ISSN impreso 1996-6660 / ISSN online 2519-5719
DOI: https://doi.org/10.31381/perfiles_ingenieria.v18i18.5398

Beneficios de sistemas biométricos basados en lectura de Iris

Benefits of biometric systems based on Iris reading

Alvaro Aníbal Visitación Moreno[1], Fabio Leonell Mogollón Reyes[2] y Alberto Mendoza de los Santos[3]

RECIBIDO: 29 de junio del 2022
ACEPTADO: 30 de setiembre del 2022

RESUMEN

El presente trabajo tiene como objetivo encontrar beneficios del uso de imágenes del iris ocular en el campo de la biometría, para lo cual se desarrolló una revisión sistemática den la que se utilizaron las siguientes bases de datos: Sciencedirect Library, IEEExplore Library, Dialnet, Scielo y Alicia. Mediante la metodología del protocolo de Bárbara Kitchenham, se seleccionaro 13 documentos que arrojaron como principales beneficios el algoritmo por NIST, que ofrece extrema precisión e incrementa la seguridad a un nivel alto.

El protocolo de autenticación SEMBA es muy seguro contra terceros maliciosos, y la transformación circular de High protege la identidad y falsificación.

En tal sentido, se concluye que los sistemas de biometría basados en el iris son de mucha utilidad para los usuarios que lo deseen usar, siempre y cuando se sigan una serie de precauciones y no se dañen los derechos éticos de las personas que usen esta tecnología.

Palabras clave: biometría de iris, técnicas biométricas, reconocimiento del iris, sistemas biométricos, patrones de reconocimiento de imagen.

ABSTRACT

The objective of this work is to find benefits and/or techniques using the treatment of images of the ocular iris in the field of biometrics, for which a Systematic Review was developed using the following databases: SCIENCEDIRECT Library, IEEEXPLORE LIBRARY , DIALNET, SCIELO and ALICIA, following the methodology of the Barbara Kitchenham protocol, where 13 documents were selected that yielded the main benefits: The NIST algorithm offers extreme precision and increases security to a high level, the SEMBA authentication protocol is very Secure against malicious third parties, High's circular transformation protects identity and counterfeiting.
And in this sense, it is concluded that iris-based biometric systems are very useful for users who wish to use it, as long as a series of precautions are followed and the ethical rights of people who use this technology are not damaged. Of great usefulness

Keywords: iris biometrics, biometric techniques, iris recognition, biometric systems, image recognition patterns

1 Universidad Nacional de Trujillo, Facultad de Ingeniería, <avisitacion@unitru.edu.pe>
2 Universidad Nacional de Trujillo, Facultad de Ingeniería, <fmogollon@unitru.edu.pe>
3 Universidad Nacional de Trujillo, Facultad de Ingeniería, <amendndozad@unitru.edu.pe>

INTRODUCCIÓN

Probar la identidad de una persona, si esta es cuestionada, se denomina autenticación [1]. Por este motivo, los sistemas biométricos tienen la capacidad de gestionar de manera correcta los pilares de la seguridad informática, la cual dispone de tres principios fundamentales como son la disponibilidad de información, la integridad y la confidencialidad. Actualmente, estos sistemas biométricos del iris dan la posibilidad a las empresas de que el proceso de identificación sea no solo más rápido, sino eficiente y confiable debido a que el intercambio de información es de manera inmediata, lo que evita la duplicidad de data y consumo de tiempo innecesario. Todo lo mencionado garantiza a la organización y a los usuarios de la misma una competitividad y productividad de mayor nivel; debido a que los procesos e individuos son tratados con mayor rapidez por el sistema de información de manera segura. El objetivo de nuestro estudio es encontrar los beneficios y/o técnicas del uso de imágenes del iris ocular en el campo de la biometría. Estos sistemas biométricos son muy beneficiosos para la autenticación en cajeros automáticos, antiterrorismo, controles fronterizos nacionales, inicio de sesión informático, en aplicaciones gubernamentales y civiles con la finalidad de agilizar los servicios y garantizar un nivel alto de seguridad a los trámites.

Para elegir la mejor opción aplicable a la autenticación por Biometría se tuvo como condición principal la seguridad y comparación del resto de técnicas la lectura de iris como muestra la Figura 1, además de la revisión de textos informativos sobre biometría que estaban incluidos en nuestro sílabo del curso Seguridad de la Información, correspondiente a las sesiones 7; Técnicas de control de accesos, 8; y Métodos de Autenticación, 11.

