Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Ingeniería de software
Recibido: 20/8/2025 | Aceptado: 11/10/2025 | Publicado: 30/3/2026

Identificadores persistentes:
DOI: 10.48168/innosoft.s29.a339
ARK: ark:/42411/s29.a339

Sistema de autenticación multimodal con reconocimiento facial y totp para acceso seguro

Multimodal authentication system with facial recognition and totp for adaptable secure access

Jesús Christopher Mecola Bernedo[1][0009-0000-0709-4220]*, **Julio David Tirado Ávila**[2][0009-0003-0703-086X], **Alberto Carlos Mendoza de los Santos**[3][0000-0002-0469-915X]

[1]Universidad Nacional de Trujillo. Dirección postal.. jmecolab@unitru.edu.pe
[2]Universidad Nacional de Trujillo. Dirección postal.. jtiradoa@unitru.edu.pe
[3]Universidad Nacional de Trujillo. Dirección postal.. amendozad@unitru.edu.pe

*Autor para correspondencia: jmecolab@unitru.edu.pe

Resumen
La creciente sofisticación de las ciberamenazas ha evidenciado la insuficiencia de los sistemas de autenticación basados únicamente en contraseñas. Como respuesta, la autenticación multifactorial (MFA) se ha consolidado como un estándar de seguridad. Sin embargo, la rigidez en la implementación de MFA puede afectar negativamente la experiencia del usuario. Este artículo presenta el diseño, implementación y evaluación de un sistema de autenticación multi-modal que ofrece una aproximación híbrida y flexible, permitiendo a los usuarios verificar su identidad mediante reconocimiento facial o una contraseña de un solo uso basada en el tiempo (TOTP), además de la credencial tradicional de contraseña. El sistema fue desarrollado en Python, utilizando una arquitectura Modelo-Vista-Controlador (MVC) para garantizar la modularidad y escalabilidad. Se emplearon las librerías OpenCV y face$_r ecognition para el módulo biométrico y PyOTP para la implementación del estándar RFC 6238 (TOTP). L$

Palabras claves: Autenticación biométrica, Reconocimiento facial, Sistemas multi-modales, Autenticación de doble factor (2FA), Usabilidad.

Abstract
The increasing sophistication of cyber threats has revealed the limitations of password-based authentication mechanisms. Although multifactor authentication (MFA) has emerged as a security standard, traditional MFA schemes often impose rigid verification flows that negatively impact usability and system adoption. This work presents the design, implementation, and evaluation of a flexible multimodal authentication system that enables user verification through facial recognition or a time-based one-time password (TOTP), in combination with a conventional password. The system was developed in Python following a Model–View–Controller (MVC) architecture to ensure modularity, maintainability, and scalability. The biometric module integrates OpenCV and the face$_r ecognition library to extract and validate facial embeddings, while PyOTP enables TOTP generation and verificati$ based MFA approach can balance usability and security, making the system a viable alternative for academic environmen$ infrastructure scenarios that require secure yet user − friendly identity verification mechanisms.

Keywords: *Biometric Authentication, Facial Recognition, Multi-modal Systems, Two-Factor Authentication (2FA), Usability.*

Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

Introducción

La creciente sofisticación de ataque cibernéticos dirigidos al robo de credenciales y suplantación de identidad ha impulsado la necesidad de mecanismos de autenticación más robustos que las contraseñas tradicionales. La creciente expansión de servicios digitales en los diferentes sectores como salud, administración, finanzas y entornos inteligentes ha incrementado el campo de ataque, haciendo que la autenticación multifactor (MFA) y métodos biométricos sean esenciales para garantizar acceso seguro y confiable [1], [2], [3], [4].

En estudios recientes se destaca una transición progresiva hacia sistemas que combinan múltiples factores de autenticación, incluyendo contraseñas temporales basadas en tiempo (TOTP), tokens físicos y características biométricas [1]. Sin embargo, aún existen brechas entre las capacidades tecnológicas propuestas y su implementación industrial, donde existe un porcentaje considerable de soluciones que continúan dependiendo de OTP como mecanismo principal de autenticación, pese a la existencia de alternativas más robustas. Asimismo, se ha demostrado que el uso exclusivo de contraseñas o de un único factor biométrico puede resultar insuficiente ante escenarios avanzados, esto ha motivado la incorporación de arquitecturas híbridas de autenticación [2], [5], [6].

Avances recientes han explorado esquemas MFA apoyados en criptografía avanzada, tecnologías blockchain, funciones físicamente no clonables (PUF) e incluso comunicaciones seguras cuánticas, logrando mejorar la eficiencia y resiliencia frente a ataques de escucha, fuerza bruta y manipulación de datos [3], [4]. Paralelamente, algunas investigaciones han demostrado el potencial del reconocimiento facial combinado con modelos de aprendizaje profundo para reducir las tasas de error en la validación biométrica, con aplicaciones en sistemas IoT, y entornos de alta seguridad [5], [6], [7]. No obstante, persisten desafíos asociados a la privacidad, la gestión segura de datos y la accesibilidad de estas tecnologías para los usuarios finales y sistemas de bajo costo [7], [8].

