Algoritmos del cifrado para protección de datos biométricos

Encryption algorithms for biometric data protection

Recibido: julio 23 de 2023 | Revisado: setiembre 20 de 2023 | Aceptado: octubre 18 de 2023

Marvin Chavez-Ferrel[1]
Alberto Mendoza-De los Santos[2]

Resumen

La presente revisión tuvo como objetivo examinar las diferentes técnicas o algoritmos de cifrado de datos biométricos usados en la autenticación para la seguridad de la información. En consecuencia, se utilizó la metodología PRISMA para seleccionar artículos en diferentes bases de datos durante el periodo comprendido entre 2019 y 2023. Las bases de datos utilizadas fueron SCOPUS, SCIELO y GOOGLE ACADÉMICO, donde al aplicar los criterios de inclusión y exclusión planteados se consideraron 13 artículos para la presente investigación. De esta forma se pudo notar la necesidad de la aplicación de los algoritmos de cifrado como forma de prevención de ataques y orientados al cumplimiento de los objetivos de la seguridad de la información, siendo los más utilizados el AES (Advanced Encryption Standard) y el cifrado caótico.

Palabras clave: cifrado; biometría; autenticación; seguridad de la información

Abstract

The objective of this review was to examine the different biometric data encryption techniques or algorithms used in authentication for information security. Consequently, the PRISMA methodology was used to select articles in different databases during the period between 2019 and 2023. The databases used were SCOPUS, SCIELO and GOOGLE ACADEMICO, where when applying the proposed inclusion and exclusion criteria, they were considered 13 articles for this research. In this way, it was possible to notice the need to apply encryption algorithms as a form of attack prevention and aimed at meeting the objectives of information security, the most used being AES (Advanced Encryption Standard) and encryption chaotic.

Keywords: encryption, biometrics, authentication, security of the information

1 Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo - Perú
2 Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo - Perú

Autor de correspondencia:
r513300420@unitru.edu.pe

https://doi.org/10.24265/campus.2023.v28n36.08

Introducción

La información es un activo vital dentro de cualquier institución, la seguridad de la información y la ciberseguridad está definidas por un compuesto de instrucciones y elementos, que tienen como misión brindar las tres características fundamentales de la misma las cuales son: disponibilidad, confidencialidad, integridad; implementar políticas de y controles de seguridad de los datos se ha convertido en un proceso de vital importancia para que las organizaciones mantengan salvaguardada sus sistemas ataques, daños o perdidas. (Ramírez y Rinconc, 2022).

En ese contexto, una de las técnicas para garantizar la seguridad de la información usada por las organizaciones es la autenticación biométrica, esta basa en la identificación de características físicas o comportamentales únicas de un individuo, como huellas dactilares, reconocimiento facial, voz, patrones de escritura, entre otros. Estos datos biométricos se utilizan para verificar la identidad de un usuario y proporcionar acceso a sistemas o datos sensibles. La principal ventaja de la autenticación biométrica es que es difícil de falsificar o robar, ya que los rasgos biométricos son inherentes y exclusivos de cada persona (Prieto, 2015).

Sin embargo, a medida que se usa más tecnologías como el reconocimiento facial, las huellas dactilares y la voz para acceder a nuestros dispositivos, cuentas y edificios, ha surgido una preocupación creciente entre los usuarios: ¿cómo se están almacenando y protegiendo nuestros datos biométricos?

La seguridad de almacenamiento es la principal preocupación. Los usuarios temen que los sistemas que almacenan sus datos biométricos puedan ser vulnerables a ataques cibernéticos y que sus características únicas puedan ser robadas. La posibilidad de suplantación de identidad es una preocupación legítima que se encuentra en el centro de esta inquietud.

La preocupación también se extiende a cómo se utilizan nuestros datos biométricos. ¿Pueden ser utilizados para rastrear nuestras actividades, dirigir publicidad hacia nosotros o tomar decisiones automatizadas que afecten nuestra vida cotidiana? Los usuarios quieren saber cómo se utilizan sus rasgos únicos y cuáles son sus derechos en relación con estos datos. La falta de transparencia en la recopilación y uso de datos biométricos es otra fuente de inquietud. Los usuarios desean entender claramente los propósitos detrás de la recopilación de sus datos y quieren que se les informe sobre cómo se utilizarán y protegerán. A pesar de la creencia de que los datos biométricos son difíciles de falsificar, la posibilidad de engañar a los sistemas biométricos es un tema que preocupa a muchos usuarios. ¿Podrían nuestros rasgos biométricos ser suplantados o engañados, lo que pondría en peligro nuestra seguridad?

