

# Analisis bibliografico - Reconocimiento facial

Sergio Peinado Cuevas - 506221009, Michael Esteban Castillo Lopez - 506221049

**Resumen**—In the contemporary era, Facial Expression Recognition (FER) plays a pivotal role in numerous fields due to its vast application areas, such as e-learning, healthcare, marketing, and psychology. FER involves analyzing facial features to identify and verify individuals, making it a crucial area within artificial intelligence (AI) and machine learning (ML). This technology has applications ranging from security and surveillance to personalized services.

To explore this topic further, we conducted a comprehensive and critical bibliographic analysis of various findings and projects related to facial recognition. Our review included over 100 academic papers retrieved from Scopus. We identified common themes, emerging trends, and advancements in FER. Additionally, we examined predominant methodological approaches, including machine learning and deep learning techniques, face detection, pre-processing, handcrafted feature extraction, and emotion classifiers.

Challenges such as illumination, pose, and scale variation impact the accuracy of FER systems in controlled and spontaneous facial expression datasets. Looking ahead, the development of multimodal FER systems for real-time scenarios, considering computational efficiency, remains an important avenue for enhancing system performance and reducing error rates.

## I. INTRODUCCIÓN

El reconocimiento facial, es una tecnología que ha ganado una importancia significativa en las últimas décadas, consolidándose como una de las áreas más innovadoras y desafiantes dentro de la inteligencia artificial (IA) y el aprendizaje automático (ML). Esta tecnología permite la identificación y verificación de personas mediante el análisis de sus características faciales y tiene aplicaciones que abarcan desde la seguridad y la vigilancia hasta la personalización de servicios. Por manejar temas tan útiles es que se decidió la elección de este tema para la búsqueda en la base de datos scopus, con la finalidad de aprender más sobre el tema y como esta búsqueda nos ayuda con estrategias e información para la realización de nuestro proyecto de detección de fraude en exámenes.

En este análisis bibliográfico realizamos una revisión exhaustiva y crítica de los diversos hallazgos y proyectos sobre el reconocimiento facial. A través de la recopilación y análisis de más de 100 artículos académicos, identificamos temas comunes, tendencias emergentes y avances en esta área. Además, se busca comprender los enfoques metodológicos predominantes para futuros proyectos.

## II. DESCRIPCIÓN DEL TEMA Y JUSTIFICACIÓN DE LA ELECCIÓN

### II-A. ¿Que es el reconocimiento facial?

El reconocimiento facial es una tecnología que permite identificar o verificar la identidad de una persona mediante el análisis y comparación de las características faciales. Funciona capturando una imagen o un video del rostro de una

persona y utilizando algoritmos de procesamiento de imágenes y aprendizaje automático para extraer características únicas, como la distancia entre los ojos, la forma de la nariz y la estructura ósea. Estas características se comparan con una base de datos de rostros almacenados para encontrar coincidencias y determinar la identidad del individuo. Esta tecnología se utiliza en una variedad de aplicaciones, incluyendo seguridad, autenticación de usuarios, vigilancia y personalización de servicios.

### II-B. ¿Como funciona?

El reconocimiento facial funciona en tres pasos principales:

1. Captura de la Imagen: Se toma una foto o video del rostro de una persona mediante una cámara.
2. Análisis de Características: La imagen capturada se analiza usando algoritmos que identifican y miden características faciales clave, como la distancia entre los ojos, la forma de la nariz, y la estructura de la mandíbula. Estas características se convierten en un "mapa" o "firma" facial digital.
3. Comparación y Verificación: El mapa facial se compara con una base de datos de rostros previamente almacenados. Si hay una coincidencia, se verifica la identidad de la persona; si no, se rechaza o se marca como desconocido.

Este proceso permite identificar o autenticar personas de manera rápida y precisa en diversas aplicaciones, siendo esto el inicio o raíz de varios proyectos que divergen según el objetivo.

### II-C. ¿Porque la eleccion del tema?

El reconocimiento facial se eligió como tema de estudio debido a su relevancia y potencial en el campo de la seguridad académica, particularmente en la detección de intentos de copia durante exámenes. La capacidad de analizar y detectar expresiones faciales y comportamientos sospechosos en tiempo real ofrece una solución eficaz para mantener la integridad de los procesos de evaluación.

