan responder a las preguntas de investigación, se llevó a cabo búsquedas avanzadas sobre el área de investigación en bases de datos científicas en línea accesibles. Las bases de datos contienen trabajos publicados de mucho interés en la revisión y son utilizadas por muchos investigadores de Ingeniería en software. Varios artículos fueron descargados de las diferentes bases de datos en función de su relevancia.

Las fuentes de búsqueda se detallan a continuación en la Tabla 6.

Tabla 6. Bases de datos científicas

Bases de datos	URL
GOOGLESCHOLAR Library	https://scholar.google.com
SCIENCEDIRECT Library	http://www.sciencedirect.com .
IEEEXPLORE Library	http://ieeexplore.ieee.org/

Se consideró hacer uso de las bases de datos de la tabla 6, con adecuadas consultas basadas en las palabras clave que se seleccionó tomando en cuenta dos aspectos: las preguntas de investigación y las palabras clave de artículos referentes al tema de investigación revisados con anterioridad[18][19][22][28][38][27][39][26][40][41]. Estas son:

Vulnerability of fingerprint, attacks on biometric systems, biometrics, fingerprint, security, template, attack hill-climbing, attack side-channel in fingerprint, timing attacks.

Una vez definidas las bases de datos e identificadas las palabras clave se realizó las consultas posibles utilizando los operadores lógicos AND y OR, generando con esto las cadenas de búsqueda (CB) que se muestran en la tabla 7. Cabe resaltar que se

estimó como estudio todos los artículos de conferencia, trabajos de universidades realizados y artículos de revistas, además se consideró los artículos que contengan las palabras claves en el abstract y los resultados encontrados en áreas de computación.

Tabla 7. Revisión preliminar y términos

Biblioteca digital	Identificación	Cadena de Búsqueda
IEEE	CB1	vulnerability of fingerprint
IEEE	CB2	Vulnerability biometric system AND hill-climbing
IEEE	CB3	"Abstract":fingerprint AND "Abstract":hill-climbing OR "Abstract":side-channel
Sciencedirect	CB4	TITLE-ABSTR-KEY(biometric fingerprint attack).
Sciencedirect	CB5	TITLE –ABS-KEY(attack hill-climbing fingerprint)
Sciencedirect	CB6	vulnerability of fingerprint
Google Scholar	CB7	Vulnerabilidad de biometria dactilar
Google Scholar	CB8	biometria dactilar ataques hill climbing y side channel

2.2. Selección de estudios primarios.

Luego de aplicar las cadenas de búsqueda y obtener los primeros estudios se describe los criterios de inclusión y exclusión que se va a utilizar para la selección de estudios primarios. Estos son:

Criterios de inclusión

- ✓ Artículos Científicos publicados a partir del 2006, debido a que no existe variedad de artículos más actualizados que colaboren con la investigación específicamente para el tema de la presente revisión sistemática.
- ✓ Material científico que en resumen o en las conclusiones contenga las palabras clave.
- ✓ Artículos que se obtenga como resultado de la búsqueda en el área de tecnología y seguridad.

Criterios de exclusión

- ✓ Publicaciones informales que no siguen una metodología científica.
- ✓ Todas las que no cumplen con los criterios de inclusión.

Los resultados generales de las búsquedas se presentan en la Tabla 8.

Tabla 8. Resultados del fase de selección de artículos incluidos y excluidos.

Biblioteca	Cadena de búsqueda	Total de estudios	Estudios incluidos	Estudios excluidos
IEEE	CB1	146	93	53
	CB2	7	1	6
	C03	18	4	14
	C04	1242	5	1237
ScienceDirect	CB5	1458	29	1429
	CB6	158	68	90
	CB7	3278	186	3092
Google Scholar	CB8	855	517	338
	CB9	12	5	7
Total		13481	1294	12187

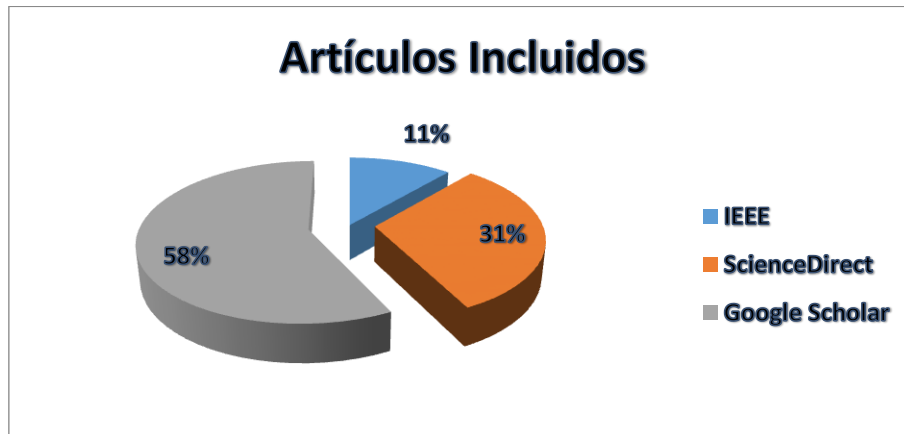


Figura 19. Artículos por base de datos

Una vez aplicado los criterios de inclusión se generó como resultado 1294 documentos siendo: el 58% de la librería Google Scholar, el 31% de ScienceDirect y del 11% de IEEE (Figura 19). El número de artículos revisados fueron 91 que se detallan en la Tabla 24 del Anexo 1.

2.3. Extracción de datos y seguimiento.

Para la selección de estudios basados en la Tabla 24 del Anexo 1 se aplicaron los criterios de selección de estudios que establecen la pauta de extracción de información relevante para este trabajo. Por cada artículo seleccionado, se sintetizaron al menos uno de los siguientes elementos:

- Técnicas de Falsificación, basado en la PI01.
- Resultados de los ataques, basado en la PI03.
- Conclusiones relevantes.

2.4. Síntesis de datos.

El criterio utilizado para la selección de artículos fue: que vulnerabilidad tienen los sistemas biométricos basados en huellas dactilares que son atacados por diferentes formas de ataque algorítmico. Dando como resultado un total de 14 artículos.

Artículos Seleccionados en La Revisión Sistemática.

- ✓ **A01:** A. Roy, S. Member, N. Memon, A. Ross, and S. Member, "MasterPrint : Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems," IEEE Trans. Inf. FORENSICS Secur., vol. 6013, no. 1556, pp. 1–13, 2017
- ✓ **A02:** D. Menotti et al., "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 4, pp. 864–879, 2015.
- ✓ **A03:** G. E. Delgado Parra, "Biometría," Inst. Univ. Politécnico Santiago Mariño Inst. Univ. Tecnol. Agro Ind., no. Instituto Universitario Politécnico Santiago Mariño, 2015.
- ✓ **A04:** E. Maiorana, G. E. Hine, P. Campisi, and S. Member, "Hill-Climbing Attacks on Multi-Biometrics Recognition Systems," IEEE Trans. Inf. FORENSICS Secur., vol. 6013, no. c, pp. 1–16, 2014.
- ✓ **A05:** M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," Forensic Sci. Int., vol. 204, no. 1–3, pp. 41–49, 2011.
- ✓ **A06:** A. H. B. Muñoz, "ATAQUES TIPO 'SIDE-CHANNEL' A SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO DE HUELLA DACTILAR," Univ. Autónoma Madrid Esc. politécnica Super., 2010.
- ✓ **A07:** J. Galbally, J. Fierrez, and J. Ortega-garcia, "Análisis Temporal de Vulnerabilidades de los Sistemas Basados en Huella Dactilar," Biometric Recognit. Gr. ATVS, EPS, Univ. Autónoma Madrid, 2008.
- ✓ **A08:** A. Ribalta, "Seguridad en los Sistemas biométricos," Universidad abierta de Cataluña, 2007.
- ✓ **A09:** D. Maltoni, "A Tutorial on Fingerprint Recognition," Univ. Bol., pp. 43–68, 2006.

- ✓ **A10:** A. K. Jain, A. Ross, S. Pankanti, and S. Member, "Biometrics : A Tool for Information Security," IEEE Trans. Inf. FORENSICS Secur. VOL. 1, NO. 2, JUNE 2006 Biometrics, vol. 1, no. 2, pp. 125–143, 2006.
- ✓ **A11:** U. Uludag and A. K. Jain, "Attacks on Biometric Systems : A Case Study in Fingerprints," Dep. Comput. Sci. Eng. Michigan, vol. 5306, pp. 622–633, 2006.
- ✓ **A12:** E. Politecnica and C. De Cantoblanco, "Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card," Esc. Politec. Super. - Univ. Auton. Madrid, pp. 151–159, 2006.
- ✓ **A13:** M. T. J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-Gonzalez F. Alonso-Fernandez, Javier Ortega-Garcia, "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks," Esc. Politec. Super. - Univ. Auton. Madrid, pp. 130–136, 2006.
- ✓ **A14:** M. M. Díaz, "Vulnerabilidades en sistemas de reconocimiento basados en huella dactilar: ataques hill-climbing," Univ. AUTÓNOMA MADRID Esc. POLITÉCNICA Super. VU, 2006.

f. Resultados

1. Extracción de datos

Una vez aplicados los criterios de selección se obtuvo 14 artículos, de los cuales se extrae la información más relevante. En las tablas de la 8 a la 21 se muestra la información extraída de cada documento seleccionado. Información como: título del artículo seleccionado, técnicas de falsificación, resultados y las conclusiones relevantes presentadas en cada documento analizado.