A pesar de estos avances, la mayoría de las soluciones MFA se basan en esquemas de autenticación rígidos que requieren la activación simultánea de múltiples factores, lo cual puede comprometer la experiencia del usuario, incrementar el tiempo de acceso y limitar así la adopción de la tecnología en contextos cotidianos. Por ello existe la necesidad de modelos más flexibles que permitan al usuario autenticarse mediante distintos factores según los recursos de los que dispone, sin comprometer la seguridad.

En este trabajo se propone un sistema de autenticación multimodal flexible basado en reconocimiento facial y contraseñas temporales TOTP bajo una lógica OR, lo que permite al usuario seleccionar dinámicamente el método de autenticación según su conveniencia y disponibilidad. El sistema se implementa en Python con

arquitectura modular, empleando visión por computadora para reconocimiento facial y estándares TOTP para autenticación temporal, integrando mecanismos de auditoría, bloqueo tras intentos fallidos y almacenamiento seguro. Nuestro objetivo principal es demostrar que un enfoque híbrido puede mantener niveles elevados de seguridad mientras se mejora la usabilidad y reduce la brecha tecnológica entre soluciones experimentales y aplicaciones de acceso general.

Metodología computacional

La metodología se basó en un enfoque de ingeniería de software seguro y modular, orientado a la construcción de un sistema de autenticación multimodal flexible que permita validar la identidad mediante el reconocimiento facial o códigos temporales basados en tiempo (TOTP), utilizando lógica OR.

Arquitectura General del Sistema

Se adoptó el patrón arquitectónico MVC para separar capa lógica, gestión de datos e interfaz. Las principales capas consideradas fueron:

Vista (GUI): desarrollada con CustomTkinter para lograr una interfaz moderna y multiplataforma.

Controladores: PyOTP para la generación y validación de códigos TOTP.

Seguridad y Persistencia: bcrypt para el hashing de contraseñas y SQLite como base de datos embebida.

Tecnologías utilizadas

La solución se implemento en Python 3.8+, integrando bibliotecas robustas y ampliamente soportadas:

CustomTkinter para interfaz GUI moderna.

OpenCV para capturar y procesar imágenes.

Fase_recongnition + dlib para extraer y verificar los embeddings faciales.

PyOTP para autenticación TOTP conforme al estándar RFC-6238.

Bcrypt para el hashing seguro de credenciales.

SQLite para almacenamiento local cifrado.

Pillow para manipulación básica de imágenes.ç

Todas estas herramientas fueron seleccionadas para permitir un despliegue en equipos convencionales sin necesidad de tener hardware especializado.

Módulo de Reconocimiento Facial

Para la detección del rostro, se utiliza un modelo clasificador basado en Histogramas de Gradientes Orientados (HOG), el cual ofrece un equilibrio adecuado entre eficiencia computacional y precisión, especialmente en escenarios en donde no se disponen de unidades de procesamiento gráfico avanzadas [9]. Posteriormente, las características biométricas fueron codificadas en vectores embeddings faciales mediante modelos basados en redes neuronales profundas, estableciendo mediciones mediante distancia euclidiana para la verificación [10]. Con el fin de mejorar la estabilidad del reconocimiento frente a variaciones de iluminación, expresión y postura, se almacenaron cinco codificaciones por usuario y se definió un umbral empírico de 0.6 para determinar coincidencias válidas.

Módulo de Autenticación 2FA/TOTP

La implementación del segundo factor se adhiere al estándar RFC 6238, que genera códigos de seis dígitos con rotación cada treinta segundos para maximizar la seguridad temporal del token [11]. Asimismo, se integró soporte para tolerancia de ventana temporal en un intervalo de ± 1 para reducir falsos rechazos por desfase de horario, siguiendo recomendaciones del RFC 4226 orientadas a mecanismos HMAC-OTP [12]. El registro del usuario se ejecuta generando una clave secreta almacenada de forma segura, para sincronización con aplicaciones móviles como Google Authenticator, manteniendo independencia del sistema respecto a servicios externos.

Seguridad y Protección de Datos

Para la seguridad y protección de credenciales, se empleó el algoritmo bcrypt, reconocido por su capacidad para aplicar salt automático y un costo computacional adaptable a lo largo del tiempo, característica que fortalece la resistencia frente a ataques y cracking de contraseñas [13]. Además, se incorporaron medidas de seguridad alineadas a lineamientos del NIST Digital Identity Guyidelines [14] y recomendaciones OWASP para autenticación robusta, incluyendo bloqueo automático tras tres intentos fallidos, auditoria y registro de eventos, sesiones no persistentes en memoria y almacenamiento seguro de secretos [15]. La base de datos SQLite fue utilizada para asegurar portabilidad y operaciones en entornos offline, permitiendo mantener la información biométrica y los registros de autenticación guardados localmente.

Lógica OR de Autenticación

A diferencia de esquemas tradicionales MFA basados en lógica AND, este sistema implementa OR.

Este diseño incrementa accesibilidad y continuidad operativa sin comprometer la disponibilidad del sistema, siendo especialmente adecuado para usuarios sin un factor disponible en ese momento (e.g., cámara dañada o teléfono descargado).