### II-D. Nuestro proyecto

Nuestro proyecto tiene como objetivo desarrollar un sistema de asistencia para docentes durante la realización de exámenes, tanto virtuales como presenciales. Este sistema utilizará una cámara para capturar video en tiempo real, el cual será analizado por algoritmos de reconocimiento facial y detección de movimientos sospechosos. El video se mostrará en un computador manejado por el docente, quien recibirá alertas automáticas cuando el sistema detecte comportamientos que podrían indicar intentos de copia durante el examen. Esta

tecnología busca mejorar la integridad de los procesos de evaluación y facilitar la labor de supervisión de los docentes.

### III. METODOLOGÍA APLICADA

#### III-A. Query inicial

Nuestra búsqueda comienza con el siguiente query:

”TITLE-ABS-KEY (face AND detection)”

El cual arroja 61,263 documentos a dia de hoy 31 de mayo, aqui es donde surge la necesidad de limitar nuestra busqueda para encontrar los documentos que nos pueden aportar mas informacion frente otros que probablemente no se enfoquen completamente en nuestras necesidades o no logremos tener un acceso completo al documento (debido a nuestra plan de suscripcion a la base de datos).

#### III-B. Construcción del query

**III-B1. Filtro por area academica:** Empezamos limitando la aparicion de los documentos segun el area academica, en este caso seleccionamos ingenierias, matematicas y ciencia de computación. Este simple cambio nos encuentra 43,640 documentos la cual sigue siendo una cifra grande pero tenemos la certeza de que todos los documentos son acorde a nuestro tema de interes.

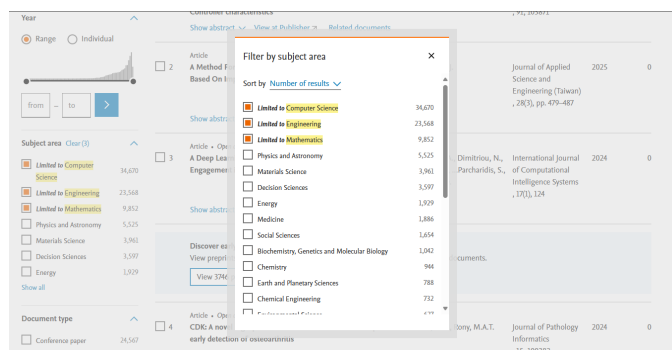


Figura 1. Subject area

**III-B2. Filtro por tipo de documento:** Este filtro es esencial porque permite a los investigadores enfocar sus búsquedas en formatos específicos, como artículos de investigación, revisiones o conferencias. Esto mejora la relevancia de los resultados, ahorra tiempo y asegura que se obtenga la información más adecuada y de calidad para sus necesidades académicas o científicas.

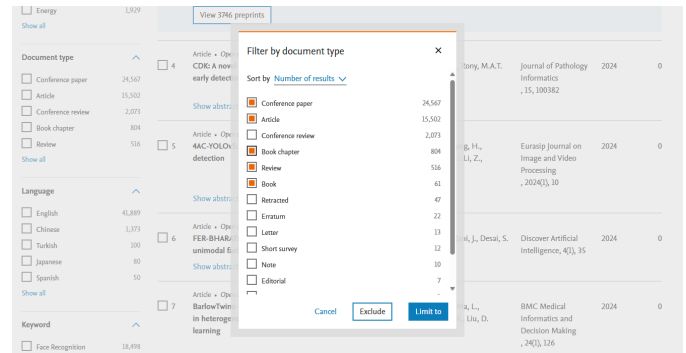


Figura 2. Document type

**III-B3. Filtro por idioma:** Para nuestro caso elegiremos los idiomas ingles y español, el primero porque es el idioma mas relevante y en el que mas documentos se publican y el segundo es un buen agregado ya que manejamos el idioma, si bien los documentos escritos español no estan en la misma cantidad que los escritos en ingles, podriamos omitir grandes hallazgos que nos benefician.