Tabla 9. Resultados del artículo A01

Nombre del Artículo	Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems
Técnicas de falsificación	
Un sistema biométrico basado en la huella digital es potencialmente vulnerable a una variedad de ataques, es por ello que se han identificado ocho puntos de ataque en un sistema biométrico que pueden agruparse en cuatro categorías, que son: 1. Ataques en la interfaz de usuario (nivel de entrada), 2. Ataques en las interfaces entre módulos, 3. Los módulos, y 4. Ataques a la base de datos. Así también ataques de fuerza bruta y ataques basados en adivinar al diccionario.	
Conclusiones y resultados relevantes	
<ul style="list-style-type: none">Resultados preliminares sobre un conjunto de datos ópticos de huellas dactilares y un conjunto de datos de huellas digitales capacitivas indican que es posible localizar o generar huellas dactilares parciales que pueden usarse para suplantar a un gran número de usuarios. En este sentido, exponemos una vulnerabilidad potencial de sistemas de autenticación parcial basados en huellas dactilares, especialmente cuando se registran varias impresiones por dedoEl trabajo establece el hecho de que es realmente posible realizar un ataque del	

diccionario en un dataset de la huella digital con la exactitud substancial usando un sistema de MasterPrints llamados a huellas dactilares de cierta población de huellas dactilares, cuidadosamente elegido. Las MasterPrints pueden ser huellas dactilares completas o parciales tomadas de un conjunto de datos o diseñadas sintéticamente utilizando un método de escalada.

Tabla 10. Resultados del artículo A02

Nombre del Artículo	Deep Representations for Iris, Face, and Fingerprint Spoofing Detection
Técnicas de falsificación	
<p>Existen técnicas de Ataques directos e indirectos, en donde los ataque directos son los más comunes ya que no necesita el atacante saber mayor información de los diferentes niveles de conocimiento del sistema biométrico, es así que para las huellas dactilares, el método de falsificación más común consiste en el uso de réplicas artificiales creadas de manera cooperativa, donde un molde de la huella digital se adquiere con la cooperación de un usuario válido y se utiliza para replicar la huella digital del usuario con diferentes materiales, Gelatina, látex, play-doh o silicona.</p> <p>Podemos clasificar los métodos de detección de falsificación de huellas dactilares a grandes rasgos en dos grupos: basados en hardware (explorando sensores adicionales) y soluciones basadas en software (basándose únicamente en la información obtenida por el sensor de adquisición estándar del sistema de autenticación)</p>	
Conclusiones y resultados relevantes	
<ul style="list-style-type: none"> • Los resultados indican fuertemente que los sistemas de detección de falsificación 	

basados en redes convolucionales pueden ser robustos a ataques ya conocidos y posiblemente adaptados, con poco esfuerzo, a ataques basados en imágenes que aún están por venir.

Tabla 11. Resultados del artículo A03

Nombre del Artículo	Biometría
Técnicas	
<p>Se puede considerar algunas características para la selección de tecnología biométrica y su aplicabilidad como:</p> <p>a). Universalidad: Todas las personas tienen o presentan una característica. b). Singularidad: Dos personas cualesquiera son distinguibles una de la otra en base de sus características. c). Estabilidad: La característica tiene que ser lo suficientemente estable a lo largo del tiempo y en condiciones ambientales diversas. d). Cuantificable: La característica tiene que ser medible cuantitativamente. e). Aceptabilidad: El nivel de aceptación de la característica por parte de las personas debe ser suficiente como para ser considerada parte del sistema de identificación biométrico. f). Rendimiento: El nivel de exactitud requerido debe ser elevado para que la característica sea aceptable. g). Usurpación: Permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas.</p>	
Conclusiones relevantes	
<ul style="list-style-type: none"> • En función de las características que se usan en la identificación del individuo se distinguen dos áreas: Biometría Estática, que se basa en el estudio de las características físicas del ser humano y la Biometría Dinámica que estudia las características de la conducta del ser humano basados en el proceso de identificación de rasgos derivados de una acción realizada. • El acceso a negocios y servicios necesitan garantías de seguridad las cuales 	

deben estar enmarcadas en técnicas exhaustivas de identificación mediante hardware y aplicaciones que cumplan estas tareas en lapsos de tiempos cortos con un alto grado de precisión. La tendencia del mercado está orientada a la creación de nuevos elementos biométricos que permitan la lectura de varios rasgos físicos del cuerpo humano para ofrecer un grado de certeza amplio, confiable y seguro.

Tabla 12. Resultados del artículo A04

Nombre del Artículo	"Hill-Climbing Attacks on Multi-Biometrics Recognition Systems"
Técnicas de falsificación	
<p>Los ataques de escalada son ejecutados iterativamente Representaciones sintéticas de la biometría del usuario atacado hasta que se logra el reconocimiento exitoso. En cada paso, los datos empleados se modifican de acuerdo con los resultados de intentos anteriores, expresados en términos de puntuaciones coincidentes, que se supone que son conocidas por el atacante, con el fin de mejorar la salida de coincidencia resultante. No es necesario conocer a priori ninguna información específica sobre el usuario objetivo para llevar a cabo esta estrategia: de hecho, sólo se necesita información estadística sobre las características de las plantillas empleadas. Tales ataques pueden ser perpetrados tanto en el módulo de extracción de características como en el módulo de sincronización.</p> <p>Los ataques Hill-Climbing también pueden realizarse dirigiéndose al módulo matcher, con el objetivo de generar plantillas sintéticas que permitan un reconocimiento exitoso. Específicamente, las plantillas de diafragma binario basadas en el modelo de hoja de caucho son generadas sintéticamente y modificadas en píxeles hasta el reconocimiento exitoso</p>	

Conclusiones y Resultados relevantes

- La huella dactilar es, sin duda, la modalidad más utilizada en los sistemas de reconocimiento biométrico. Su procesamiento implica el análisis de patrones de cresta y valle en la superficie de un dedo, que tradicionalmente consiste en la extracción de anomalías locales de crestas tales como bifurcaciones o terminaciones, llamadas puntos de minucias.
- Se ha observado que los ataques de escalada pueden representar una amenaza significativa para los sistemas biométricos, requiriendo menos esfuerzo que un ataque de fuerza bruta para romper con éxito el sistema. La cuantificación de puntuación no uniforme también se ha analizado como una posible contramedida a los ataques de escalada, observando su efectividad en el aumento de la robustez de los sistemas sin un empeoramiento significativo del desempeño de la verificación.

Tabla 13. Resultados del artículo A05

Nombre del Artículo	"Vulnerabilities of fingerprint reader to fake fingerprints attacks"
Técnicas de falsificación	
Se observa que existen diferentes materiales para realizar falsificación de huellas dactilares como: moldes termoplásticos, gelatina, silicona, silicio, acetato, y según la calidad del dispositivo hacen que exista cierta vulnerabilidad o acceso a la seguridad.	
Conclusiones relevantes	
<ul style="list-style-type: none"> • Las puntuaciones producidas por este tipo de huellas digitales falsas son más altas que las producidas por las huellas dactilares falsas elaboradas a partir de modelos indirectos. Por otra parte, el número de pasos implicados en su elaboración es más bajo; Reduce así los riesgos de pérdida o modificación de la información relativa a la impresión. Sin embargo, las huellas dactilares falsas presentan puntuaciones aún inferiores a las producidas por huellas dactilares 	

reales. La etapa de moldeo y la retirada del dedo del material de moldeo pueden efectivamente introducir modificaciones en pequeñas partes del patrón, como las construcciones producidas por movimientos involuntarios del dedo o una eliminación demasiado prematura, o incluso pérdida de información, tal como arrancar durante la etapa de extracción. Esta modificación o pérdida de información puede reducir las puntuaciones asociadas a la impresión. Los materiales utilizados para la fabricación de moldes influyen en la calidad.

- Este experimento mostró que las puntuaciones calculadas para cada transacción de un mismo sujeto y dedo son bastante estables, en particular considerando las huellas dactilares falsas. Las huellas dactilares falsas son reproducciones de grabados originales. No hay actividad fisiológica y la textura no es idéntica a la textura de la piel, por lo tanto, es normal que las transacciones muestran pequeñas variaciones. En cuanto a la estabilidad de la diferencia observada entre las muestras, hay que señalar que el patrón, la calidad de la impresión y el sujeto a personificar tienen una influencia en la calidad de la huella digital falsa.