Evaluación del Sistema

Se realizaron pruebas funcionales para medir la precisión biométrica mediante tasas FAR y FRR, tiempo promedio de autenticación tanto facial como TOTP, consumo de recursos en ejecución, comportamiento del sistema ante intentos fallidos consecutivos y percepción de usabilidad por parte de usuarios de prueba. Se destaca que el sistema prioriza eficiencia y seguridad en entornos de uso local, por lo que aún no incorpora técnicas avanzadas de detección de vida (liveness detection). La incorporación de mecanismos anti-spoofing se identifica como trabajo futuro, tomando como referencia estudios recientes de revisión sistemática en detección de falsificación facial con cámaras RGB convencionales [16, 17].

Documentación visual del funcionamiento

Para garantizar reproducibilidad y claridad visual, se incorporarán capturas del sistema en las siguientes etapas:

Pantalla inicial (selección facial/TOTP).

Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

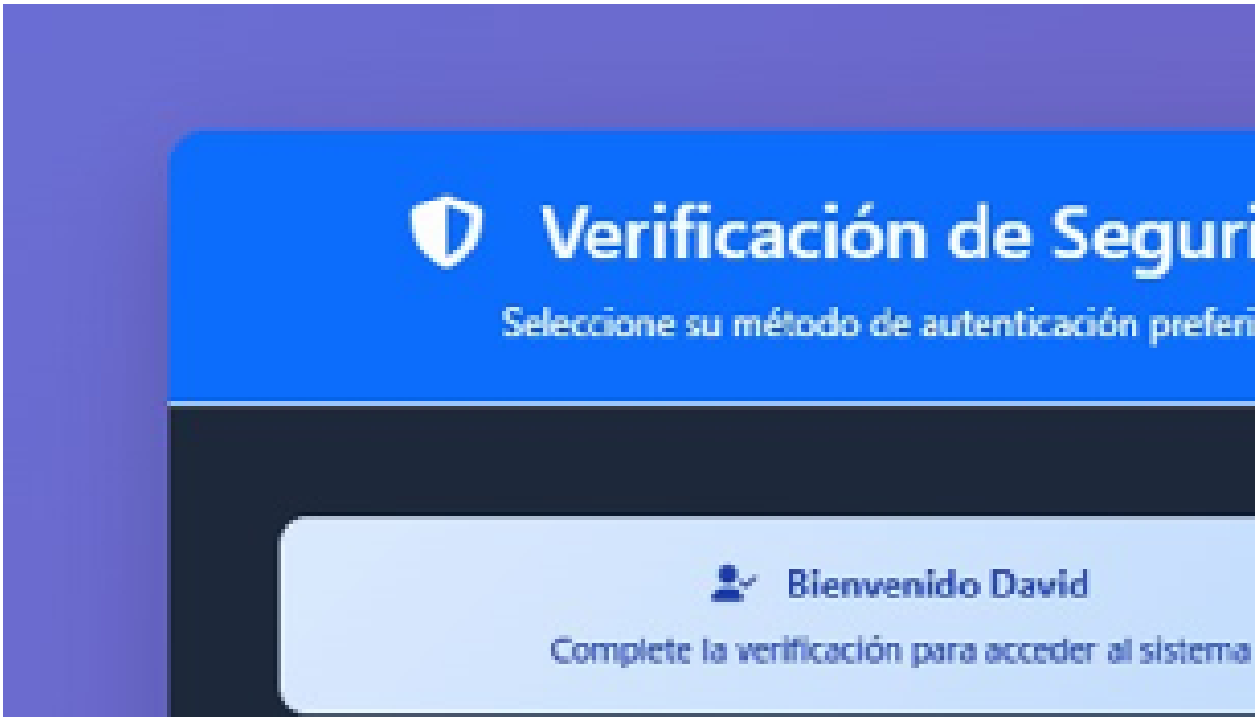
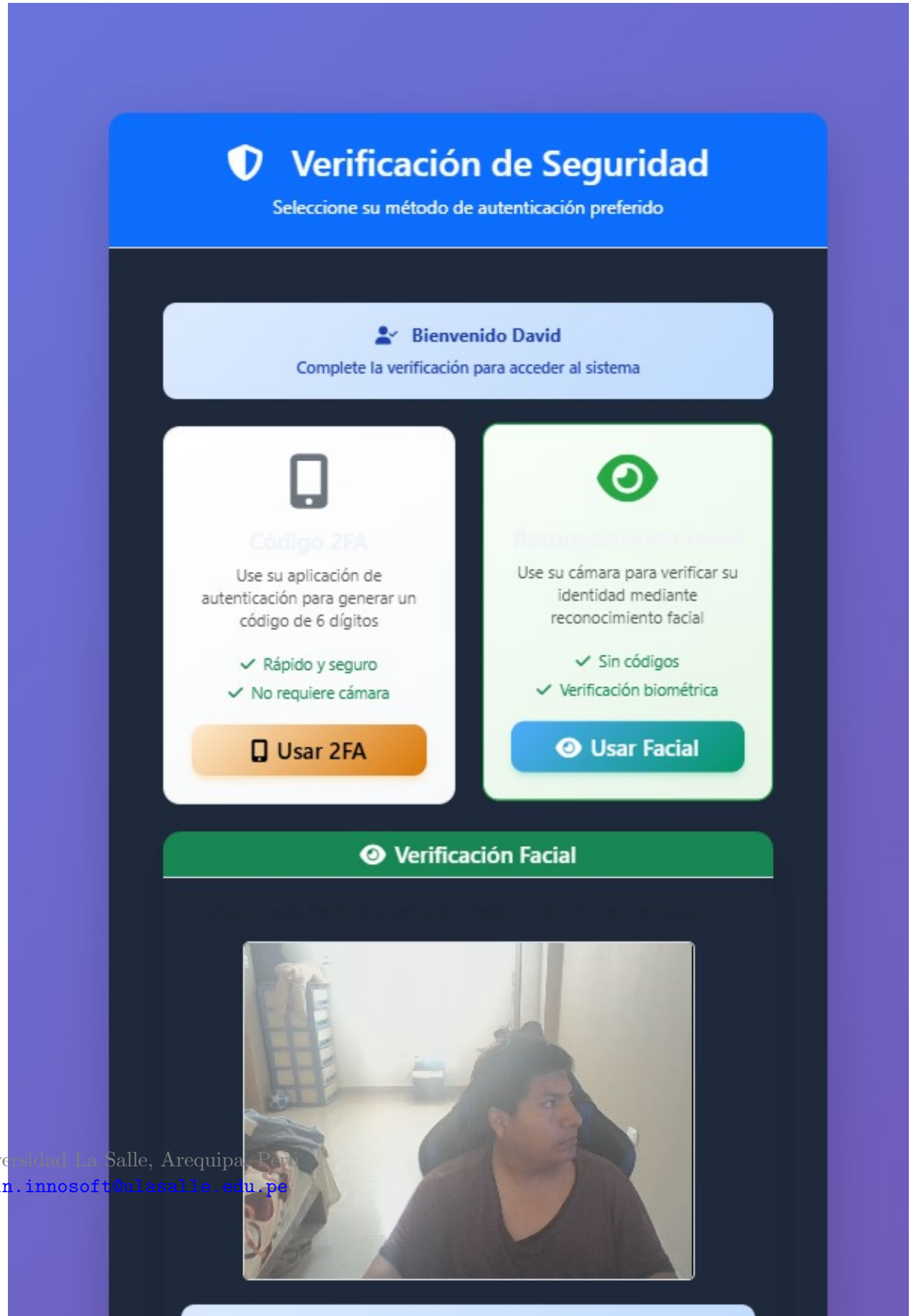