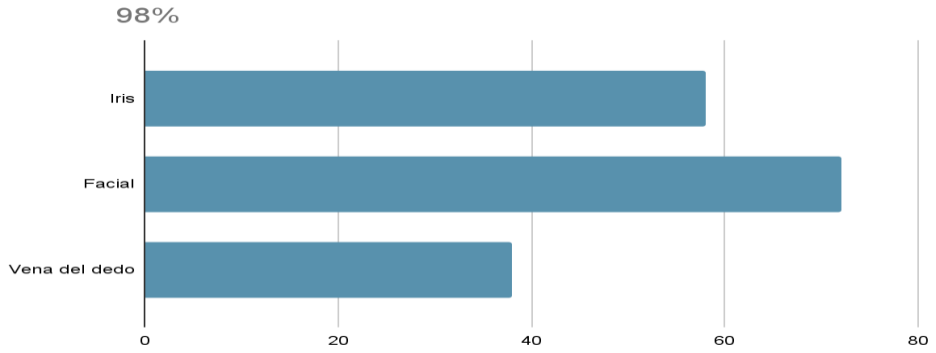

Figura 1. *Precisión de los tipos de biometría.Elaboración propia.*
Nota. Los datos empleados pertenecen a la investigación [2].

De lo anteriormente expuesto surge la siguiente interrogante: ¿de qué manera el uso de los sistemas de biometría basados en el iris ocular humano permite brindar ventajas a un usuario? A partir de esta, se plantearon otras preguntas más específicas como ¿cuáles son los beneficios del reconocimiento de iris en los sistemas biométricos?, y ¿qué técnicas son utilizadas para la identificación de iris en los sistemas biométricos?

I. METODOLOGÍA

El protocolo que se usa en esta revisión sistemática es postulado por Bárbara Kitchenham y está formado por 3 etapas, cada una de las cuales tiene sus respectivas ocupaciones: Planificación de la revisión, Ejecución de la revisión y Publicación de la Revisión.

1.1. Identificación de la investigación

Con el fin de obtener artículos de calidad que permitan dar respuesta a nuestras preguntas de investigación, se realizó una serie de búsquedas en las siguientes bases de datos detalladas a continuación en la Tabla 1.

Tabla 1. *Bases de datos científicas*

Bases de datos	URL
IEEEXPLORE LIBRARY	http://ieeexplore.ieee.org/
DIALNET	https://dialnet.unirioja.es/
SCIELO	https://www.scielo.org/
ALICIA	https://alicia.concytec.gob.pe/

Elaboración propia

Se tomó en consideración utilizar los datos de la tabla 2, junto a las consultas apropiadas, y se fijó la atención en dos factores, que son las preguntas de investigación y las palabras claves de artículos científicos alusivos al tema de investigación precedente en español y en inglés para mayor rango de búsqueda.

Iris biometrics security, iris biometrics, biometrics security, técnicas biométricas, reconocimiento del iris, sistemas biométricos

A continuación, a partir de la delimitación de las bases de datos y la distinción de las palabras claves, se procedió a utilizar los operadores lógicos AND y OR, lo que dio origen a las cadenas de búsqueda (CB) (figura 2). Concretamente se consideró como estudio a los artículos de conferencias, tesis, trabajos de universidades y artículos de revistas; también se utilizaron artículos que contenían las palabras claves en el abstract o resumen.

1.2. Revisión preliminar de términos

Bases de datos	Identificación	Cadena de Búsqueda
IEEE	CB1	Iris biometrics
IEEE	CB2	Biometrics AND security
IEEE	CB3	Iris biometrics AND security
DIALNET	CB4	Técnicas biométricas
DIALNET	CB5	Reconocimiento del iris
SCIELO	CB6	Sistemas biométrico
ALICIA	CB7	Reconocimiento del iris

Figura 2. *Revisión preliminar y términos. Elaboración propia*

1.3. Selección de estudios primarios

Una vez ejecutadas las CB y obtenidos los primeros estudios se pasa a determinar los criterios que serán útiles en la selección de investigaciones primarias.