Tabla 14. Resultados del artículo A06

Nombre del Artículo	"SIDE-CHANNEL' A SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO DE HUELLA DACTILAR"
Técnicas de falsificación	
1. Ataques al sensor o escáner (punto 1). 2. Ataques al módulo extractor de características (punto 3). 3. Ataques al módulo comparador (punto 5). 4. Ataques a la base de datos del sistema (punto 6). 5. Ataques a los distintos canales de comunicación entre los módulos existentes en el sistema (puntos 2, 4, 7 y 8).	
<pre> graph TD 1[1 Sensor] -- 2 --> 3[3 Extractor de características] 3 -- 4 --> BD[(Base de datos)] IS[Identidad solicitada] -- 6 --> BD BD -- 7 --> 5[5 Comparador] 5 -- 8 --> S[Score] S --> D[Decisión] </pre>	

El ataque al sensor o escáner es un tipo de ataque directo al sistema, y en él, el atacante no tiene ningún conocimiento sobre el funcionamiento de dicho sistema. El resto de ataques se denominan indirectos y van dirigidos a alguno de los módulos internos del sistema. En ellos el impostor necesita de algún tipo de conocimiento sobre el funcionamiento o estructura interna del sistema (por ejemplo, características extraídas o el formato de la plantilla).

Ataque de software Side-Channel, se produce cuando un atacante es capaz de utilizar información adicional obtenida de la implementación física de un sistema criptográfico. Si la información side-channel es suficiente, permitirá romper un sistema cifrado.

Dentro del ataque side-channel, existe uno basado en la información temporal que ha demostrado tener una gran eficiencia. Estos ataques denominados timing-attacks se han convertido en una amenaza real a tener en cuenta a la hora de implementar sistemas de seguridad.

Conclusiones y resultados relevantes

- Se ha podido corroborar con este ataque que la correlación entre puntuación y tiempo existe. Por tanto, podemos afirmar que los sistemas de reconocimiento automático de huella dactilar basados en minucias son potencialmente vulnerables a ataques side-channel en función del tiempo y que es necesario tenerlos en cuenta a la hora de diseñar este tipo de aplicaciones.
- Los resultados de este ataque no han conseguido acceder al sistema para ninguna huella o puntuación inicial establecida, pero si se ha conseguido un aumento en la puntuación razonable. Además, se ha corroborado que existe una relación entre puntuación y tiempo y por tanto que los sistemas de reconocimiento automático de huella dactilar basados en minucias son potencialmente vulnerables a este tipo de ataques

Tabla 15. Resultados del artículo A07

Nombre del Artículo	“Análisis Temporal de Vulnerabilidades de los Sistemas Basados en Huella Dactilar,”
Técnicas de falsificación	
<p>Los ataques de tipo hill-climbing: Estos algoritmos de ataque generan un determinado número de plantillas sintéticas que se modifican según un proceso iterativo de acuerdo a la puntuación que producen al ser comparadas con la plantilla atacada: si en cada iteración la puntuación aumenta los cambios se mantienen y si no se descartan. De esta forma el score va aumentando hasta que se alcanza el umbral de aceptación y se rompe el sistema.</p>	
Conclusiones y resultados relevantes	
<ul style="list-style-type: none"> • A pesar de que los ataques de tipo hill-climbing han probado su eficiencia a la hora de romper los sistemas biométricos, presentan la fuerte restricción de necesitar la puntuación devuelta por el comparador para poder acceder a la aplicación. De hecho, incluso en el caso de que el atacante obtenga la medida de similitud, el ataque aún se puede prevenir cuantificando la puntuación de forma que el algoritmo hill-climbing no obtenga la realimentación necesaria por parte del sistema que permita ejecutar el proceso iterativo de aumento de la medida de similitud. 	

Tabla 16. Resultados del artículo A08

Nombre del Artículo	“Seguridad en los Sistemas biométricos”
Técnicas de falsificación	
<ul style="list-style-type: none"> • Ataques de suplantación de la persona (spoofing - falsificación) va dirigido a obtener acceso ilícito a un recurso. El tipo de ataque consiste en suplantar la identidad de un usuario con acceso al recurso deseado. 	

- Ofuscación biométrica (obfuscation) va dirigida a falsear o enmascarar los datos biométricos, antes o después de la adquisición de estos por parte del sistema, para evitar que el sistema reconozca a un individuo.
- Ataque de denegación de servicio (denial of service) está dirigido a retrasar, detener o degradar la calidad del sistema.
- Los ataques de conspiración, el usuario, posiblemente por soborno, facilita el acceso al sistema. En los ataques de coacción, la víctima, posiblemente bajo amenaza o chantaje, facilita el acceso al sistema. Estas vulnerabilidades evaden el sistema de seguridad, puesto que los datos son verdaderos.
- Ataques a los módulos de verificación del sistema biométrico.
- Los ataques side-channel se basan en obtener este resultado del algoritmo de comparación que cuantifica la validez del dato biométrico pre- sentado en el sistema, analizando el tiempo de ejecución, el consumo de energía de la máquina, las ondas electromagnéticas desprendidas o simplemente el ruido producido.

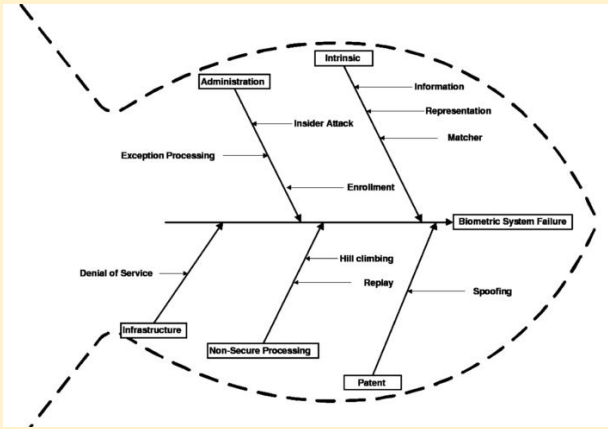
Conclusiones y resultados relevantes

Estos tipos de ataques se aplican habitualmente a sistemas criptográficos a pesar de que se pueden adaptar fácilmente para ser aplicados a sistemas biométricos. Los ataques basados en tiempo consisten en el análisis del tiempo de cálculo usado para ejecutar el algoritmo de comparación. Es fácil ver que este tiempo depende fuertemente de los datos de entrada. Varios experimentos han demostrado que los algoritmos usados en las comparaciones de los datos suelen usar más tiempo en la comparación de datos incorrectos que en la comparación de datos correctos. Los ataques basados en el análisis de la cantidad de energía, pérdidas electromagnéticas y de ruido van dirigidos en la misma dirección

Tabla 17. Resultados del artículo A09

Nombre del Artículo	"A Tutorial on Fingerprint Recognition"
Técnicas de falsificación	
<p>Un sistema biométrico basado en huellas dactilares es esencialmente un sistema de reconocimiento de patrones que reconoce a una persona al determinar la autenticidad de su huella digital. Dependiendo del contexto de la aplicación, un sistema biométrico basado en huellas digitales puede ser llamado un sistema de verificación o un sistema de identificación:</p> <ul style="list-style-type: none"> • un sistema de verificación autentica la identidad de una persona comparando las huellas dactilares capturadas con su propia plantilla biométrica previamente almacenada en la sistema. Conduce una comparación uno a uno para determinar si la identidad reclamada por el individuo es verdadera; • un sistema de identificación reconoce a una persona buscando en la base de datos completa de la plantilla una coincidencia. Realiza comparaciones uno a muchos para establecer la identidad del individuo. 	
Conclusiones y resultados relevantes	
<ul style="list-style-type: none"> • La mayoría de los enfoques de emparejamiento de huellas digitales introducidos en las últimas cuatro décadas son las Minucias, pero recientemente las técnicas basadas en la correlación están recibiendo renovado interés. Se han propuesto nuevos métodos basados en la textura y la integración de enfoques basados en diferentes características parece ser la forma más prometedora de mejorar significativamente la precisión de los sistemas de reconocimiento de huellas dactilares. 	