Figura 1. Figura 1. Pantalla inicial

Registro biométrico y captura facial en vivo.

Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft



Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

Configuración del reconocimiento facial con cuadro delimitador.

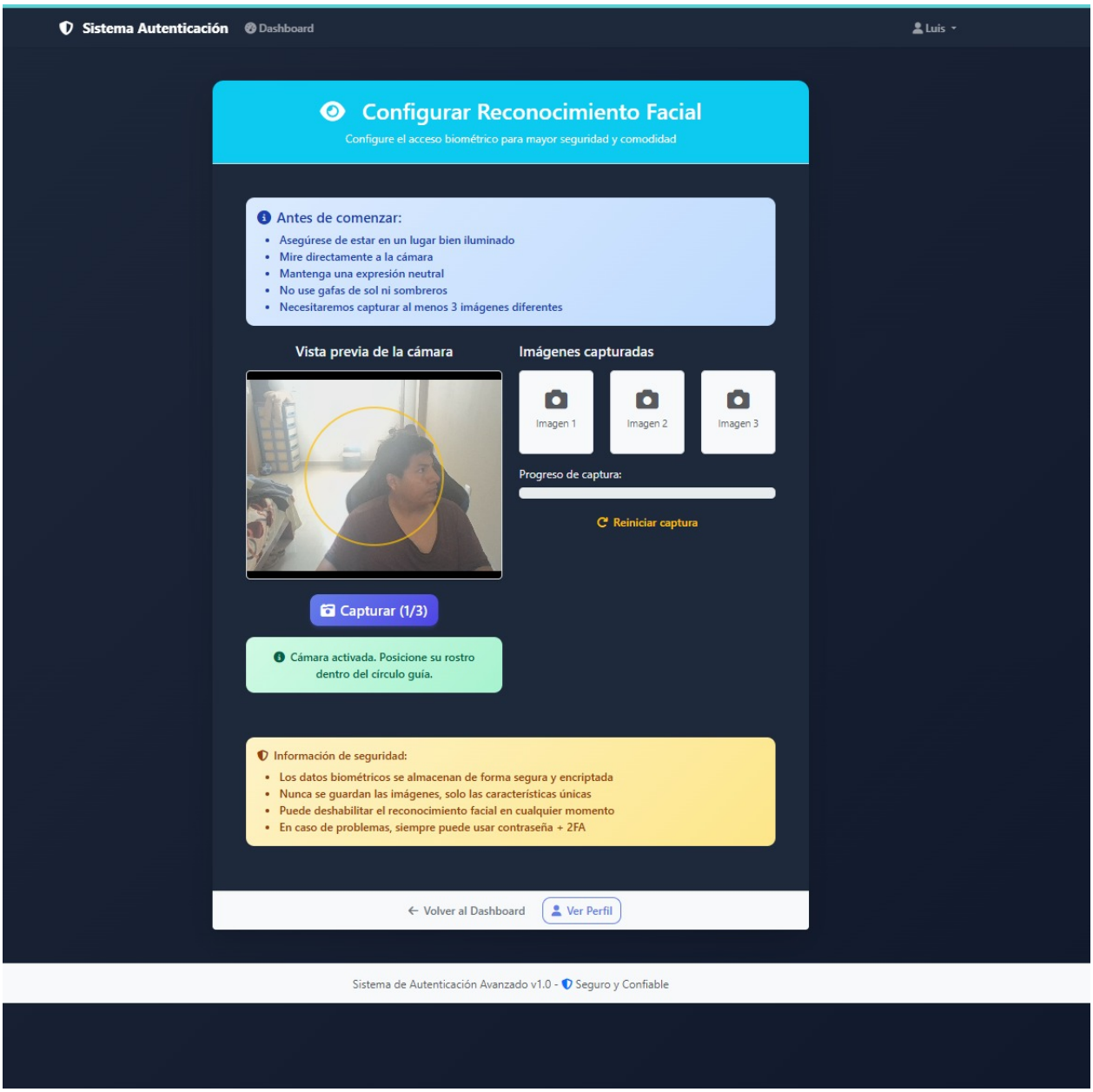