A) Criterios de inclusión

- Artículos de Investigación publicados a desde el año 2015, a pesar de la escasa información que se ha encontrado, se trata de un año no tan lejano a las nuevas actualizaciones de la tecnología que avanzan a pasos agigantados.
- Investigaciones que contengan en su resumen o en las conclusiones las palabras clave utilizadas.
- Artículos que se obtengan de la exploración en el campo de la ciencia, seguridad y tecnología.

B) Criterios de exclusión

- Investigaciones que están inadecuadamente estructuradas por una metodología científica.
- No cumplen con los requisitos antes mencionados en criterios de inclusión.

1.4. Resumen de los resultados de las búsquedas

Después de haber realizado la búsqueda de artículos, el resumen se presenta a continuación, en la tabla 2.

Tabla 2. *Resultados de la etapa de selección de artículos incluidos y excluidos.*

Base de Datos	Cadena de búsqueda	Total de estudios	Estudios incluidos	Estudios excluidos
IEEE	CB1	227	85	142
	CB2	193	58	135
	CB3	144	45	99
DIALNET	CB4	184	12	172
	CB5	132	10	122
SCIELO	CB6	17	5	10
ALICIA	CB7	15	3	12

Elaboración propia

1.5. Extracción de datos y seguimiento

Por cada investigación seleccionada, se buscó encontrar al menos uno de los siguientes criterios:

- Beneficios de la identificación biométrica de iris, basado en la PI01.
- Las técnicas más eficientes para la identificación de biometría de iris, basado en la PI02.
- Conclusiones relevantes

1.6. Síntesis de datos

N°	DOCUMENTO	AUTOR(ES)	AÑO	LUGAR DE PUBLICACIÓN
D01	Advanced ATM System Using Iris Scanner	Indranil banerjee, Sjivangam Mookherjee, et al. [1]	2019	Kolkata, India
D02	SEMBA: secure multi-biometric authentication	Mauro Barni, Giulia Droandi, et. al. [2]	2018	Italia
D03	Human biometrics detection and recognition system using SVM and genetic algorithm iris as an example	Anfal Waled y Sefer Kurnaz [3]	2021	Estambul, Turquía
D04	Propuesta de mejora de un sistema biométrico multiusuario para cajeros automáticos en instituciones bancarias en la ciudad de Lima	MarÍn Moya Jonathan [4]	2017	Lima, Perú
D05	Evaluación del impacto del preprocesamiento de imágenes en la segmentación del iris	Valencia Murillo, José; Poveda Sendales, Daniel, Valencia Vargas, Daniel [5]	2019	La Rioja, España
D06	Design and Implementation of a Student Attendance System Using Iris Biometric Recognition	Olatunji J. Okesola, Okonigene Robert, et al [6]	2017	Ogun State, Nigeria
D07	Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology	Raj Gusain, Hemant Jain y Shivedra Pratap [7]	2018	Dehradun, India
D08	Iris as Biometrics for Security System	Bhakti B. Bhaganagare y Avinash D. Harale [8]	2017	Maharashtra, India
D09	Deep Learning Approach for Multi-modal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits.	Silva, P., Luz, E., Zanlorensi, L., Menotti, D. and Moreira, G. [9]	2018	Arabia Saudita
D10	Iris based cancelable biometric cryptosystem for secure healthcare smart card	Firdous Kausar [10]	2021	Muscat, Omán
D11	Enhanced Biometric Recognition for secure Authentication Using Iris Preprocessing and Hyperelliptic Curve Cryptography	vani Rajasekar, J. Premalatha, and K. Sathya [11]	2020	India
D12	Multimodal Biometrics Authentication System Fingerprint and Iris	Miss. Kamble Sunayana Nivrutti, Prof. Gund. V. D., Prof. Kazi K [12]	2018	Solapur, Maharashtra, India
D13	Advanced IRIS Recognition System: A Review	Saumitra Vatsal, Mr. Shyam Shankar Dwivedi [13]	2018	Lucknow, India.

Figura 3. *Resultados de la etapa de elección de artículos incluidos y excluidos*
Elaboración propia

II. RESULTADOS

2.1. Extracción de datos

Aplicando los criterios de selección se obtuvieron 13 documentos de investigación, de los que se extrajo la información necesaria referente a las preguntas de investigación.