Tabla 18. Resultados del artículo A10

Nombre del Artículo	“Biometrics : A Tool for Information Security,”
Técnicas de falsificación	
<p>El diagrama de la figura de fallas biométricas muestra la seguridad proporcionada por un sistema biométrico se puede socavar debido a una variedad de razones. (A) Administración: Se puede abusar de la capacidad administrativa del sistema para comprometer la integridad del sistema. (B) Intrínseco: La limitación inherente en el contenido de la información, y los esquemas de representación / concordancia pueden resultar en la aceptación errónea de un intruso. (C) Infraestructura: Un ataque de denegación de servicio puede desactivar la funcionalidad del sistema. (D) Procesamiento no seguro: Un hacker podría explotar la naturaleza del proceso adoptado por el sistema para acceder fraudulentamente al sistema. (E) Patente: Los identificadores biométricos no son secretos y, por lo tanto, un intruso, aunque desconocen las complejidades del sistema, podrían crear artefactos físicos o digitales para engañar al sistema.</p>  <p>El diagrama ilustra las causas de la falla de un sistema biométrico. Se muestra un camino central que conduce a 'Biometric System Failure'. Los factores que contribuyen a esta falla se agrupan en cinco categorías principales:</p> <ul style="list-style-type: none"> Administración: Incluye 'Insider Attack' y 'Exception Processing'. Intrínseco: Incluye 'Information', 'Representation', 'Matcher' y 'Enrollment'. Infraestructura: Incluye 'Denial of Service'. Procesamiento no seguro: Incluye 'Non-Secure Processing'. Patente: Incluye 'Hill climbing', 'Replay' y 'Spoofing'. <p>Las flechas indican que cada una de estas categorías contribuye directamente a la falla del sistema.</p>	
Conclusiones y resultados relevantes	
<ul style="list-style-type: none"> • Si bien la tecnología biométrica puede mitigar algunos de los problemas de inscripción (por ejemplo, múltiples identidades), no puede resolver el problema de 	

tener que confiar en sistemas de gestión de identidad heredados imperfectos.

- Los ataques de esfuerzo cero: los rasgos biométricos de un intruso oportunista pueden ser suficientemente similares a un individuo legítimamente rodado, lo que resulta en un False Match y una violación de la seguridad del sistema. Este suceso se relaciona con la probabilidad de observar un grado de similitud entre las plantillas originarias de diferentes fuentes por azar.
- Ataques adversos: Se refiere a la posibilidad de que un impostor determinado pueda disfrazarse como un usuario enrollado usando un artefacto físico o digital de un usuario legítimamente inscrito. Un individuo también puede manipular deliberadamente su rasgo biométrico para evitar la detección mediante un sistema biométrico automatizado.

Tabla 19. Resultados del artículo A11

Nombre del Artículo	"Attacks on Biometric Systems: A Case Study in Fingerprints,"
Técnicas de falsificación	
Existen los ataques mediante la falsificación de huellas dactilares ya sea con la cooperación o no del usuario que pertenece al sistema biométrico.	
Ataque mediante el algoritmo Hill-Climbing.	
Conclusiones y Resultados relevantes	
<ul style="list-style-type: none"> • Se encontró que los dedos gomosos se podrían inscribir en todos los 11 sistemas, y se aceptaron con una probabilidad de 68-100%. Cuando el propietario no coopera, una huella digital residual de una placa de vidrio se realiza con un adhesivo. Después de capturar una imagen de la impresión, el procesamiento basado en PCB similar a la operación descrita anteriormente se utiliza para crear los dedos gomosos. Todos los 11 sistemas inscribieron los dedos gomosos y aceptaron los dedos gomosos con más del 67% de probabilidad. 	

- Para superar tales falsos ataques biométricos, se propuso dos métodos basados en software (no basados en sensores que miden la temperatura, la conductividad, etc.) para la detección de vivacidad de huellas dactilares. Utilizaron un sensor capacitivo comercialmente disponible y la única entrada al módulo de detección de vivacidad es ubicando 5 segundos las huellas dactilares. En su método estático, la periodicidad de los poros de sudor a lo largo de las crestas se utiliza para la detección de la vivacidad. En el método dinámico, se mide el patrón de difusión del sudor a lo largo del tiempo a lo largo de las crestas.
- Tras analizar la viabilidad de los ataques contra los sistemas biométricos basados en huellas dactilares, hemos demostrado que el propuesto sistema atacante es bastante efectivo, al romper en cuentas protegidas con plantillas compuestas de puntos característicos la ubicación y la información sobre el ángulo. El sistema fue capaz de sintetizar las plantillas que garantiza una identificación positiva en un número relativamente pequeño de intentos (271 en promedio). Aunque nos propuso varias medidas para contrarrestar tales ataques, cada uno tiene sus propias limitaciones, especialmente para los sistemas biométricos multimodales. Actualmente estamos trabajando en sistemas de ataque modificado con el objetivo de disminuir el número de intentos aún más.

Tabla 20. Resultados del artículo A12

Nombre del Artículo	"Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card,"
Técnicas de falsificación	
<p>Los ataques de Hill-Climbing consisten en una aplicación que envía plantillas de minucias generadas sintéticamente al atacante y, de acuerdo con la puntuación de coincidencia, modifica aleatoriamente las plantillas hasta que se excede el umbral de decisión. Lleva a cabo ataques de escalada contra el NFIS2 Sistema de referencia y un sistema Match-on-Card (MoC), y luego estudiar algunos factores implicados en la tasa de éxito del ataque. También se hace una comparación directa entre nuestros</p>	

ataques de escalada y los ataques de fuerza bruta.

Conclusiones y resultados relevantes

En este trabajo, se ha realizado y estudiado Hill- Climbing aplicado al sistema de referencia NFIS2 y un sistema integrado Match-on-Card. NFIS2 es un sistema de reconocimiento de huellas dactilares basado en PC, mientras que el sistema MoC es un sistema de hardware limitado. Como se ha demostrado, el rendimiento del algoritmo de ataques depende en gran medida del sistema que este bajo el ataque y de las iteraciones que se realizan. Los ataques con un número reducido de minucias son muy exitosos contra el sistema MoC, mientras que su desempeño contra NFIS2 es muy pobre.

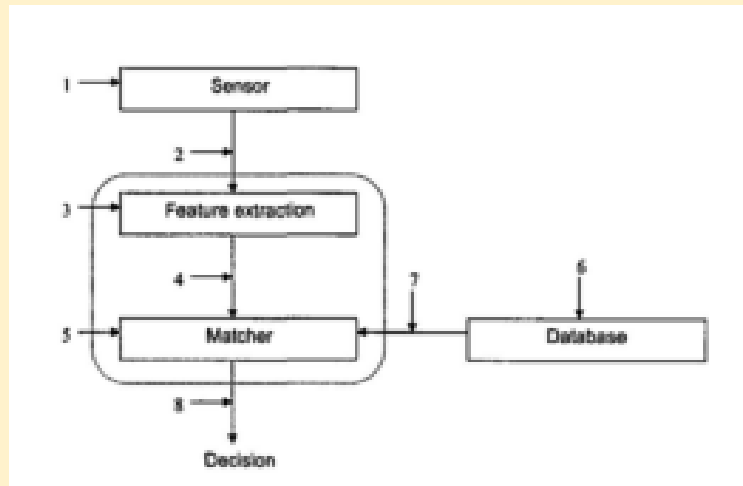
NFIS2 ha demostrado ser más robusto contra el algoritmo Hill-Climbing, al menos con un número reducido de iteraciones. Por otro lado, si permitimos un mayor número de iteraciones (como 5000 en los experimentos), la mayoría de las cuentas se pueden romper. Puede ser derivado de los resultados que los ataques de escalada de montaña son menos efectivos que los ataques de fuerza bruta, al menos en el caso de NFIS2. Esta declaración debe tomarse con cuidado, ya que los ataques de escalada requieren mucho menos recursos que los que necesita un ataque de fuerza bruta. De hecho, para realizar un ataque eficaz de fuerza bruta, el atacante debe tener una base de datos de más de mil plantillas de huella digital real, mientras que no hay necesidad de plantillas reales en el caso de un ataque de escalada.

Tabla 21. Resultados del artículo A13

Nombre del Artículo	"Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks,"
Técnicas de falsificación	
La creación de plantillas gomosas ha generado que exista la falsificación física de las huellas dactilares que afectan a sensor que realiza la obtención de la huella para su	

verificación. Es así que, hay ataques pueden agruparse en dos clases genéricas:

i) Ataques directos, en los que el intruso no tiene ningún conocimiento sobre el funcionamiento del sistema y que comprende ataques de tipo 1 como lo muestra la figura, y ii) Ataques indirectos en los que el impostor tiene algún conocimiento sobre el funcionamiento interno del sistema (por ejemplo, la forma en que se almacenan los datos) y que comprende todos los 7 ataques restantes de la figura.



Resultados

Un nuevo método para generar dedos gomosos fue generada y se describió una base de datos de huellas digitales falsas de tamaño medio y se evaluaron dos sistemas de verificación de huellas dactilares diferentes, uno basado en minucias y otro basado en crestas. Tres escenarios diferentes fueron considerados en los experimentos, a saber: i) inscripción y prueba con huellas digitales reales, ii) inscripción y prueba con huellas dactilares falsas y iii) inscripción con huellas dactilares reales y prueba con imitaciones falsas. Resultados para un óptico y un barrido térmico sensores se dieron. El sistema de verificación de huellas dactilares NIST funciona mejor. Debido a la diferente tecnología utilizada en ambos casos. El sensor óptico se basa en los efectos de refracción de la luz que tienen lugar de manera similar tanto en la piel como en el silicona, por lo que obtenemos imitaciones de buena calidad. Por otra parte, el sensor térmico se basa en la diferencia de temperatura entre crestas y valles que es casi inexistente en las huellas dactilares de silicona. Aunque las imitaciones se calientan al

respirar para obtener la diferencia de temperatura necesaria, la calidad de las muestras es muy pobre.