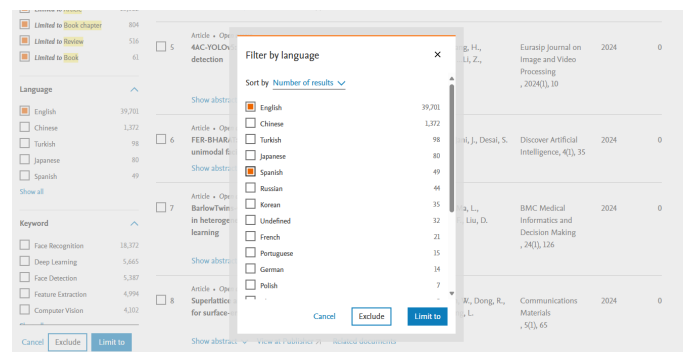


Figura 3. Language

**III-B4. Filtro por palabras clave:** Se eligieron un total de 30 palabras claves, de las cuales solo cuatro cumplen con los filtros que elegimos anteriormente, disminuyendo la cantidad de documentos a un total de 27,943. Con esta cifra y por sobre todo las cuatro palabras clave que se encontraron en los documentos, podemos deternernos y empezar con el analisis bibliografico para determinar si hay un documento que cumpla con nuestra busqueda ya que, de las palabras claves seleccionadas de las cuales no se encontraron documentos, tenemos 'Optimization', 'Facial expression recognition', 'Students' y 'Gesture recognition'.

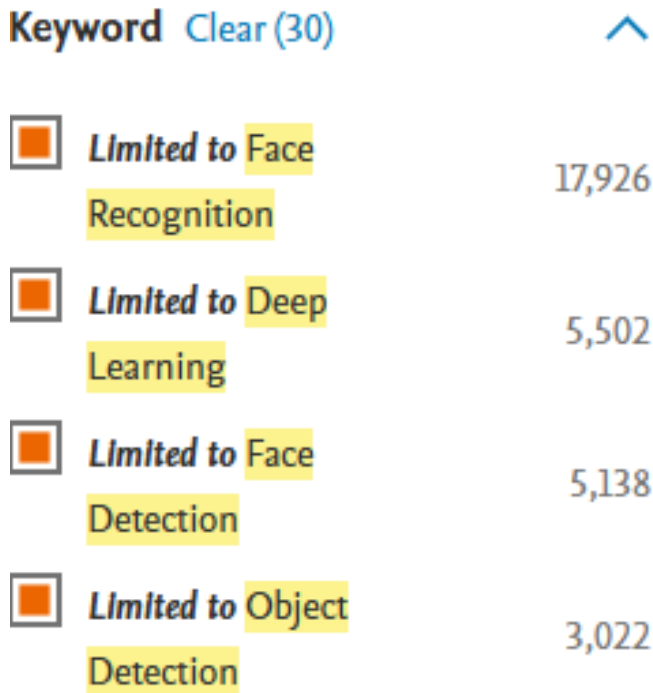


Figura 4. Keyword

#### IV. RESULTADOS DEL ANÁLISIS

El query resultante de todos estos filtros:

TITLE-ABS-KEY ( face AND detection AND fraud )  
AND ( LIMIT-TO ( SUBJAREA , ÇOMP”) OR LIMIT-TO ( SUBJAREA , <sup>EN</sup>GI”) OR LIMIT-TO ( SUBJAREA , ”MATH”) ) AND ( LIMIT-TO ( DOCTYPE , çp”) OR LIMIT-TO ( DOCTYPE , <sup>3</sup>r”) OR LIMIT-TO ( DOCTYPE , re”) OR LIMIT-TO ( DOCTYPE , çh”) ) AND ( LIMIT-TO ( LANGUAGE , <sup>English</sup>”) ) AND ( LIMIT-TO ( EXACTKEYWORD , ”Face Recognition”) OR LIMIT-TO ( EXACTKEYWORD , ”Deep Learning”) )

#### IV-A. Discusión de los Resultados

Este query de búsqueda en Scopus busca documentos que contengan las palabras "facez" "detection".<sup>en</sup> su título, resumen o palabras clave, limitados a las áreas de informática, ingeniería o matemáticas. Además, se restringe a documentos como artículos de conferencia, artículos de revista, libros, revisiones o capítulos de libros, en inglés o español, y que incluyan palabras clave como reconocimiento facial", "aprendizaje profundo", "detección facial." "detección de objetos".

Con un total de 156 documentos procederemos a exportarlos en formato csv para poder realizar su analisis con la ayuda del Google Colab que nos brindo el profesor Oscar Mendez Aguirre.