2.1.1. Sistema de cajero automático avanzado con escáner de iris

- La ventaja que ofrece nuestro sistema es el uso de biometría bajo la norma ISO/IEC 1794-6. Está respaldado por NIST lo que garantiza un algoritmo extremadamente preciso que está certificado por STQC.
- El uso del escáner de iris como principal control de validación de identidad hace que el sistema se asegure automáticamente.
- El uso de un lector de huellas dactilares ligado a una tarjeta RFID y a la par de un escáner de iris, incrementa el nivel de seguridad del sistema un nivel más alto.
- En caso se extravíe la tarjeta no hay riesgo de fraude sin la lectura de huella dactilar e iris, por lo que

ninguna transacción sería posible.

2.1.2. SEMBA: secure multi-biometric authentication

- ➢ SEMBA es un protocolo de autenticación multimodal basado en SPDZ, protocolo de cálculo seguro de dos o más partes en contra de un activo adversario que corrompe hasta n-1 de n jugadores.
- ➢ El uso de este sistema multimodal aumenta el proceso en términos de multiplicaciones y tiempo de evaluación (Luo et al. 573 ms, SEMBA 30ms, experimento, y 120ms, online), la precisión a un costo insignificante de incremento de complejidad y es seguro contra terceros maliciosos, lo que proporciona un nivel de seguridad alto.

2.1.3. Detección de biometría humana y sistema de reconocimiento utilizando SVM y el iris del algoritmo genético como ejemplo

- ➢ Proponen métodos alternativos para realizar un sistema cooperativo de reconocimiento de iris.
- ➢ Para la segmentación de iris utilizan el popular método “Girl 's eye”, lo que constituye una clara referencia al método desarrollado por Richard P. Wildes.
- ➢ En la etapa de extracción de propiedades del iris se utiliza a la familia de onditas Daubechies.
- ➢ El proceso de clasificación, el procesamiento digital de la sub-imagen de iris, aplica la Máquina de Vectores de Soporte (SVM) y produce resultados más precisos en el análisis de la realidad del espacio geográfico (SVM - 90%, CNN - 85%).

2.1.4. Propuesta de mejora de un sistema biométrico multiusuario para cajeros automáticos en instituciones bancarias en la ciudad de Lima

- ➢ Se hizo un análisis de comparación para elegir la mejor opción entre las técnicas de reconocimiento, utilizados en los cajeros automáticos de los bancos y resultó que la lectura de iris es la más segura, aunque puede llegar a ser algo molesto para los usuarios.
- ➢ Y a diferencia de las tarjetas de crédito, se tendrá los siguientes beneficios:

  - Mínima posibilidad de robo
  - Mínima posibilidad de pérdida
  - No hay costo de mantenimiento
  - No hay vulnerabilidad ante el espionaje
  - Mínima vulnerabilidad por fuerza bruta
  - Se pueden autenticar usuarios reales

2.1.5. Evaluación del impacto del preprocesamiento de imágenes en la segmentación del iris

- ➢ Los resultados demuestran que el algoritmo Filtro Gaussiano, que permite visualizar las regiones más suaves en los sitios donde los valores intensos son homogéneos sin diluir los bordes de la imagen, generó uno de los incrementos más grandes de los porcentajes de segmentación y resultó exitosa para determinar los márgenes exteriores del iris y los márgenes exteriores de la pupila. Se hizo uso de la transformada circular de Hough, pasa de 59% (algoritmo de segmentación tradicional introducida por Masek) a 73%, y se aplicó un filtro Gaussiano con máscara 5x5 , además de usar la base de datos CASIA.
- ➢ Estos resultados permiten enfatizar en el valor de una fase previa en el pre procesamiento de una imagen para garantizar una mejor efectividad en la segmentación.

2.1.6. Diseño e implementación de un sistema de asistencia estudiantil mediante reconocimiento biométrico de iris

- ➢ El uso de iris como control biométrico en la toma de asistencia elimina los problemas de suplantación de identidad y falsificación.
- ➢ En las pruebas realizadas se aplicó una mejorada técnica de segmentación de iris mediante el uso de la transformación circular de Hough, y se obtuvieron los siguientes resultados:

- La FMR (Tasa de Coincidencia Falsa) obtenido fue de 0%
- La FPIR (Tasa de Identificación Positiva Falsa) es igual a 0
- La FNIR (Tasa Negativa de Identificación Falsa) es de 0

2.1.7. Mejora del sistema de seguridad bancaria usando reconocimiento facial, escáner de iris y tecnología Palm Vein

- ➢ La tecnología de reconocimiento de la vena de la palma (PVR) garantiza un alto nivel de seguridad debido a la precisión de la confiable técnica, Zhang-Suen thinning technique, que es considerada como la más segura en cuestiones de seguridad.
- ➢ El algoritmo "Hamming Distance" de Daugman ofrece un reconocimiento eficiente, mediante la transformada de fourier, de la biometría facial, incluye iris.