Conclusiones relevantes

Con el sensor óptico pero también es más vulnerable a los ataques directos en comparación con los experimentos con el sensor térmico. El rendimiento general del sistema basado en crestas fue peor que la basada en minucias, sin embargo, mostró ser menos vulnerable a ataques directos y también fue más resistente a muestras de baja calidad.

Tabla 22. Resultados del artículo A14

Nombre del Artículo	“Vulnerabilidades en sistemas de reconocimiento basados en huella dactilar: ataques hill-climbing,”
Técnicas de falsificación	
Ataques software denominado hill-climbing: El ataque es de tipo 4, es decir, ataca directamente el matcher y no utiliza información alguna de la imagen de la huella. Emplea exclusivamente patrones sintéticos de minucias generados aleatoriamente o según una distribución que se estime aproximada a la huella, basada en histogramas de minucias de las huellas de una base de datos. Únicamente es necesario conocer cuál es el sensor, para así saber cuál es su resolución y el tamaño de las imágenes que genera. Esta premisa es fácil de cumplir ya que los sensores suelen estar expuestos a la vista y la información acerca de los mismos es publicada por los fabricantes.	
Conclusiones y Resultados relevantes	
En los ataques realizados sobre ambos sistemas se observa una tasa de éxito muy	

diferente. El sistema NFIS2 se muestra mucho más robusto frente a ataques hill-climbing, al menos con un número reducido de iteraciones. En cambio, se puede observar que si se permite un número mayor de iteraciones como en este caso, de 5000, la mayoría de los ataques supera el umbral de decisión.

En el caso del sistema Match-on-Card se obtienen tasas de éxito más altas, y de nuevo, permitiendo un número mayor de iteraciones, en este caso de 2000, se logran realizar la mayoría de ellos con éxito.

Dado que un ataque hill-climbing requiere para su funcionamiento la puntuación obtenida en el matcher o comparador, la solución más trivial para proteger un sistema de esta clase de ataques sería la de que el matcher no revelase la puntuación sino simplemente la indicación de aceptación o rechazo por parte del sistema. Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que empleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible.

Otra solución propuesta para defender un sistema de esta clase de ataques es encriptar la puntuación de salida para que no se pueda conocer su valor real. Una última solución posible es la de restringir el número de intentos de acceso al sistema por parte de un mismo usuario en un cierto periodo de tiempo.

2. Síntesis de datos.

En la Tabla 23, se presenta el resumen del proceso de selección de estudios de cada etapa. Las búsquedas realizadas generaron un total de 7174 trabajos encontrados, obteniendo 908 artículos al aplicar los criterios de inclusión y exclusión, es decir el número de artículos revisados fueron 91, de los mismos se seleccionaron 14 artículos de acuerdo al criterio de selección.

Tabla 23. Resultados de selección de estudios primarios.

Base de Datos	Encontrados	Coincidencias	Revisados	Seleccionados
IEEE	1413	103	21	6
ScienceDirect	4894	283	28	4
GoogleScholar	867	522	42	4
Total	7174	908	91	14

En la figura 20, se muestra que la mayor cantidad de artículos seleccionados son los publicados en el año 2006, seguido del año 2015 y del 2010, pero hay un solo artículo seleccionado por los años 2007, 2008, 2011, 2014 y 2017, debido a que no existe variedad de artículos para el tema de estudio específico abordado en este trabajo, cabe mencionar que por esta razón se ha tomado en consideración como criterio de inclusión artículos con mayor antigüedad.

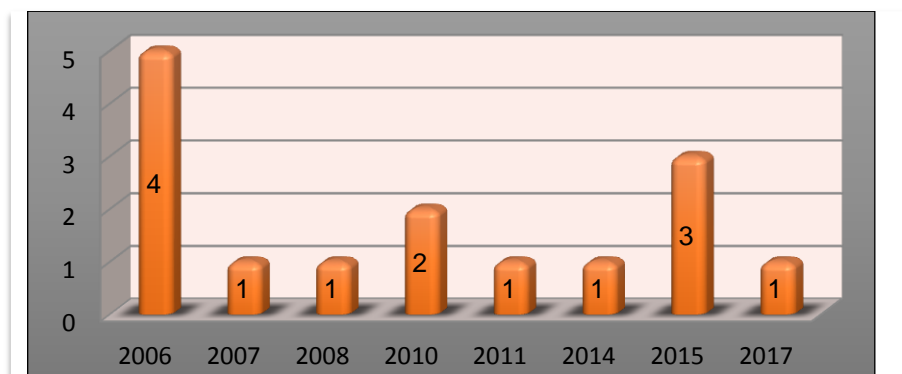


Figura 20. Artículos seleccionados por año.

Luego de extraer la información de cada estudio seleccionado se puede observar que de los problemas abordados en los mismos, la mayoría de documentos mencionan la de falsificación de huellas dactilares a través de materiales sintéticos que intentan vulnerar el sensor biométrico de huella dactilar, así como también otras formas de ataque mediante algoritmos como Hill.Climbing y Side-Channel, que vulneran la seguridad a nivel del comparador de patrones y tiempo.

g. Discusión

1. Discusión de la Revisión Sistemática

- No hay una solución única hasta el momento que pueda eliminar las vulnerabilidades y prevenir ataques maliciosos. Por cuanto, depende también de la tecnología con la que se cuenta, ya que con el método básico de falsificación al sistema biométrico de huella dactilar, se puede acceder luego de realizar varios intentos y según la calidad del material sintético utilizado para duplicar la huella dactilar.
- Se menciona en A09 que un sistema biométrico basado en huellas dactilares es esencialmente un sistema de reconocimiento de patrones que reconoce a una persona al determinar la autenticidad de su huella digital. Dependiendo del contexto de la aplicación, un sistema biométrico basado en huellas digitales puede ser llamado un sistema de verificación que es cuando ya existe en la base de datos el patrón de huella para permitir el acceso determinando si es verdadero o no, y un sistema de identificación que es la parte donde un usuario ingresa el patrón a ser guardado para establecer la identidad de un usuario.
- En A03 se menciona las características que se puede tomar en cuenta para seleccionar tecnología biométrica que se acople a la usabilidad que se desea dar según el tipo de organización o información que se quiere colocar seguridad, los mismos que son: a). Universalidad: Todas las personas tienen o presentan una característica. b). Singularidad: Dos personas cualesquiera son distinguibles una de la otra en base de sus características. c). Estabilidad: La característica tiene que ser lo suficientemente estable a lo largo del tiempo y en condiciones ambientales diversas. d). Cuantificable: La característica tiene que ser medible cuantitativamente. e). Aceptabilidad: El nivel de aceptación de la característica por parte de las personas debe ser suficiente como para ser considerada parte del sistema de identificación biométrico. f). Rendimiento: El nivel de exactitud requerido debe ser elevado para que la característica sea aceptable. g). Usurpación: Permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas. Por lo tanto los avances de la

biometría están reflejados en las investigaciones que patrocinan las empresas de tecnología a nivel mundial, con el constante estudio del cuerpo humano para ser identificado de forma tecnológica como ser único, es por ello indispensable el uso de dos o más elementos biométricos para ofrecer un alto grado de seguridad.

- En A01 se hace referencia a que un sistema biométrico basado en la huella digital es potencialmente vulnerable a una variedad de ataques, identificando ocho puntos de ataque en un sistema biométrico que pueden agrupar en cuatro categorías, que son: 1. Ataques en la interfaz de usuario (nivel de entrada), 2. Ataques en las interfaces entre módulos, 3. Los módulos, y 4. Ataques a la base de datos. Dando como resultado que existen ataques llamados de fuerza bruta y basados en adivinar el diccionario.
- En A02, A05, A08 y A11 coinciden en que hay ataques continuos a la seguridad de los sistemas biométricos a través de la creación de huellas sintéticas en materiales gomosos como silicona, play-doh (plastilina), gelatina, ya sea con la cooperación o no del usuario conducen a la falsificación en la parte inicial del sistema de biometría como es el sensor, dando como resultado el acceso a la información en la mayoría de intentos realizados con el fin de vulnerar el sistema de acceso.
- A04, A07, A11, A12 y A14 mencionan que los ataques mediante el algoritmo Hill-Climbing permite vulnerar el sistema biométrico ya que requiere para su funcionamiento la puntuación obtenida en el matcher o comparador, la solución más trivial para proteger un sistema de esta clase de ataques sería la de que el matcher no revelase la puntuación sino simplemente la indicación de aceptación o rechazo por parte del sistema. Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que empleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible. Por lo tanto este ataque puede representar una amenaza significativa para los sistemas biométricos, requiriendo menos esfuerzo que un ataque de fuerza bruta para romper con éxito el sistema.