Para garantizar la seguridad de la información en el contexto de la autenticación biométrica, se utilizan algoritmos de protección de datos biométricos. Estos algoritmos desempeñan un papel crucial en la gestión y almacenamiento de los datos biométricos para evitar su compromiso y asegurar la privacidad de los usuarios.

Método

Se realizó una investigación documental utilizando la metodología PRISMA como guía para revisión sistemática. Se planteó las siguientes preguntas para la implementación de la metodología: ¿Cuáles son los algoritmos de cifrado para protección de datos biométricos? ¿Cuáles son los beneficios de algoritmos de cifrado para protección de datos biométricos?

Las revisiones sistemáticas son resúmenes claros y organizados de información que responden preguntas específicas. Son muy confiables porque se basan en muchos estudios y siguen un proceso claro para reunir, seleccionar y evaluar la evidencia sobre el objetivo de la investigación (Moreno et al., 2018).

Criterios de inclusión y de exclusión

Se utilizó como criterio de inclusión a los artículos publicados entre los años 2019 y 2023. Además, se consideró que contengan los términos como "Algoritmos de Cifrado", "Seguridad de la información biométrica", "Autenticación". Asimismo, los artículos deben estar tanto en español como en inglés para mayor profundización de la revisión.

Finalmente, se consideró los criterios de exclusión como cuando no se detalla de forma practica el uso del algoritmo y no existe una relación del algoritmo de cifrado con biometría. Para una mayor comprensión, se resume lo expuesto con anterioridad en la Tabla 1.

Tabla 1
Criterios de inclusión y exclusión

CRITERIOS DE INCLUSIÓN	Artículos o tesis publicados en el periodo de 2019 - 2023
	Idioma en Español o Inglés
	Se muestra la aplicación de una tecnología y/o algoritmo biométrico
CRITERIOS DE EXCLUSIÓN	No se detalla de forma practica el uso del algoritmo
	No existe una relación del algoritmo de cifrado con biometría

Proceso de recolección de la información

El proceso de búsqueda y recolección de datos se llevó a cabo utilizando una combinación de palabras clave relacionadas con la aplicación de algoritmos de cifrados en la autenticación biométrica. Las palabras clave incluyeron "algoritmos de cifrado para protección de datos biométricos", "autenticación biométrica" y "seguridad de la información". Se utilizó un enfoque transparente para buscar lecturas científicas, y se emplearon diferentes fuentes de datos como SciELO, Google Académico y Scopus.

En el caso del buscador académico SciELO se utilizó el siguiente motor de búsqueda: "encryption algorithm". Los resultados fueron un total de 26 artículos encontrados, de las cuales aplicando los criterios de inclusión y exclusión se seleccionaron dos.

Luego para Google Académico, se buscó con el siguiente motor de búsqueda: "Algoritmo de cifrado y biometría"; donde los resultados fueron un total de 24100 escritos generalizados, ya que es una cantidad muy elevada se le aplicó el filtrado por "artículos", resultando un total final de 141 artículos académicos de los cuales fueron seleccionados cuatro.

Para el caso de Scopus se hizo la búsqueda en base a "TITLE-ABS-KEY (encryption AND biometrics AND information AND security) AND PUBYEAR > 2018 AND PUBYEAR < 2023 AND (LIMIT-TO (EXACTKEYWORD, "Biometrics") OR LIMIT-TO (EXACTKEYWORD, "Authentication") OR LIMIT-TO (EXACTKEYWORD, "Cryptography")) AND (LIMIT-TO (LANGUAGE, "English") OR LIMIT-TO (LANGUAGE, "Spanish")) AND (LIMIT-TO (OA, "all")) AND (LIMIT-TO (DOCTYPE, "ar"))" la cual arrojó un resultado de 26, y fueron seleccionados siete en base a los criterios de exclusión/inclusión.