#### IV-B. Analisis de títulos

En esta tabla de frecuencia de palabras utilizadas en los títulos de los artículos. Contiene cuatro columnas etiquetadas

como ‘index’, ‘Word’, ‘Frequency’ y ‘Rank’. Hay 20 filas, cada una representando una palabra diferente, con la frecuencia correspondiente de cuántas veces aparece la palabra en los títulos de los artículos y su rango basado en esa frecuencia. La primera palabra es “detection” con una frecuencia de 72 y un rango de 1.0, indicando que es la palabra más frecuente en este contexto. La última palabra listada es “detecting” con una frecuencia de 9 y un rango de 13.0. La tabla proporciona una visión de qué términos se utilizan más comúnmente en la materia en cuestión, sugiriendo su importancia o prevalencia en las discusiones o literatura relacionada con este campo.

Index	Word	Frequency	Rank	1/2
0	detection	72	1.0	
1	face	58	2.0	
2	using	35	3.0	
3	recognition	31	4.0	
4	learning	29	5.0	
5	deep	27	6.0	
6	based	24	7.0	
7	system	23	8.0	
8	fraud	21	9.0	
9	spoofing	12	10.0	
10	card	12	10.0	
11	facial	12	10.0	
12	analysis	12	10.0	
13	credit	11	11.0	
14	deepfake	11	11.0	
15	image	11	11.0	
16	machine	10	12.0	
17	network	9	13.0	
18	approach	9	13.0	
19	detecting	9	13.0	

Figura 5. Analizar títulos

La una nube de palabras esta relacionada con la tecnología de reconocimiento facial. Las palabras más prominentes, que son más grandes en tamaño indicando una mayor frecuencia o importancia, son “using”, “face”, “detection” y “system”. Otras palabras notables incluyen “recognition”, “algorithm”, “based” y “biometric”. Esta visualización es interesante ya que resalta conceptos y términos clave asociados con el reconocimiento facial, lo que sugiere que podría usarse para analizar el enfoque de un texto o estudio particular sobre este tema.

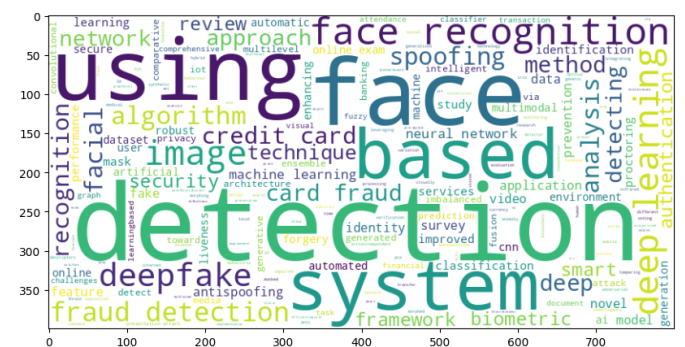


Figura 6. Nube de palabras: Titulos

#### IV-C. Analisis de abstracts

Los artículos presentados ofrecen una visión amplia y diversa del campo del reconocimiento facial, destacando diversas aplicaciones y desafíos. En general, estos documentos muestran cómo las técnicas de aprendizaje profundo, la detección de anomalías y la anonimización de datos pueden mejorar

significativamente los sistemas de reconocimiento facial en términos de seguridad, precisión y privacidad.

La detección de comportamientos anómalos y la vitalidad de rostros son cruciales para prevenir fraudes y suplantaciones de identidad, mientras que la anonimización protege la privacidad de los usuarios, especialmente en entornos gubernamentales y de seguridad. Además, la integración de descriptores de identidad comportamental y la evaluación de algoritmos en rostros falsos proporcionan nuevas vías para mejorar la robustez y fiabilidad de estos sistemas.

También se destaca la aplicación práctica del reconocimiento facial en la prevención del fraude con tarjetas de crédito y la detección de comportamientos sospechosos, lo que demuestra su relevancia en la protección de transacciones financieras y en la detección de identidades falsas en plataformas sociales.