- Según A06 y A08 menciona que existen diferentes formas de atacar al sistema biométrico a través de la suplantación o falsificación, ofuscación biométrica, denegación del servicio, ataque de conspiración, estos ataques van dirigidos a usar la falsificación con la cooperación o no del usuario y los ataques a los módulos verificación del sistema biométrico que es donde usan software como el side-Channel que se basa en obtener el resultado del algoritmo de comparación que cuantifica la validez del dato biométrico presentado en el sistema, analizando el tiempo de ejecución, el consumo de energía de la máquina, las ondas electromagnéticas desprendidas o simplemente el ruido producido. Si la información side-channel es suficiente, permitirá romper un sistema cifrado.

2. Desarrollo de la propuesta alternativa

El tema planteado para el presente trabajo de titulación es “**Revisión Sistemática de Literatura: Vulnerabilidad de sistemas biométricos basados en huellas dactilares**”, se lo propuso considerando algunos aspectos, en primer lugar esta área de investigación todavía es novedosa teniendo en cuenta que el asunto a tratar son las vulnerabilidades que esta tecnología mantiene en cuanto a seguridad de la información. En segundo lugar para el exitoso desarrollo de este se cuenta con una gama de métodos aplicables al área de investigación, para este caso se decidió utilizar una revisión sistemática considerando que es una de las pocas que se direcciona a la ingeniería y además cuenta con un protocolo claramente establecido y estandarizado que asegura la claridad y transparencia en el proceso de revisión. Para poder realizar con normalidad este Trabajo de Titulación se cumplió con los siguientes objetivos:

2.1. Planificar la Revisión Bibliográfica para obtener información primaria

Para desarrollar este objetivo se identificó la necesidad de realizar la revisión sistemática que es conocer cuáles han sido los avances en cuanto a seguridad de los sistemas biométricos de huella dactilar y que vulnerabilidades o ataques han sido abordados. Seguidamente se realizó el paso más importante de una revisión que es la especificación de las preguntas de investigación, las mismas que guiaron en la forma de recolectar los estudios, como controlar si los estudios son elegibles y como llevar a cabo el análisis. Para culminar se propone el protocolo de revisión a seguir que es el de Barbara Kitchenham.

2.2. Realizar un proceso de revisión sistemática para estudios primarios.

El desarrollo de la revisión comenzó con la elección de las fuentes de información considerando la accesibilidad a la web así como la inclusión de motores de búsqueda que permitan realizar consultas avanzadas, luego con las palabras claves ya definidas se realizó concatenaciones utilizando los operadores lógicos AND y OR para formar las cadenas de búsqueda que nos sirvieron para recopilar 91 estudios primarios los mismos que luego de pasar por los criterios de selección se redujeron a 14 estudios

relevantes los cuales se analizó y se sintetizó los aspectos principales tomando en consideración las técnicas de falsificación, problemas de seguridad, resultados y conclusiones relevantes.

2.3. Analizar los algoritmos de ataque a la vulnerabilidad de los sistemas biométricos basados en huellas dactilares.

Mediante la investigación realizada durante el objetivo 2 se observó algoritmos que atacan al sistema biométrico basado en huellas dactilares como el Hill-Climbing que se basa en la modificación de patrones o templates que se han guardado en la base de datos, así también el algoritmo de ataque Side-Channel que está basado en el tiempo, ya que consiste en monitorizar el movimiento de datos que entra y sale de la CPU o la memoria. Sabiendo el tiempo que tarda en mover cierta información es posible saber la longitud que puede tener una clave, o de manera más clara, la longitud que seguro no va a tener.

2.4. Sintetizar la información recopilada en la revisión sistemática.

Luego de cumplir rigurosamente el proceso del objetivo 2 y 3 se procedió a sintetizar la información a través de una discusión entre los aspectos relevantes de los 14 estudios utilizados para esta Revisión Sistemática tomando en cuenta técnicas de falsificación, problemas de seguridad, resultados y conclusiones relevantes.

Se pudo evidenciar en el transcurso de la Revisión que no existe gran cantidad de información con respecto a los algoritmos que atacan la vulnerabilidad de los sistemas biométricos basados en huella dactilar, además de no encontrarse datos más actualizados, pese a esto se logró concluir con éxito la investigación rescatando valiosos resultados que ayudaron a emitir las respectivas conclusiones y a finalizar el presente Trabajo de Titulación.

3. Valoración Social, Técnica, Económica y Científica

La valoración del Trabajo de Titulación se expresa describiendo los beneficios presentados en cuatro aspectos:

3.1. Valoración Social

- Conocer las formas de falsificación de huellas dactilares.
- Conocer el procedimiento adecuado para la realización de Revisiones Sistemáticas.
- Conocer en que se basan los algoritmos de identificación de huella dactilar para evitar ser atacados por agentes maliciosos.

3.2. Valoración Técnica

- A través del gestor bibliográfico Mendeley se ahorró tiempo ya que este permite organizar las referencias de manera sencilla desde las fuentes y de varios modos.
- El uso de los navegadores de internet permitió el acceso a las bases de datos que contienen información o artículos que aportaron para la realización del presente trabajo de titulación.
- El uso del correo electrónico y las redes sociales permitió la constante comunicación entre el investigador y el director del Trabajo de Titulación

3.3. Valoración Económica

- Uno de los principales beneficios es el aporte de la UNL con el control y seguimiento del Trabajo, ya que cubre los gastos del Tutor o Director de Tesis.
- El uso de herramientas tecnológicas colaboro al ahorro de tiempo y dinero pues se evitó realizar impresiones innecesarias así como asistencias personales a la UNL.

3.4. Valoración Científica

- ✓ El beneficio en el aspecto científico radica en el aporte de trabajos futuros que resultaron del proceso de la investigación.

h. Conclusiones

- ✓ Se cumplió exitosamente todos los parámetros propuestos en el protocolo de Kitchenham como es: Planificación de la Revisión, Ejecución de la Revisión y Publicación de Resultados. Cabe resaltar que gracias a este autor se aseguró calidad, consistencia, y transparencia en el proceso de la Revisión Sistemática..
- ✓ Se puede concluir que existen algunas bibliotecas científicas como IEEE, Science Direct que permiten realizar la investigación con búsquedas avanzadas, ya sea en base a palabras clave que se encuentren tanto en los títulos, abstract o resumen, concatenadas con los operadores AND / OR y según el rango de años de publicación, lo que permite seleccionar artículos según criterios de inclusión y exclusión mas relevantes.
- ✓ Este Trabajo de Titulación se lo realizó luego de haber cumplido con la etapa de actualización de conocimiento bajo la modalidad Unidad de Titulación resultando como trabajo complementario del mismo, además este trabajo de titulación servirá como guía para estudiantes que quieran realizar investigaciones utilizando el método de Revisiones Sistemáticas de Bárbara Kitchenham
- ✓ De acuerdo con la parte técnica, todos los sistemas de tecnología biométrica operan utilizando un procedimiento de cuatro fases: captura (se recoge una muestra física o de comportamiento durante el proceso de registro, inscripción, identificación o verificación), extracción (se extraen datos únicos de la muestra y se crea una plantilla), comparación (la plantilla se compara con la nueva muestra obtenida), match/non match (el sistema decide si las características extraídas de la nueva muestra coinciden o no), en base esto existen técnicas de ataques directos e indirectos, en donde los ataque directos son los más comunes ya que no necesita el atacante saber mayor información de los diferentes niveles de conocimiento del sistema biométrico, es así que para las huellas dactilares, el método de falsificación más común consiste en el uso de réplicas artificiales creadas de manera cooperativa, donde un molde de la huella digital se adquiere con la cooperación de un usuario válido y se utiliza para replicar la huella digital del usuario con diferentes materiales, Gelatina, látex, play-doh o silicona, y los ataques indirectos en los que el impostor tiene algún conocimiento sobre el funcionamiento

interno del sistema (por ejemplo, la forma en que se almacenan los datos), es aquí donde aplican software de ataque que consisten en algoritmos como Hill-Climbing y Side-Channel.