Figura 3. Figura 3. Configuración del reconocimiento facial

Generación y lectura del codigo de sincronización TOTP.

Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

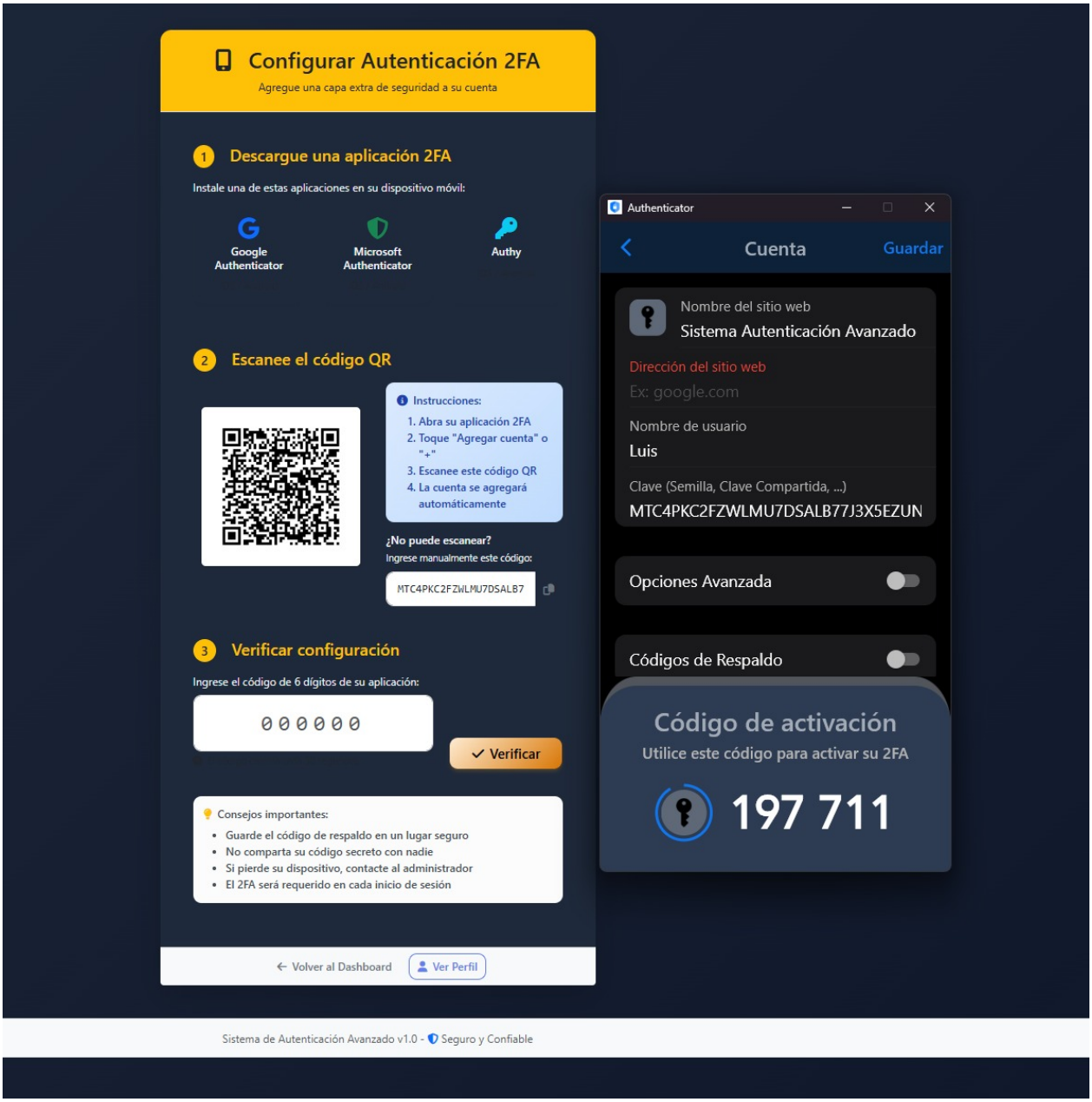


Figura 4. Figura 4. Generación y lectura del código de sincronización TOTP

Ventana de verificación TOTP.

Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

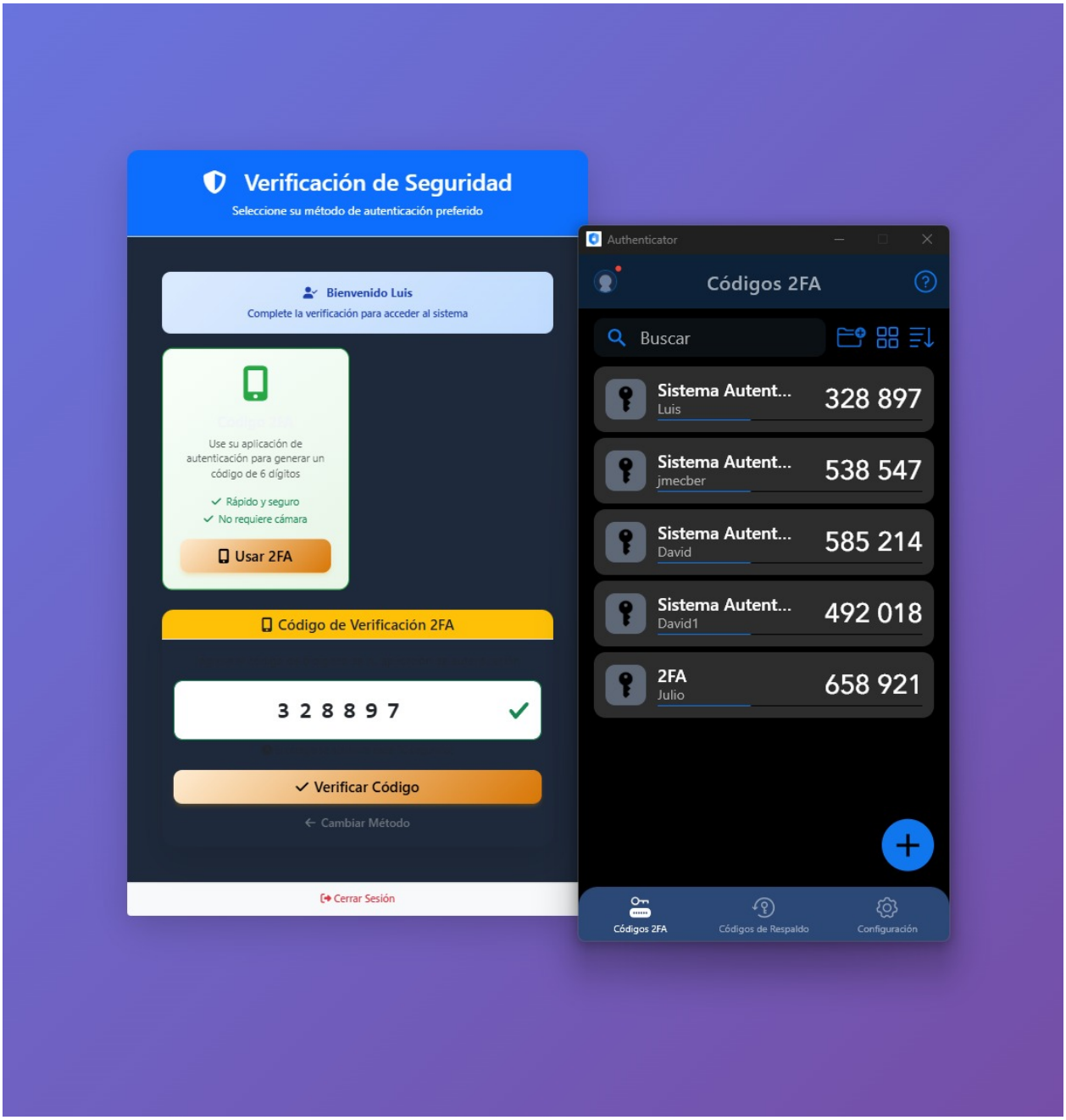


Figura 5. Figura 5. Verificación del TOTP

Gráficas de tiempo y precisión.

Revista Innovación y Software
Vol. 7, No. 1, Mes Marzo - Agosto, 2026
ISSN: 2708-0935
Pág. 80-93
https://revistas.ulasalle.edu.pe/innosoft