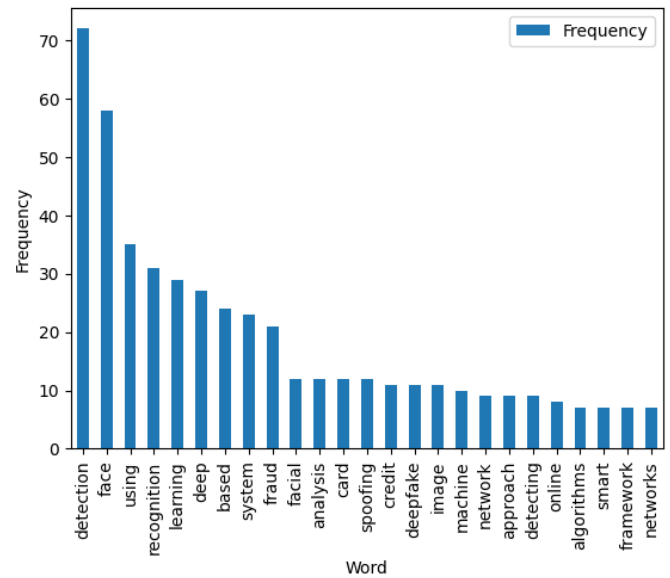


Figura 8. Frecuencia de las palabras clave

Title: An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks  
Summary: Due to its importance in several applications, including fraud and spammer detection, anomaly detection has emerged as a  
Title: Document anonymization for border guards and immigration services  
Summary: The personal information must be well protected and a data breach must be avoided at all times. Anonymization removes th  
Title: Action-Independent Generalized Behavioral Identity Descriptors for Look-alike Recognition in Videos  
Summary: There is a long history of exploitation of the visual similarity of look-alikes for fraud and deception. However, the be  
Title: A Privacy Preserving E-Voting System Based on Blockchain  
Summary: To address these challenges, this paper proposes a blockchain-based e-voting system to ensure the fairness of the electo  
Title: Measuring, characterizing, and detecting facebook like farms  
Summary: Using relevant lexical and non-lexical features, we build a classifier to detect like farms accounts that achieves a pre  
Title: Entropy-based face recognition and spoof detection for security applications  
Summary: Identity spoofing is defined as the action by which a person impersonates a third party to carry out a series of illegal  
Title: Novel Face Liveness Detection Using Fusion of Features and Machine Learning Classifiers  
Summary: © 2020 IEEE. As the technology is growing which is birth to different types of frauds into areas like face detection, fi  
Title: Credit Card Fraud Detection Based on Machine and Deep Learning  
Summary: With the rapid evolution of the technology, the world is turning to use credit cards instead of cash in their daily life  
Title: Credit Card fraud Detection and Prevention by Face Recognition  
Summary: We therefore introduced a new approach to prevent theft during online transactions in order to protect information throu  
Title: Performance of face recognition algorithms on dummy faces  
Summary: The contributions of this paper are: 1) Preparation of dummy face database of 50 subjects 11) Testing of face recognitio

Figura 7. Analisis abstract

#### IV-D. Analisis palabras clave

El gráfico de barras es importante porque proporciona una representación visual de la frecuencia de ciertos términos en un conjunto de datos dado. Los términos representados están relacionados con la tecnología y los datos, como “detection”, “recognition”, “learning”, entre otros. La palabra “detection” es la más frecuente, lo que sugiere que es un tema clave en el contexto de estos datos. Este tipo de análisis puede ser útil para entender las tendencias o las áreas de enfoque dentro de un campo como la ciencia de datos, la tecnología o la investigación.

Este gráfico es interesante ya que proporciona una visión de qué términos se utilizan más comúnmente en la materia en cuestión, sugiriendo su importancia o prevalencia en las discusiones o literatura relacionada con este campo.