- ✓ El algoritmo de ataque hill-climbing aplicado a sistemas de reconocimiento biométrico consiste en la sucesiva modificación de un patrón de características obtenido sintéticamente hasta conseguir que el sistema acepte dicho patrón. Por otro lado un ataque side-channel se produce cuando un atacante es capaz de utilizar información adicional obtenida de la implementación física de un sistema criptográfico[25]. Si la información side-channel es suficiente, permitirá romper un sistema cifrado. No se trata de ataques por fuerza bruta que aprovechan la existencia de una tasa de falsa aceptación, sino que utilizan información de la implementación del sistema como puede ser el tiempo (timing-attacks)[28], el consumo de energía (powerattacks), las pérdidas electromagnéticas o el ruido del sistema. Existen varios tipos de ataques side-channel, dentro de los cuales, aquellos basados en la información temporal han demostrado tener una gran eficiencia. Estos ataques denominados timing-attacks se han convertido en una amenaza real a tener en cuenta a la hora de implementar sistemas de seguridad, por lo que profundizaremos a continuación en su funcionamiento.

i. Recomendaciones

- ✓ Se recomienda el uso de la herramienta de software Mendeley, ya que es un gestor de citas bibliográficas el cual permite que el usuario pueda administrar los documentos, agregar notas y resaltar o subrayar textos directamente en los documentos, ayudando así a mantener de manera organizada y ordenada los artículos y trabajos para su revisión y citarlos en las herramientas de texto que se use.
- ✓ Se recomienda el uso de la metodología de Barbara Kinchenman para la realización de Revisiones Sistemáticas, ya que este permite realizar un análisis de información exhaustivo en base a parámetros que posee este protocolo y así responder a las preguntas de investigación que son la base para realizar la misma.
- ✓ Estructurar bien las cadenas de búsqueda, concatenando las palabras claves con los operadores lógicos AND y OR en base a las preguntas de investigación ya que de ello depende la obtención de estudios primarios relevantes y de calidad.
- ✓ Se recomienda el uso de la opción búsqueda avanzada dentro de las bases de datos científicas para optimizar la calidad de artículos o trabajos que se desee encontrar.
- ✓ Se recomienda antes de adquirir un Sistema biométrico analizar su aplicación a través de las características que posee cada uno, ya que según el estudio realizado el sistema biométrico basado en Huella dactilar por ser uno de los más usados y económicos se ha convertido en uno de los más vulnerables a falsificar los patrones de la base de datos ya sea mediante hardware o software.

j. Bibliografía

- [1] Ferrer G. y Maya A., "Sistema biometrico de huella dactilar 1," pp. 1–39, 2013.
- [2] B. Kitchenham and C. Ebse, "Guidelines for performing Systematic Literature Reviews in Software Engineering Executive summary," 2007.
- [3] B. Kitchenham, "Procedures for Performing Systematic Reviews."
- [4] M. L. Pró, M. Juan, C. Gonzáles, L. W. Contreras, and L. C. Yañez, "Tecnologías Biométricas aplicadas a la seguridad en las organizaciones," *Fac. Ing. Sist. e Informática Univ. Nac. Mayor San Marcos*, pp. 55–66, 2009.
- [5] S. Perez, "Tecnologías biométricas aplicadas a la ciberseguridad," *10 incibe*, vol. 1, 2016.
- [6] M. M. Aguilera, "Reconocimiento biométrico basado en imágenes de huellas palmares," Universidad Autonoma de Madrid, 2012.
- [7] P. Perez, "Estudio sobre las tecnologías biométricas aplicadas a la seguridad," *Inst. Nac. Tecnol. La Comun.*, p. 100, 2011.
- [8] V. G. Arrieta, A., Marín, J., Sánchez, L. G., Romero, L., Sánchez, L. A., & Batista, "Gestion y Reconocimiento óptico de los puntos carateristicos de imagenes de huellas dactilares.," *Universidad de Salamanca*, España.
- [9] A. H. B. Muñoz, "ATAQUES TIPO 'SIDE-CHANNEL' A SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO DE HUELLA DACTILAR," *Univ. Autónoma Madrid Esc. politécnica Super.*, 2010.
- [10] R. Cruz, "Clasificación de huellas digitales mediante minucias," 2009.
- [11] R. Hernández, "Estudio de técnicas de reconocimiento facial," 2010, p. 86.
- [12] A. Mendoza Arteaga, G. Mendoza Cedeño, E. Macías Arias, and S. Chun Molina, "Sistemas de reconocimiento facial, como herramienta para la búsqueda de personas Sistema," *Sinapsis La Rev. científica del ITSUP*, vol. 8, no. 1390–7832, pp. 2–5, 2016.
- [13] M. Gómez-barrero, J. Galbally, P. Tomé, and J. Fiérrez, "Sobre las vulnerabilidades frente a ataques software basados en algoritmos genéticos de sistemas basados en iris," 2012.
- [14] M. Baca, P. Grd, and T. Fotak, "Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics," *New Trends Dev. Biometrics*, pp. 1–24, 2012.
- [15] O. Bouihrouzan, "Seguridad e Inseguridad en los Sistemas Biométricos.," Universidad Politecnica de Madrid, 2016.
- [16] E. T. P. J. B. W. Mark, *Biometrías 2*, 2011th ed. Argentina: Tecnologías de Información, VI Congreso Internacional de Biometría de la República Argentina, 2011.

- [17] A. Khodabakhsh, A. Mohammadi, and C. Demiroglu, "Spoofing voice verification systems with statistical speech synthesis using limited adaptation data," *Comput. Speech Lang.*, vol. 42, no. 112, pp. 20–37, Mar. 2017.
- [18] A. K. Jain, A. Ross, S. Pankanti, and S. Member, "Biometrics: A Tool for Information Security," *IEEE Trans. Inf. FORENSICS Secur. VOL. 1, NO. 2, JUNE 2006 Biometrics*, vol. 1, no. 2, pp. 125–143, 2006.
- [19] S. S. Kulkarni, "A Fingerprint Spoofing Detection System Using LBP," pp. 3413–3417, 2016.
- [20] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, p. 11, 2012.
- [21] A. Alcalde, "Biometría Aplicada a La Seguridad - Sistemas Biometricos," *Ingeniería Informática en la ETSIT, Granada.*, 2016. [Online]. Available: <https://elbauldelprogramador.com/sistemas-biometricos/#vulnerabilidades-de-los-sistemas-biom%C3%A9tricos-de-reconocimiento>.
- [22] M. T. J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-Gonzalez F. Alonso-Fernandez, Javier Ortega-Garcia, "Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks," *Esc. Politec. Super. - Univ. Auton. Madrid*, pp. 130–136, 2006.
- [23] M. F. Zanuy, "Experimentos prácticos sobre la vulnerabilidad de sistemas biométricos," *Esc. Univ. Politécnica Mataró*, pp. 67–72, 2010.
- [24] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition," 2003.
- [25] E. Sava, "Attacks on Implementations of Cryptographic Algorithms: Side-Channel and Fault Attacks *," pp. 7–14, 2013.
- [26] M. M. Díaz, "Vulnerabilidades en sistemas de reconocimiento basados en huella dactilar: ataques hill-climbing," *Univ. AUTÓNOMA MADRID Esc. POLITÉCNICA Super. VU*, 2006.
- [27] U. Uludag and A. K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," *Dep. Comput. Sci. Eng. Michigan*, vol. 5306, pp. 622–633, 2006.
- [28] O. Systems and P. C. Kocher, "Timing Attacks on Implementations of."
- [29] J. M. Rayas, E. F. U., del Real, J. A. M., Dévora, J. G. U., Alvarado, C. V., & Miranda, "Herramienta para la Automatización de la Revisión Sistemática," no. 3, 2013.
- [30] I. Xplorer, "Una Guía Corta para Escribir Revisiones Sistemáticas de Literatura," vol. 81, no. 187, pp. 9–10, 2014.
- [31] S. J. Guirao Goris, "UTILIDAD Y TIPOS DE REVISIÓN BIBLIOGRÁFICA _ Guirao Goris _ ENE, Revista de Enfermería," *Agosto*, 2015. [Online]. Available:

<http://ene-enfermeria.org/ojs/index.php/ENE/article/view/495/guirao>.

- [32] M. Coughlan and P. Cronin, *Doing a literature review in nursing, health and social care*. Sage, 2016.
- [33] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies.," *Health Info. Libr. J.*, vol. 26, no. 2, pp. 91–108, Jun. 2009.
- [34] S. J. Guirao Goris, "Utilidad y tipos de revisión de literatura," *ENE, Rev. Enferm.*, vol. 9, no. 2, pp. 1–7, 2015.
- [35] P. Cronin, F. Ryan, and M. Coughlan, "Undertaking a literature review: a step-by-step approach.," *Br. J. Nurs.*, vol. 17, no. 1, pp. 38–43.
- [36] R. Whitemore, A. Chao, M. Jang, K. E. Minges, and C. Park, "Methods for knowledge synthesis: an overview.," *Heart Lung*, vol. 43, no. 5, pp. 453–61.
- [37] R. Whitemore, A. Chao, M. Jang, K. E. Minges, and C. Park, "Methods for knowledge synthesis: An overview," *Hear. Lung J. Acute Crit. Care*, vol. 43, no. 5, pp. 453–461, Sep. 2014.
- [38] D. Maltoni, "A Tutorial on Fingerprint Recognition," *Univ. Bol.*, pp. 43–68, 2006.
- [39] D. S. Zorita, "Reconocimiento automático mediante patrones biométricos de huella dactilar," *Dep. Señales, Sist. y Radiocomun. Esc. Técnica Super. Ing. Telecomunicación Univ.*, 2003.
- [40] E. Politecnica and C. De Cantoblanco, "Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card," *Esc. Politec. Super. - Univ. Auton. Madrid*, pp. 151–159, 2006.
- [41] Y. Vasquez, M. Gómez, M. Flórez, and C. Beltrán, "La biometría dactilar vs la suplantación humana," *Univ. Investig. y Desarro. -UDI Resum.*, 2015.

k. Anexos

Anexo 1. Artículos Revisados

Tabla 24. Artículos Revisados.