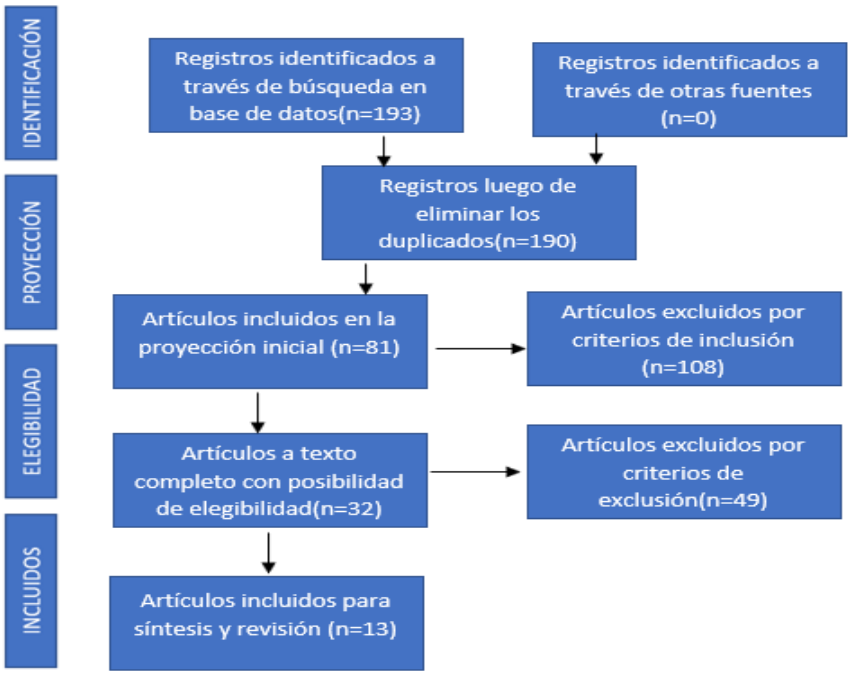
Tabla 2

Bases de datos y artículos seleccionados

Bases de datos	Motor de Búsqueda	Resultados	Seleccionados
SciELO	encryption algorithm	26	2
Google Académico	Algoritmo de cifrado y biometría	141	4
Scopus	TITLE-ABS-KEY (encryption AND biometrics AND information AND security) AND PUBYEAR > 2018 AND PUBYEAR < 2023) AND (LIMIT-TO (OA , "all"))"	26	7

Figura 1

Proceso de selección de artículos / *Flujograma PRISMA*



Resultados

Con los artículos seleccionados y la posterior revisión, se obtuvieron resultados de cada uno de ellos y estos son presentados en la Tabla 3, donde se muestra el(los) autor(es), técnica o algoritmo, país y resultados.

Tabla 3
Resultados de artículos seleccionados

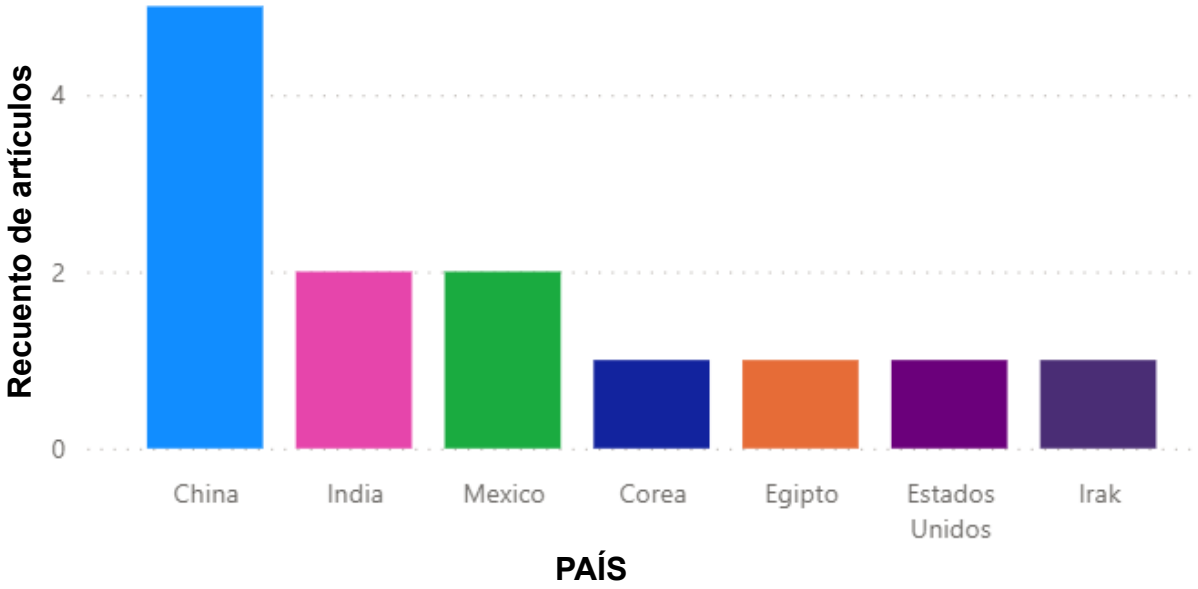
Nº	Autor(es)	Técnica o algoritmo	País	Resultados
1	Lee, J. et al. (2023)	PUF	Corea	Para demostrar que el protocolo propuesto es seguro contra diversos ataques y proporciona funciones de seguridad, se realizó una verificación formal y una verificación informal a través del modelo ROR, la lógica BAN y la herramienta AVISPA Protocolo propuesto puede ser seguro contra ataques de adivinación, repetición, MITM, suplantación y captura de sensores y puede proporcionar anonimato, secreto directo perfecto y autenticación mutua segura.
2	Man, Z. (2023)	Algoritmo de cifrado de imágenes de difusión por rotación adaptativo basado en doble caos	China	La información se almacena en forma de texto cifrado, lo que puede impedir que personal no autorizado la robe y altere ilegalmente El algoritmo es adaptable y eficaz contra ataques de texto sin formato seleccionados. Tras realizarse pruebas al algoritmo se pudo determinar que las claves de cifrado tienen buena aleatoriedad, puede resistir ataques de fuerza bruta, su clave es altamente sensible y puede ocultar efectivamente la información.
3	Patil, S. et al. (2022)	Interpolación de Lagrange y transformada de coseno discreta	India	Los rasgos multibiométricos originales de tamaño 512x512 se reducen a una plantilla de base de datos de 8x8. La técnica de transformación a través de Lagrange y DCT permite crear una imagen irreversible, invinculable y renovable. Permite una autenticación con alta precisión, una base de datos de tamaño constante, ahorro en almacenamiento y protección de rasgos multibiométricos.
4	Hammad, M. et al. (2019)	Biohashing	China	Al aplicar biohashing, técnica biométrica cancelable, se pudo proteger la plantilla de funciones de ECG y huellas dactilares y aumentar la precisión de la autenticación del sistema. La técnica biohashing mejorada permitió proteger las funciones extraídas y permitir la fusión interna, es decir, de las características importantes de cada biométrico y adoptar un sistema multimodal. Se obtuvo Acc(precisión) de 99,12%, FRR(tasa de falsos rechazos) de 0 y FAR(tasa de aceptaciones falsas) de 1,2%.