2.1.8. Iris como sistema biométrico para seguridad

- ➢ El sistema propuesto garantiza un nivel de seguridad alto mediante el reconocimiento libre de errores para el ingreso de personal en áreas restringidas, a través del reconocimiento biométrico de iris.
- ➢ Para garantizar el correcto reconocimiento biométrico de iris utilizaron la hoja modelo de Daugman's rubber, Hamming distance y hardware como RS 232(comunicador en serie), microcontrolador, fuente de poder, laptop y una pantalla LCD.

2.1.9. Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits

- ➢ El sistema propuesto utiliza un modelo biométrico multimodal para la identificación de usuario, y logra una precisión de 99,39% según se demostró en los experimentos realizados.
- ➢ Mediante el uso de la biometría multimodal, es decir, de tres CNNs, reconocimiento de iris, facial y vena de los dedos, se logró el porcentaje mencionado en el punto anterior; mientras que el uso de la biometría unimodal de iris logró una precisión de 98.58%.

2.1.10. Iris based cancelable biometric cryptosystem for secure healthcare smart card

- ➢ El sistema que proponen es seguro y la autenticación biométrica criptosistema cancelable basado en el iris proporciona autenticación y cifrado seguro datos de médicos del usuario.
- ➢ Los resultados del experimento demostraron que se obtuvo una llave (key) de 256 bits con una FAR (Tasa de Aceptación Falsa) de 0%, FRR (Tasa de Falso Rechazo) de 7%.
- ➢ El análisis de seguridad indicó que un atacante es incapaz de obtener la llave, mediante ataque de coincidencia cruzada, desde la data almacenada en la tarjeta médica inteligente porque el biométrico cancelable está integrado a un criptosistema biométrico.

2.1.11. Enhanced Biometric Recognition for Secure Authentication Using Iris Preprocessing and Hyperelliptic Curve Cryptography

- ➢ Proponen dos enfoques novedosos como el 2D Gabor kernel para extracción de características y el enfoque HECC para encriptar la plantilla original de iris a plantillas cifradas. Esto con el fin de evitar que un atacante comprometa la base de datos de plantillas.
- ➢ Los resultados que se obtuvieron fueron de una TAR (Tasa de Aceptación Verdadera) de 100%, ERR (Tasa de Error Igual) de 2.5% y una precisión mejorada de 99.74% con un tiempo de reconocimiento de 3 segundos. Debido a su alta precisión y seguridad, el estudio será destinado a aplicaciones militares.

2.1.12. Multimodal Biometrics Authentication System Fingerprint and Iris

- ➢ Para el propósito de la clasificación, el support vector machine (SVM) se utiliza como clasificador principal mientras que la distancia de Hamming es utilizado como clasificador secundario; de su combinación, se logra una precisión del 99,88% en CASIA (base de datos de imágenes de iris).

2.1.13. Advanced IRIS Recognition System: A Review

- ➢ Se escoge el uso de la Retina para el trabajo de reconocimiento debido a que está bien protegido por la córnea, tiene una estructura casi plana y su dilatación y construcción tienen lugar en virtud de dos músculos, dilatador pupillae y pupillae constrictor, respectivamente, los cuales controlan el diámetro de las pupilas.
- ➢ Se hace énfasis en el reconocimiento de iris para la autenticación en cajeros automáticos, antiterrorismo, controles fronterizos nacionales, inicio de sesión informático.
- ➢ Como técnica de coincidencia, todos los pasos de procesamiento de imágenes son incorporados en el momento de la inscripción de las plantillas de iris codificadas en la base de datos que son del sistema. Una vez que se extrae el patrón de bits cifrado que corresponden a la imagen binaria formada, se compara con todos patrones de bits encriptados y almacenados mediante el XOR booleano y la medida de disimilitud entre dos bits de iris. Los patrones se calculan mediante el uso de HD (distancia de Hamming) representado en:

$$HD = \frac{1}{N}\sum_{j=1}^{N} X_j(XOR)Y_j$$

donde N denota el número total de bits para cada patrón de iris.