N°	Artículo	Autores	Año de publicación	Lugar de publicación
1	Sistema de detección de huella digital	Eduardo, Luis López, Morán Covarrubias, M C Gerardo Fuentes	2002	Universidad de Colima Maestria
2	Reconocimiento automático mediante patrones biométricos de huella dactilar.	D. S. Zorita	2003	<i>Dep. Señales, Sist. y Radiocomun. Esc. Técnica Super. Ing. Telecomunicación Univ.</i>
3	Attacks on Biometric Systems : A Case Study in Fingerprints”	U. Uludag and A. K. Jain	2004	IEEE, Department of Computer Science and Engineering, Michigan State University
4	Biometrics : A Tool for Information Security	Jain, Anil K Ross, Arun Pankanti, Sharath Member, Senior	2006	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
5	Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks J.	J. Galbally- Herrero, J. Fierrez-Aguilar, J. D. Rodriguez- Gonzalez F. Alonso-	2006	Biometrics Research Lab.- ATVS, Escuela Politecnica Superior - Universidad Autonoma de Madrid

		Fernandez, Javier Ortega-Garcia, M. Tapiador		
6	Attacks on Biometric Systems : A Case Study in Fingerprints	Uludag, Umut Jain, Anil K	2006	Department of Computer Science and Engineering, Michigan
7	Biometrics : A Tool for Information Security	Jain, Anil K Ross, Arun Pankanti, Sharath Member, Senior	2006	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
8	Vulnerabilidades en sistemas de reconocimiento basados en huella dactilar: ataques hill-climbing	M. M. Díaz	2006	UNIVERSIDAD AUTÓNOMA DE MADRID
9	A Tutorial on Fingerprint Recognition	Davide Maltoni	2006	Biometric Systems Laboratory - DEIS - University of Bologna via
10	Gestion y Reconocimiento óptico de los puntos característicos de imágenes de huellas dactilares.	Arrieta, A., Marín, J., Sánchez, L. G., Romero, L., Sánchez, L. A., & Batista	2006	Universidad de Salamanca
11	Seguridad en los Sistemas biométricos	Albert Solé Ribalta	2007	Universidad abierta de Cataluña
12	Reconocimiento biométrico en aplicaciones de E-Government . Análisis de confiabilidad /	Carri, José I Pasini, Ariel Pesado,	2007	XIII Congreso Argentino de Ciencias de la Computación

	tiempo de respuesta	Patricia Giusti, Armando De Giusti		
13	Fingerprint Readers : Vulnerabilities to Front- and Back- end Attacks	Palka, Sean Hamilton, Booz Allen Wechsler, Harry	2007	George Mason University
14	Sistemas biométricos multimodales que emplean rasgos audio-visuales	MSc. Susana C. Romaniz Grupo	2008	XIV Congreso Argentino de Ciencias de la Computación
15	Reconocimiento de Huellas Dactilares Usando Características Locales	Gualberto Aguilar, Gabriel Sánchez, Karina Toscano, Mariko Nakano, Héctor Pérez	2008	Revista Facultad de Ingenieria, Universidad de Antioquia
16	Análisis Temporal de Vulnerabilidades de los Sistemas Basados en Huella Dactilar	Galbally, Javier Fierrez, Julian Ortega-garcia, Javier	2008	Biometric Recognition Group ATVS, EPS, Universidad Autónoma de Madrid
17	Tecnologías Biométricas aplicadas a la seguridad en las organizaciones	Mg. Luzmila Pró Mg. Juan Carlos Gonzáles Lic. Walter Contreras Lic. Carlos Yañez	2009	Revista de ingeniería de sistemas e informática

18	Experimentos prácticos sobre la vulnerabilidad de sistemas biométricos	Zanuy, Marcos Faúndez	2010	Escola Universitària Politécnica de Mataró
19	ATAQUES TIPO "SIDE-CHANNEL" A SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO DE HUELLA DACTILAR	Muñoz, Alicia Hortensia Beisner	2010	Universidad Autónoma de Madrid Escuela politécnica superior
20	Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales	Etchart, Graciela Luna, Lucas Leal, Carlos Benedetto, Marcelo Gabriel Alvez, Carlos	2011	XIII Workshop de Investigadores en Ciencias de la Computación
21	Estudio sobre las tecnologías biométricas aplicadas a la seguridad	Pablo Pérez San-José (director)	2011	Instituto Nacional De Tecnologías De La Comunicación
22	Vulnerabilities of fingerprint reader to fake fingerprints attacks	Espinoza, Marcela Champod, Christophe Margot, Pierre	2011	Forensic Science International
23	Reconocimiento biométrico de iris en ambientes de alta seguridad	Devincenzi, Juan Alberto Finamore, María Laura Chichizola, Franco	2012	XVIII Congreso Argentino de Ciencias de la Computación

		De, Laura Naouf, Marcelo		
24	On the Vulnerability of an EEG-based Biometric System to Hill-climbing Attacks Algorithms' Comparison and Possible Countermeasures	Maiorana, Emanuele Hine, Gabriel Emile Rocca, Daria La Campisi, Patrizio Volterra, Via Vito	2013	Section of Applied Electronics, Department of Engineering, University of Roma
25	Analysis of textural features for face biometric anti-spoofing	Waris, Muhammad Adeel Zhang, Honglei Ahmad, Iftikhar Kiranyaz, Serkan Gabbouj, Moncef	2013	European Signal Processing Conference
26	Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida	Adriana Maya Vargas Dr. Gabriel Ferrer	2013	Universidad Militar Nueva Granada Facultad, Bogotá
27	Using a Biometric System to Control Access and Exit of Vehicles at Shopping Malls in South Africa	Hans, Robert T.	2014	International Conference on Computer, Communications, and Control Technology (I4CT)
28	Hill-Climbing Attacks on Multi-Biometrics Recognition Systems	Maiorana, Emanuele Hine, Gabriel Emile Campisi,	2014	EEE TRANSACTIONS ON INFORMATION FORENSICS AND

		Patrizio Member, Senior		SECURITY
29	Biometric antispoofing methods: A survey in face recognition	Galbally, Javier Marcel, Sébastien Fierrez, Julian	2014	IEEE Access
30	Cifrado caótico de plantilla de huella dactilar en sistemas biométricos	Murillo-Escobar M.A. Cruz-Hernández C. Abundiz-Pérez F. López-Gutiérrez R.M.	2014	Memorias del XVI Congreso Latinoamericano de Control Automático, CLCA 2014 Cancún, Quintana Roo, México Cifrado
31	Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions	Hadid, Abdenour	2014	IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops
32	La biometría dactilar vs la suplantación humana	Y. Vasquez, M. Gómez, M. Flórez, C. Beltrán	2015	Universitaria de Investigación y Desarrollo -UDI Resúmen
33	Deep Representations for Iris, Face, and Fingerprint Spoofing Detection	Menotti, David Chiachia, Giovanni Pinto, Allan Schwartz, William Robson Pedrini, Helio	2015	IEEE Transactions on Information Forensics and Security

		Falcão, Alexandre Xavier Rocha, Anderson		
34	BIOMETRÍA	Ing. MSc. Gerson Enrique Delgado Parra	2015	Instituto Universitario Politécnico Santiago Mariño & Instituto Universitario de Tecnología Agro Industrial
35	A Minutiae Count Based Method for Fake Fingerprint Detection	Abhishek, Kumar Yogi, Ashok	2015	Procedia - Procedia Computer Science
36	Security of Biometric Systems	Adámek, Milan Matýsek, Miroslav Neumann, Petr	2015	Procedia Engineering
37	Face Anti-Spoofing Based on Radon Transform	Razvan D. Albu	2015	IEE. International Conference on Engineering of Modern Electric Systems (EMES)
38	Tecnologías biométricas aplicadas a la ciberseguridad	S. Perez	2016	10 incibe
39	A Fingerprint Spoofing Detection System Using LBP	Samruddhi S. Kulkarni Dr. Hemprasad Y. Patil	2016	International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)
40	Two strategies to optimize the decisions in signature	Yu, Shilian Ai, Ye Poh, Norman Xu, Bo	2016	Information Sciences journal www.elsevier.com/locate

	verification with the presence of spoofing attacks	Zhou, Yicong Li, Weifeng		e/ins
41	Spoofing voice verification systems with statistical speech synthesis using limited adaptation data	Khodabakhsh, Ali Mohammadi, Amir Demiroglu, Cenk	2017	Computer Speech & Language
42	Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems	Roy, Aditi Member, Student Memon, Nasir Ross, Arun Member, Senior	2017	IEEE Transactions on Information Forensics and Security