5	Wang, F. et al. (2019)	Mapa caótico de Chebyshev	China	En el presente trabajo se agrega una carga de cálculo adicional, como el cálculo del polinomio de Chebyshev, para garantizar la seguridad de la información. El esquema presentado es inmune a ataques de adivinanzas fuera de línea, esquema es inmune al ataque de divulgación de claves de sesión, ataque de desincronización, proporciona secreto directo y anonimato del usuario.
6	Kou, L. et al. (2019)	Método de bóveda difusa	Estados Unidos	El protocolo propuesto puede lograr un proceso de autenticación rápido protegiendo las plantillas biométricas. No solo resuelve eficazmente las posibles amenazas a la seguridad de la percepción de la información de IoT, sino que también se implementa fácilmente sin cambiar ninguna condición del hardware. Para mejorar la seguridad del algoritmo, se recomienda que el trabajo futuro puede mejorar el algoritmo aplicando el algoritmo de cifrado ligero.
7	Wu, T. et al. (2021)	Criptografía de curva elíptica (ECC)	China	La seguridad de la comunicación del esquema fue validada por la herramienta ProVerif, y la lógica BAN indicó que la autenticación mutua se puede completar de forma segura. Proporciona anonimato al usuario, un secreto directo perfecto, superar ataques internos privilegiados y de la información temporal específica de la sesión conocida.
8	Taher, B. et al. (2021)	Hash perceptual	Irak	La ventaja de utilizar p-hash es su capacidad tolerante a variaciones sin importancia en la calidad y el formato de la entrada. El tamaño del valor hash que se genera mediante hash perceptivo difiere de 64 a 128 bits. Utilizando la lógica BurrowsAbadi-Needham (BAN), la herramienta de simulación de validación automatizada de protocolos y aplicaciones de seguridad de Internet (AVISPA) y el análisis de seguridad informal demuestran que el algoritmo propuesto es superior a los usados por protocolos de autenticación existentes, en seguridad, funcionalidad y gastos de comunicación y hardware.
9	Wang, Y. et al. (2021)	Generación de claves biológicas Cifrado AES	China	Se utiliza códigos binarios aleatorios para representar datos biométricos y un modelo de aprendizaje profundo para establecer la relación entre los datos biométricos y el código binario aleatorio para cada usuario. Para proteger la privacidad y garantizar la revocabilidad de la clave biométrica, se usa una operación de permutación aleatoria para mezclar los elementos del código binario y actualizar una nueva clave biométrica. Se construyó un módulo de compromiso difuso para generar los datos auxiliares sin revelar ninguna información biométrica durante la inscripción. Para la evaluación se utilizan tres conjuntos de datos de referencia, incluidos ORL, Extended YaleB y CMU-PIE. Los resultados del experimento muestran una tasa de aceptación genuina (GAR) superior a los métodos más modernos con una tasa de aceptación falsa (FAR) del 1% y, mientras tanto, satisface las propiedades de revocabilidad y aleatoriedad de las claves biométricas.