2.2. Síntesis de datos

En la tabla 3 se describe en forma resumida el proceso de selección de estudios correspondientes a su respectiva etapa.

Tabla 3. *Resultados de selección de estudios primarios*

Base de Datos	Encontrados	Coincidencias	Seleccionados
IEEE	564	192	6
DIALNET	316	22	2
SCIELO	17	5	2
ALICIA	15	3	3
TOTAL	912	223	13

Elaboración propia

Luego de extraer la información de cada estudio seleccionado se puede observar en la figura 4 que, a partir del problema abordado, una gran cantidad de documentos mencionan las ventajas de los sistemas biométricos basados en lectura de Iris. Del mismo modo, se puede encontrar el uso de técnicas como algoritmos para mejorar el uso de estos sistemas.

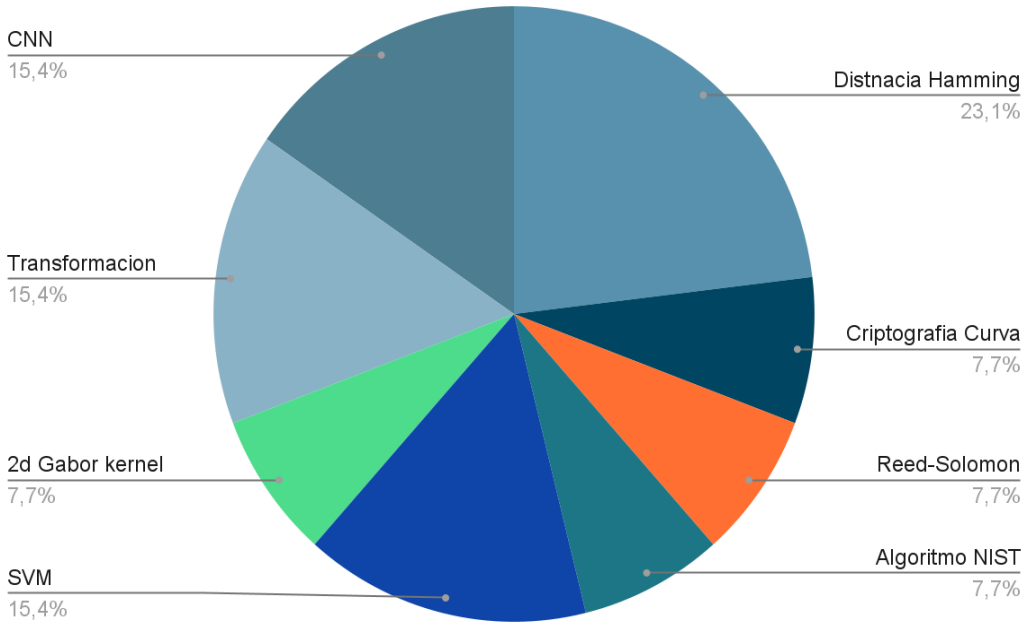

Figura 4. *Resultados de selección de estudios primarios*

Elaboración propia

III. DISCUSIÓN Y CONCLUSIONES

4.1. Discusión

- Los trabajos [3] **y** [2] coinciden en usar la base de datos de patrones de Iris correspondiente a CASIA para las pruebas en sus investigaciones.
- Uno de los pasos importantes para lograr el reconocimiento por iris es la segmentación como en [4] utiliza el popular método “Girl 's eye”, que es una clara referencia al método desarrollado por Richard P. Wildes, en comparación con [3] que utiliza la transformada circular de Hough, que pasa de 59% (algoritmo de segmentación tradicional introducida por Masek) a 73% en éxito de precisión. Por otro lado, en el proyecto [5], se utiliza la transformación circular de Hough y se obtuvo la FMR (Tasa de Coincidencia Falsa) de 0%.