Los títulos de los artículos y la cantidad de palabras clave que contienen son:

1. “Checking an authentication of person depends on RFID with thermal image” - 12 palabras clave
2. “Deep Learning Approach for Detecting Fake Images Using Texture Variation Network” - 11 palabras clave
3. “Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks” - 11 palabras clave
4. “Detecting Deepfake Human Face Images Using Transfer Learning: A Comparative Study” - 11 palabras clave
5. “A comprehensive review on face recognition methods and factors affecting facial recognition accuracy” - 11 palabras clave
6. “Detecting handcrafted facial image manipulations and GAN-generated facial images using Shallow-FakefaceNet” - 11 palabras clave
7. “Subscription Fraud Prevention in Telecommunication Using Multimodal Biometric System” - 11 palabras clave
8. “Fraud Detection by Facial Expression Analysis Using Intel RealSense and Augmented Reality” - 11 palabras clave
9. “Loan Fraud Users Detection in Online Lending Leveraging Multiple Data Views” - 11 palabras clave
10. “Efficiency analysis of genetic algorithm and genetic programming in data mining and image processing” - 11 palabras clave

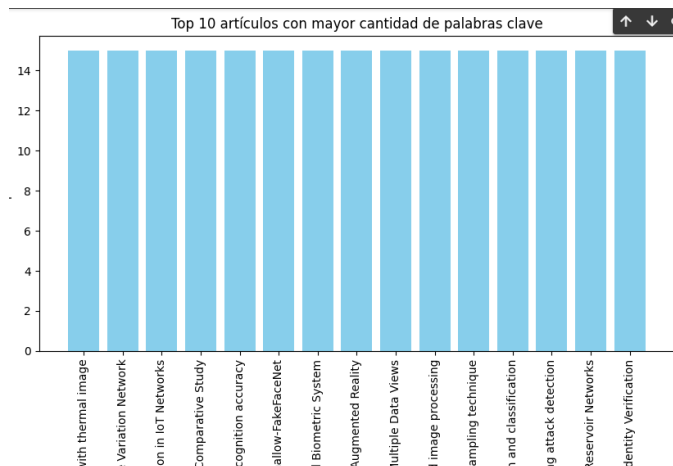


Figura 9. Artículos con mas palabras clave

#### IV-E. Analisis de autores

La lista de autores muestra colaboración entre varios investigadores, posiblemente de diferentes instituciones o disciplinas. La interdisciplinariedad es crucial en campos como el reconocimiento facial, que combina aspectos de inteligencia artificial, seguridad, privacidad, y biometría.

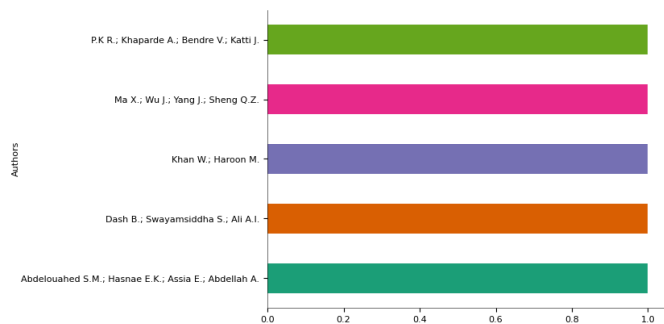


Figura 10. Autores relevantes

El gráfico sugiere una comunidad de investigación activa y colaborativa en el campo del reconocimiento facial, con varios autores contribuyendo de manera significativa. Esto es alentador para el desarrollo continuo y la innovación en esta área tecnológica, abarcando desde mejoras en la precisión de los algoritmos hasta la implementación de medidas de seguridad y privacidad.

#### V. CONCLUSIONES

El uso de herramientas tecnológicas para graficar los datos que no podemos llegar a ver en nuestra totalidad nos permite llenarnos de una idea completa de los documentos, facilitándonos el entendimiento y agilizando el proceso de albergación de información.

[1]. [2]. [3]

#### REFERENCIAS

- [1] M. H. Wasim Khan, "An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks," *International Journal of Cognitive Computing in Engineering*, vol. 3, no. 1, pp. 153 – 160, 2022.
- [2] H. Bouma, R. Pruim, A. V. Rooijen, J.-M. ten Hove, J. van Mil, and B. Kromhout, "Document anonymization for border guards and immigration services," in *Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies IV*, H. Bouma, R. Prabhu, R. J. Stokes, and Y. Yitzhaky, Eds., vol. 11542, International Society for Optics and Photonics. SPIE, 2020, p. 115420C. [Online]. Available: <https://doi.org/10.1117/12.2571944>
- [3] A. Khodabakhsh and H. Loisel, "Action-independent generalized behavioral identity descriptors for look-alike recognition in videos," in *2020 International Conference of the Biometrics Special Interest Group (BIO-SIG)*, 2020, pp. 1–6.