10	Shalaby, A. et al. (2021)	Algoritmo de cifrado caótico generada por una secuencia de mapas logísticos y secuencias de estados de (LFSR)	Egipto	LFSR proporciona mejores resultados criptográficamente en comparación con los métodos que cifran utilizando únicamente un esquema de mapa logístico; proporciona un alto grado de secreto y seguridad. También proporciona un método seguro de transmisión de plantillas de iris a través del canal de comunicación entre los cajeros automáticos y los servidores del banco protegiendo el iris mediante cifrado caótico.
11	Patiño, M. et al. (2021)	Advanced Encryption Standard(AES)	México	AES es un algoritmo muy robusto, ya que no posee claves débiles o semi-débiles, ya que para que un algoritmo de cifrado de imágenes tenga alta seguridad, el espacio de claves debe ser como 2 elevado a la 100, en AES-CAOS el espacio de llaves está dado por 2 elevado a la 128, por lo que no hay restricciones en la selección de la clave. Para que el algoritmo funcione bien, solo se necesita que la clave para cifrar y descifrar sea exactamente la misma. Si se cambias la clave, lo más mínimo posible, los resultados no serán correctos y hacer el descifrado será mucho más complicado.
12	Lohkande, T. et al. (2021)	TDEA (Triple Data Encryption Algorithm)	India	Algoritmo mejorado de DES, que ahora se considera inseguro, debido a que el tamaño efectivo de la clave de 56 bits es demasiado pequeño. Triple DES aumenta el tamaño de la clave de DES para proteger contra ataques sin diseñar un algoritmo de cifrado de bloque completamente nuevo, 64 bits. DES triple se está volviendo poco a poco menos usado, pero todavía es una manera confiable de proteger información importante en el mundo de las finanzas y otras áreas.
13	De Abiega, A. et al. (2022)	Bóveda difusa Algoritmo de lagrange AES	Mexico	Se plantea un algoritmo mediante bóveda difusa basada en huellas dactilares que resiste ataques de multiplicidad de registros conocidos y que no filtra información sobre las huellas dactilares protegidas a partir de datos de alineación auxiliares Se pudo comprobar que con la bóveda cifrada el ataque de fuerza bruta no logró recuperar el polinomio y por lo tanto no se pudo vulnerar la seguridad de este sistema. La prueba en este trabajo se realizó con 256 bits de seguridad, como consecuencia, este nuevo sistema biométrico de bóveda difusa no sólo sería seguro para los tiempos actuales sino también para el futuro. En futuros trabajos es necesario probar otro tipo de ataques como un ataque de correlación o un ataque a través de la multiplicidad de registros, de esta forma se podría demostrar que esta propuesta puede ser efectiva para la protección contra múltiples ataques.