- Se hizo uso de la biometría multimodal para reforzar el reconocimiento del iris, como es el caso del proyecto [6], que señala un aumento en el proceso en términos de multiplicaciones y tiempo de evaluación (573 ms, SEMBA 30ms, experimento, y 120ms, online) y mejora la precisión. También en el artículo [7] se utiliza un modelo biométrico multimodal para la identificación de usuarios y se logró una precisión de 99,39% según se demostró en los experimentos realizados.
- El algoritmo “distancia de Hamming” de Daugman es muy común cuando hablamos de biometría de iris por la precisión que ofrece y por ser el más conocido tal y como demuestran los estudios [8], [9], [4], [6] y [7]. Sin embargo, no es el único camino para lograr un alto nivel de precisión. Esto queda demostrado en [10] con el algoritmo de extrema precisión probado por las NIST, Firdous Kasar y el algoritmo de REED-SOLOMON y Vani Rajasekar et al. con su criptografía de curva hiperelíptica.

4.2. Conclusiones

Se logró identificar el objetivo teniendo como técnicas y beneficios a:

- El algoritmo está respaldado por NIST y certificado por STQC, que ofrece extrema precisión e incrementa la seguridad a un nivel alto.
- El protocolo de autenticación SEMBA, basado en SPDZ, reduce los tiempos de proceso a 120 ms en pruebas de campo reales(online) y además es seguro contra terceros maliciosos y brinda un nivel de seguridad alto.
- La transformación circular de High en la segmentación de iris da como resultado FMR=0%, FPIR=0 Y FNIR=0 y en consecuencia la eliminación de suplantación de identidad y falsificación.
- La hoja modelo de Daugman's rubber, hamming distance para un correcto reconocimiento biométrico libre de errores garantiza un nivel de seguridad alto para el ingreso en áreas restringidas.
- El sistema unimodal biométrico de iris logra una precisión en la autenticación de 95.58. Sin embargo, para circunstancias mucho más exigentes, un modelo biométrico multimodal, es decir biometría de iris, facial y venas de los dedos mediante el uso de CNNs, logra una identificación con precisión de 99.39%.
- La autenticación biométrica de criptosistema mediante el algoritmo de REED-SOLOMON (FAR=0% y FRR=7%) brinda seguridad a los datos médicos del usuario además de proporcionar un escudo contra terceros atacantes.
- El uso de preprocesamiento de iris y criptografía curva hipereliptica ofrece seguridad a los datos del usuario mediante la encriptación de las plantillas con unos resultados de TAR=100%, ERR=2.5% y una precisión de 99.74% con un tiempo de reconocimiento de 3 segundos.
- El uso del algoritmo de Hamming junto con el SVM garantizan un nivel alto de seguridad y brindan una precisión del 99.88%

También se admite que se logró cumplir con los estándares propuestos en el protocolo de Kitchenham como planificación de la revisión, ejecución de la revisión y publicación de resultados, lo cual nos ha generado calidad, consistencia, y transparencia y servido de mucha ayuda en el proceso de la revisión sistemática.

Sin embargo, en esta revisión, se ha mostrado y examinado el presente, de igual forma las tendencias en los avances tecnológicos en el reconocimiento del iris humano, que en la actualidad se van consolidando y participando en los campos de investigación. Además, se evidencia la necesidad de hacer importantes esfuerzos referentes a la indagación e implementación de sistemas para avanzar en el reconocimiento del iris más eficiente.
Por último, se debería tomar en cuenta los aspectos de privacidad y revisar los derechos de protección de datos de las personas para que útil herramienta no perjudique a los usuarios que la utilizan.

REFERENCIAS

[1] IBM, «IBM MQ,» 20 04 2021. [En línea]. Available: https://www.ibm.com/-docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740htm. [Último acceso: 29 11 2022].

[2] M. Nivrutti, P. D y P. S, «Multimodal Biometrics Authentication System using Fusion of Fingerprint and Iris,» International Journal of Trend in Scientific Research and Development, Volume-2(Issue-6), pp.1282-1286, 2018. [En línea]. Available: https://doi.org/10.31142/ijtsrd18861. [Último acceso: 30 Diciembre 2021].

[3] J. F. Valencia-Murillo, D. A. Poveda-Sendales y D. F. Valencia-Vargas, « Evaluación del impacto del preprocesamiento de imágenes en la segmentación del iris,» TecnoLógicas, ISSN 0123-7799, ISSN-e 2256-5337, Vol. 17, No. 33, 2014 (Ejemplar Dedicado a: Julio-Diciembre), Págs. 31-41, 17(33), 31–4, 2019. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=5062924&-info=resumen&idioma=SPA. [Último acceso: 30 Diciembre 2021].