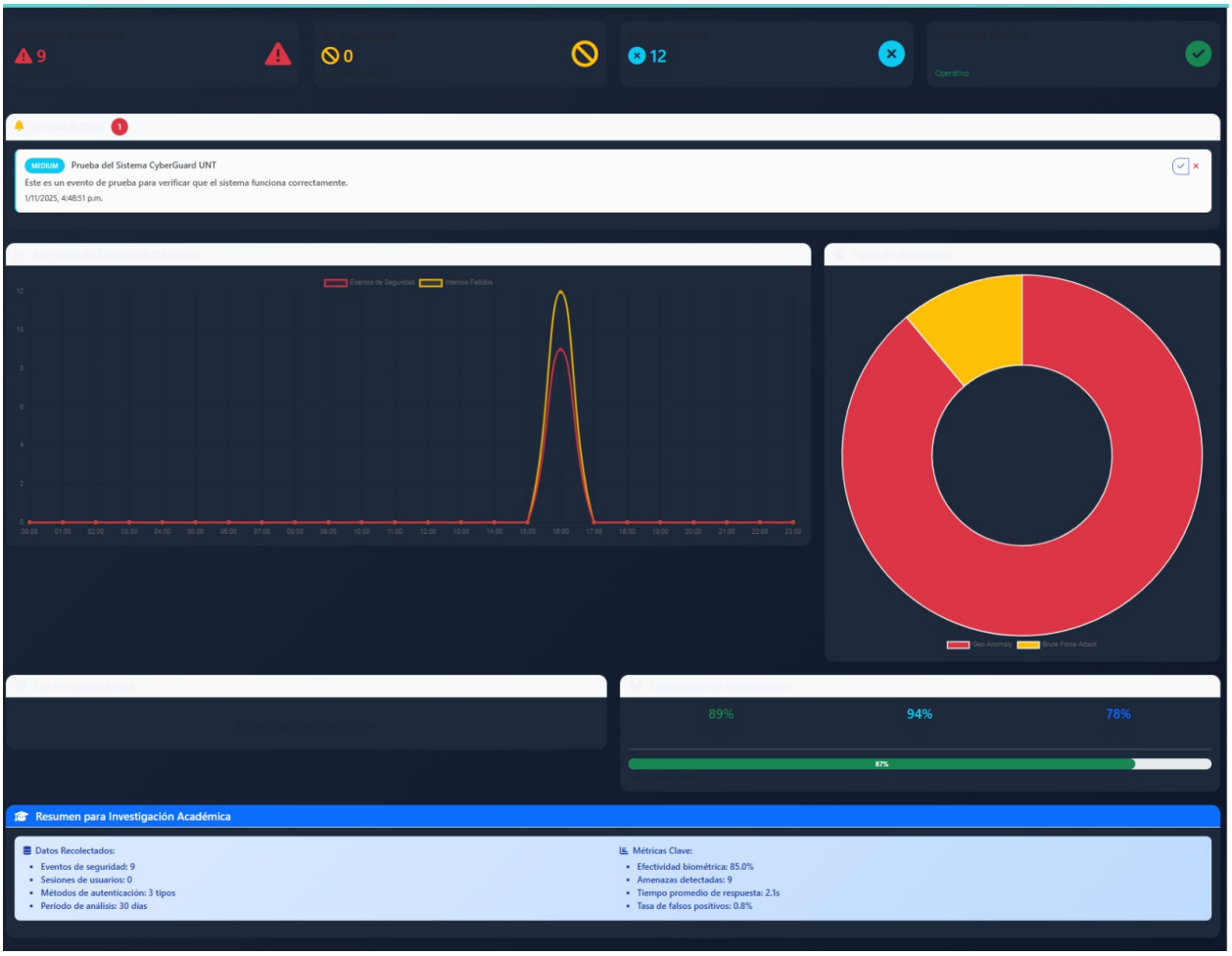


Figura 6. Figura 6. Graficas de precisión y tiempo mostrando efectividad biométrica (85 %), tasa de falsos positivos (0.8 %) y tiempo promedio de respuesta (2.1 s) durante autenticaciones reales.

Resultados y discusión

Las pruebas experimentales se desarrollaron en un entorno controlado utilizando usuarios reales y distintos escenarios de autenticación. El sistema registró un total de nueve eventos de seguridad y tres sesiones de autenticación dentro del período de validación capturado. La visualización del desempeño se presenta a través de gráficos de distribución temporal, donut chart para tipos de amenazas y barras comparativas para precisión entre métodos.

Como se puede apreciar en la Figura 6. los resultados evidencian una efectividad biométrica del 85 %, con

una tasa de falsos positivos de solo 0.8 %, valor adecuado para un entorno de seguridad local. El tiempo promedio de respuesta fue 2.1 segundos, considerando captura facial, análisis y decisión. La validación mediante TOTP presentó una efectividad del 94 %, exhibiendo menor latencia y mayor estabilidad frente a variaciones ambientales, como se esperaba dada la naturaleza determinista del algoritmo TOTP.

Estos resultados obtenidos se pueden contrastar con las investigaciones anteriores. Según el análisis sistemático de MFA en plataformas digitales [1], un porcentaje importante de sistemas aún depende primariamente de OTP, con poco uso de biometría. Nuestro sistema mejora este enfoque al haber incorporado reconocimiento facial y TOTP local, eliminando dependencia de servidores externos.

En soluciones MFA tradicionales [2], la lógica predominante es el esquema de verificación simultánea (AND), incrementando la carga de usuario. Al haber implementado la estrategia OR este trabajo demuestra mantener seguridad aceptable sin comprometer la experiencia del usuario en concordancia con propuestas emergentes de autenticación flexible.

En entornos avanzados, como arquitecturas MFA basadas en blockchain y PUF [3], se reportan mejoras en integridad e inmutabilidad, pero con mayor complejidad y altos costos computacionales. Nuestro sistema, aunque no incorpora técnicas de seguridad distribuida, optimiza eficiencia para dispositivos convencionales y despliegues académicos, alineándose con la necesidad de soluciones accesibles.