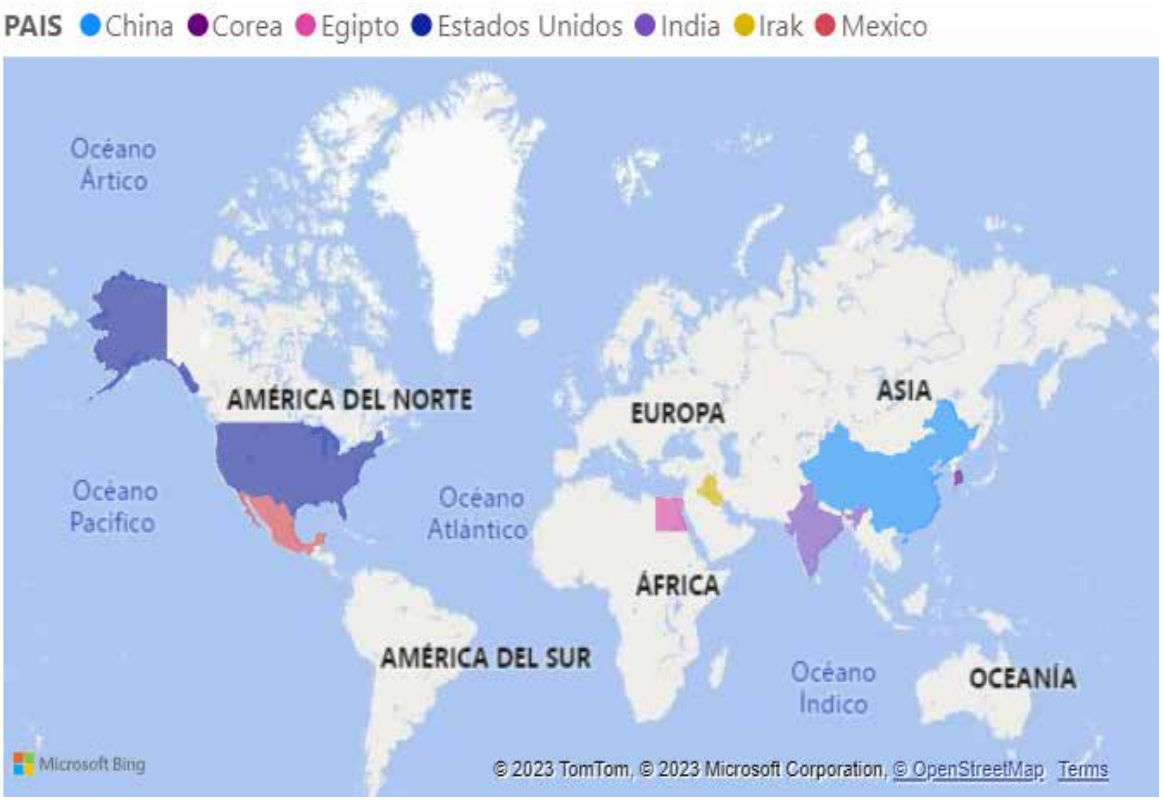
Como se muestra en la siguiente figura, el país que cuenta con mayor número de artículos tomados en cuenta en esta revisión es China con cinco publicaciones, seguido por México y la India con dos publicaciones como se observa en la Figura 2.

Figura 2
Cantidad de artículos por país



En la Figura 3 se observa la ubicación geográfica de los países donde se elaboraron los artículos cuya investigación es acerca de la aplicación algoritmos de cifrado para protección de datos biométricos usados en la autenticación para seguridad de la información

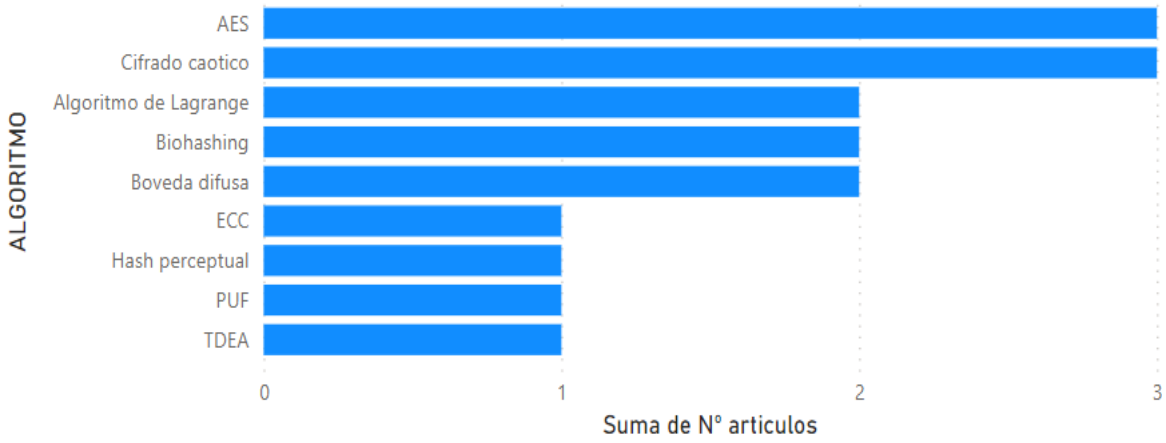
Figura 3
Mapa coroplético de los artículos seleccionados



Producto de la investigación se pudo encontrar los algoritmos y/o técnicas de cifrado usados para protección de datos biométricos que son presentados a continuación; Biohashing, Algoritmo de Lagrange, Hash perceptual, Cifrado Caotico, AES (Advanced Encryption Standard), Boveda difusa, ECC (Criptografia de curva eliptica), PUF (circuitería de función física no clonable), TDEA (Triple Data Encryption Algorithm). Es posible apreciar que los algoritmos más usados son el Cifrado caotico y el AES (Advanced Encryption Standard). Esto debido a que utilizan códigos binarios aleatorios con una gran capacidad y robustez lo que permite proporciona mayor seguridad y complejidad en el descifrado, esta información se muestra reflejada en la Figura 4.