[4] A. Al-zanganawi y S. Kurnaz , « Human Biometrics Detection And Recognition System Using SVM And Genetic Algorithm Iris As An Example,» 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020. [En línea]. Available: https://doi.org/10.1109/-ISMSIT50672.2020.9255095. [Último acceso: 30 Diciembre 2021].

[5] K. Okokpujie, E. Noma-Osaghae, O. Okesola, S. John y O. Robert, « Design and Implementation of a Student Attendance System Using Iris Biometric Recognition,» International Conference on Computational Science and Computational Intelligence (CSCI, 2017. [En línea]. Available: https://doi.org/10.1109/CSCI.2017.96 . [Último acceso: 30 Diciembre 2021].

[6] M. Barni, G. Droandi, . R. Lazzeretti y T. Pignata, «SEMBA: secure multi-biometric authentication.,» IET Biometrics, 8(6), pp.411-421, 2019. [En línea]. Available: https://doi.org/10.1049/iet-bmt.2018.5138. [Último acceso: 30 Diciembre 2021].

[7] P. Silva, E. Luz, L. Zanlorensi, D. Menotti y G. Moreira, «Multimodal Feature Level Fusion based on Particle Swarm Optimization with Deep Transfer Learning,» IEEE Congress on Evolutionary Computation (CEC), 2018. [En línea]. Available: https://doi.org/10.1109/CEC.2018.8477817. [Último acceso: 30 Diciembre 2021].

[8] R. Gusain, H. Jain y S. Pratap, «Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology,» 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018., 2018. [En línea]. Available: https://doi.org/10.1109/IoTSIU.2018.-8519850. [Último acceso: 30 Diciembre 2021].

[9] B. Bhaganagare y A. Harale, « Iris as biometrics for security system,» Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017. [En línea]. Available: https://doi.org/10.1109/-ICECCT.2017.8117952. [Último acceso: 30 Diciembre 2021].

[10] I. Banerje, S. Mookherjee, S. Saha, S. Ganguli, S. Kundu y D. Chakravarti, «Advanced ATM System Using Iris Scanner,» International Conference on Opto-Electronics and Applied Optics (Optronix), 2019. [En línea]. Available: https://doi.org/10.1109/OPTRONIX.2019.8862388. [Último acceso: 30 Diciembre 2021].

[11] J. A. Marín Moya, «Propuesta de mejora de un sistema biométrico multiusuario para cajeros automáticos en instituciones bancarias en la ciudad de Lima -2017,» 2017. [En línea]. Available: https://repositorio.utp.edu.pe/bitstream/handle/20.50-0.12867/862/Jonathan%20Marin_Tesis_Trabajo%20Profesional_2017.pdf?sequence=6&isAllowed=y. [Último acceso: 30 Diciembre 2021].

[12] F. Kausar, « Iris based cancelable biometric cryptosystem for secure healthcare smart card,» Egyptian Informatics Journal, 22(4), pp.447-453, 2021. [En línea]. Available: https://doi.org/10.1016/j.eij.2021.01.004. [Último acceso: 30 Diciembre 2021].

[13] V. Rajasekar, J. Premalatha y K. Sathya, «Enhanced Biometric Recognition for Secure Authentication Using Iris Preprocessing and Hyperelliptic Curve Cryptography,» Wireless Communications and Mobile Computing, 2020, pp.1-15, 2020, 2021. [En línea]. Available: https://doi.org/10.1155/2020/8841021. [Último acceso: 30 Diciembre 2021].

[14] S. Vatsal y S. Mr. Shankar Dwivedi, «Advanced IRIS Recognition System: A Review.,» International Journal of Modern Communication Technologies & Research (IJMCTR), 6(5),, 2018. [En línea]. Available: https://www.neliti.com/publications/265090/advanced-iris-recognition-system-a-review. [Último acceso: 30 Diciembre 2021].

[15] M. S. García Vásquez y A. Á. Ramírez- Acosta, «Avances en el reconocimiento del iris: perspectivas y oportunidades en la investigación de algoritmos biométricos,» 2015. [En línea]. Available: http://www.scielo.org.mx/pdf/cys/v16-n3/v16n3a2.pdf. [Último acceso: 30 Diciembre 2021].