Respecto a la biometría, estudios anteriores reportan incrementos significativos en precisión al combinar señales faciales y de voz [6]; nuestro enfoque facial mantiene tasas competitivas considerando los recursos disponibles, con un FAR de 0.8 % cercano al esperado en sistemas HOG + embeddings, confirmado por [9, 10].

En resumen, el sistema logra una combinación efectiva de precisión, simplicidad y flexibilidad, aportando una alternativa práctica frente a modelos complejos de autenticación multifactor y demostrando resultados consistentes con la literatura existente.

Conclusiones

Este trabajo presentó un sistema de autenticación multimodal flexible basado en reconocimiento facial y contraseñas temporales TOTP, utilizando una lógica OR con el fin de mejorar la accesibilidad y la experiencia de usuario sin comprometer la seguridad en entornos de uso local. La arquitectura implementada, desarrollada en Python mediante un modelo MVC y utilizando librerías de visión por computadora, permitió la creación de un sistema eficiente, portable y reproducible en equipos convencionales.

Los resultados experimentales evidenciaron una precisión biométrica del 85 %, una tasa de falsos positivos de 0.8 % y un tiempo promedio de respuesta de 2.1 segundos en la autenticación facial. El sistema TOTP alcanzó un umbral de 94 % de efectividad, consolidándose como un método robusto y de baja latencia. Estas métricas se encuentran en rangos de aceptación para sistemas de seguridad local y concuerdan con los valores reportados en soluciones biométricas ligeras en la literatura.

Para futuras investigaciones se propone entrenamiento con modelos avanzados de reconocimiento facial como ArcFace o FaceNet extendido, una evaluación con mayor numero de usuarios y escenarios reales.

En términos generales, los resultados obtenidos permiten validar nuestra propuesta como una solución efectiva y accesible para investigación académica, laboratorios educativos, entornos de prueba y sistemas locales que requieran autenticar usuarios mediante factores alternativos sin depender de servicios externos.

Contribución de Autoría

Jesus Christopher Mecola Bernedo: Conceptualización, Investigación, Metodología, Validación, Redacción - borrador original. Julio David Tirado Ávila: Conceptualización, Investigación, Metodología, Software, Análisis formal, Recursos, Visualización. Alberto Carlos Mendoza de los Santos: Supervisión, Administración de proyectos.

Referencias

[1] P. T. Tran-Truong, M. Q. Pham, H. X. Hijo, E. t. Nguyen, M. B. Nguyen, K. L. Tran, L. C. Van, K. T. Le, K. H. Vo, N. N. Kim, T. M. Nguyen, and A. T. Nguyen, "A systematic review of multi-factor authentication in digital payment systems: Nist standards alignment and industry implementation analysis," *Journal of Systems Architecture*, vol. 162, p. 103402, 2025.

[2] A. Al-Mutairi and R. Al-Sahli, "Secure authentication system based on multi-factor authentication," 2024.

[3] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-layered multi-factor authentication using decentralized blockchain in an iot environment," *Sensors*, vol. 24, no. 11, p. 3575, 2024.

[4] R. I. Abdelfatah, "Robust biometric identity authentication scheme using quantum voice encryption and quantum secure direct communications for cybersecurity," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, p. 102062, 2024.

[5] S. Pahuja and N. Goel, "Multimodal biometric authentication: A review," *AI Communications: The European Journal on Artificial Intelligence*, vol. 37, no. 4, pp. 525–547, 2024.

[6] B. Alharbi and H. S. Alshanbari, "Face-voice based multimodal biometric authentication system via facenet and gmm," *PeerJ Computer Science*, vol. 9, p. 1468, 2023.

[7] M. Beltrán and M. Calvo, "A privacy threat model for identity verification based on facial recognition," *Computers & Security*, vol. 132, p. 103324, 2023.

[8] L. Hallal, J. Rhinelander, and R. Venkat, "Recent trends of authentication methods in extended reality: A survey," *Appl. Syst. Innov.*, vol. 7, no. 3, p. 45, 2024.

[9] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, vol. 1, 2005, pp. 886–893.

[10] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823.

[11] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "Totp: Time-based one-time password algorithm," Internet Engineering Task Force (IETF), 2011.

[12] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "Hotp: An hmac-based one-time password algorithm," Internet Engineering Task Force (IETF), 2005.

[13] N. Provos and D. Mazieres, "A future-adaptable password scheme," in *Proc. USENIX Annual Technical Conference*, 1999, pp. 81–92.

[14] P. Grassi, J. Fenton, E. Newton, R. Perlner, A. Regenscheid, W. Burr, and J. Richer, "Digital identity guidelines: Authentication and lifecycle management," National Institute of Standards and Technology (NIST), 2017.

[15] OWASP Foundation, "Owasp cheat sheet series," 2024. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[16] Z. Ming, M. Visani, M. Luqman, and J.-C. Burie, "A survey on anti-spoofing methods for face recognition with rgb cameras of generic consumer devices," Computer Vision and Pattern Recognition (cs.CV), 2020.

[17] S. Khairnar, S. Gite, K. Kotecha, and S. Thepade, "Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions," *Big Data and Cognitive Computing*, vol. 7, no. 1, p. 37, 2023.