Figura 4

Cantidad de artículos por algoritmo aplicado



Discusión

En base a lo presentado producto de esta revisión vemos como los diversos autores de los artículos nos brindan una visión general de cómo se están implementando algoritmos o técnicas de cifrado para resguardar los datos biométricos usados en la autenticación de los sistemas de información de las organizaciones. Después de analizar los resultados se puede decir que la aplicación de algoritmos y/o técnicas de cifrado biométrico es un campo de aplicación relativamente nuevo y que está siendo altamente demandado por el creciente desarrollo de nuevas amenazas que afectan la vulnerabilidad de los sistemas que utilizan datos biométricos lo que causa preocupación en los clientes, trabajadores y otros usuarios.

Con respecto a los beneficios de los algoritmos, en la mayoría de investigaciones se pudo notar que estaban orientados a proporcionar una seguridad adicional como alternativa de protección frente a ataques, esto se ve reflejado, principalmente, en los resultados presentados por Lee et al. (2023) y Man, Z. (2023) donde el algoritmo usado es seguro contra ataques de adivinación, repetición, MITM, suplantación y captura de sensores y puede proporcionar anonimato, secreto directo perfecto, autenticación mutua y frente a ataques de fuerza bruta.

Asimismo, los algoritmos de cifrado aseguran que los datos biométricos se mantengan confidenciales, incluso si se almacenan en bases de datos centralizadas o se transmiten a través de redes no seguras, esto se ve reflejado en los resultados dados por Hammad, M. et al. (2019) Wang, Y. et al. (2021) donde la técnica usada fue el biohashing o generación de clave biológica, donde para proteger la privacidad y garantizar la revocabilidad de esta, se usa una operación de permutación aleatoria para mezclar los elementos del código binario y actualizar una nueva clave biométrica y la aplicación del cifrado se realiza sin revelar ninguna información biométrica durante la inscripción o toma de datos.

Además, los algoritmos de cifrado utilizados en la autenticación biométrica permiten la implementación de sistemas multimodales o de múltiples factores, reforzando la confidencialidad, uno de los objetivos de la seguridad de la información, este aspecto se puede notar en los artículos elaborados por Patil, S. et al. (2022) donde los rasgos multibiométricos originales se reducen a una plantilla de base de datos de menor tamaño, creando imágenes irreversibles e invinculables con alta precisión, una base de datos de tamaño constante, ahorro en almacenamiento y protección de rasgos multibiométricos.

Por último, se puede apreciar que ciertos algoritmos surgen como reemplazo o en base de las falencias encontradas por otro, como por ejemplo el algoritmo usado por Lohkande, T. et al. (2021), TDEA, surge en base al DES; sin embargo, está quedando obsoleto por lo que está siendo reemplazado por el algoritmo AES, utilizado por Patiño, M. et al. (2021), De Abiega, A. et al. (2022) y Wang, Y. et al. (2021) o por la técnica de Hash perceptual usada por Taher, B. et al. (2021), esto principalmente a que no cumple con la condición dada que para que un algoritmo de cifrado de imágenes tenga alta seguridad, el espacio de claves debe ser al menos tan grande como 2 elevado a 100, lo que garantiza robustez y la alta precisión.

Conclusiones

Las tecnologías de la información (TI) han revolucionado nuestra capacidad para recopilar, procesar y gestionar datos de manera eficiente en la era digital. En este contexto, la gestión de datos biométricos se ha convertido en un aspecto crítico de las TI, con una importancia creciente debido a su carácter altamente personal y único.

La presente investigación identificó las técnicas o algoritmos de cifrado utilizados para la protección de los datos biométricos usados en la autenticación a partir de la revisión de artículos científicos y tesis publicadas a partir de 2019 a 2023 tomando como referencia las bases de datos SCOPUS, SCIELO y GOOGLE ACADEMICO; donde se pudo determinar que AES y el cifrado caótico son las más utilizados, teniendo la presencia en tres artículos cada uno, asimismo, el país que tuvo mayor número de investigaciones referentes al cifrado biométrico fue China.

En cuanto a las limitaciones, podemos decir que los resultados obtenidos corresponden a tres bases de datos, cantidad que puede ser ampliado en una investigación más profunda que complemente la realizada en esta revisión.

Asimismo, se espera continuar ampliando la información en investigaciones futuras, dado que el campo de biometría y en específico los algoritmos de cifrado de datos biométricos se desarrollan continuamente, debido a que algunos van quedando obsoletos, ya que los atacantes encuentran formas de violarlos, por los que surgen nuevas propuestas como respuesta a la necesidad y preocupación de los usuarios acerca del mantenimiento y protección que se les aplica a estos frente a los ataques para evitar la suplantación de identidad y otros más que atenten contra su persona.

Referencias

Camargo, E. A. R., & Pinzón, M. A. R. (2022). La importancia de la seguridad de la información en el sector público en Colombia. RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, 46, 87–99. https://doi.org/10.17013/risti.46.87-99

De Abiega-L'Eglisse, A. F., Gallegos-Garcia, G., Nakano-Miyatake, M., Rosas Otero, M., & Azpeitia Hernández, V. (2022). A New Fuzzy Vault based Biometric System robust to Brute-Force Attack. *Computación y sistemas*, *26*(3). https://doi.org/10.13053/cys-26-3-4184

Hammad, M., Liu, Y., & Wang, K. (2019). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *IEEE access: practical innovations, open solutions*, *7*, 26527–26542. https://doi.org/10.1109/access.2018.2886573

Kou, L., Shi, Y., Zhang, L., Liu, D., & Yang, Q. (2019). A lightweight three-factor user authentication protocol for the information perception of IoT. *Computers, Materials & Continua*, *58*(2), 545–565. https://doi.org/10.32604/cmc.2019.03760

Lee, J., Oh, J., & Park, Y. (2023). A secure and anonymous authentication protocol based on three-factor wireless medical sensor networks. *Electronics*, *12*(6), 1368. https://doi.org/10.3390/electronics12061368

Man, Z. (2023). Biometric information security based on double chaotic rotating diffusion. *Chaos, Solitons, and Fractals*, *172*(113614), 113614. https://doi.org/10.1016/j.chaos.2023.113614

Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. Revista Clínica de Periodoncia, Implantología y Rehabilitación Oral, 11(3), 184–186. https://doi.org/10.4067/s0719-01072018000300184

Patil, S. D., Raut, R., Jhaveri, R. H., Ahanger, T. A., Dhade, P. V., Kathole, A. B., & Vhatkar, K. N. (2022). Robust authentication system with privacy preservation of biometrics. *Security and Communication*

Networks, *2022*, 1–14. https://doi.org/10.1155/2022/7857975

Patiño, M., Godínez, E., Patiño, J.,Balankin, A., Flores,R.,Martinez, M.,Garcia, S.,Manuel, V.(2021). Encriptado de Imágenes Basado en Advanced Encryption Standard y Caos. https://www.researchgate.net/publication/351824897_ENCRIPTADO_DE_IMAGENES_BASADO_EN_ADVANCED_ENCRYPTION_STANDARD_Y_CAOS

Prieto Rodríguez, J. D. (2015). Algoritmo de generación de llaves de cifrado basado en biometría facial. *Revista inventum*, *10*(19), 41–51. https://doi.org/10.26620/uniminuto.inventum.10.19.2015.41-51

Shalaby, A., Gad, R., Hemdan, E. E.-D., & El-Fishawy, N. (2021). An efficient multi-factor authentication scheme based CNNs for securing ATMs over cognitive-IoT. *PeerJ. Computer Science*, *7*(e381), e381. https://doi.org/10.7717/peerj-cs.381

Taher, B. H., Liu, H., Abedi, F., Lu, H., Yassin, A. A., & Mohammed, A. J. (2021). A secure and lightweight three-factor remote user authentication protocol for future IoT applications. *Journal of Sensors*, *2021*, 1–18. https://doi.org/10.1155/2021/8871204

T. Lokhande, S. Sonekar y A. Wani, "Development of an Algorithmic Approach for Hiding Sensitive Data and Recovery of Data based on Fingerprint Identification for Secure Cloud Storage," 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2021, pp. 800-805, doi: 10.1109/SPIN52536.2021.9566026.

Wang, F., Xu, G., & Xu, G. (2019). A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map. *IEEE access: practical innovations, open solutions*, *7*, 101596–101608. https://doi.org/10.1109/access.2019.2930542

Wu, T.-Y., Yang, L., Lee, Z., Chen, C.-M., Pan, J.-S., & Islam, S. K. H. (2021). Improved ECC-based three-factor multiserver authentication scheme. *Security and Communication Networks*, *2021*, 1–14. https://doi.org/10.1155/2021/6627956

Wang, Y., Li, B., Zhang, Y., Wu, J., & Ma, Q. (2021). A secure biometric key generation mechanism via deep learning and its application. *Applied Sciences (Basel, Switzerland)*, *11*(18), 8497. https://doi.org/10.3390/app11188497