Letter

JIM
ISSN: 2183-0606
(CC BY 4.0)

Vol. 13, 2 (2025)
p. XVI-XXV

A Machine Learning Framework for Forgery Detection in Digital ID Documents

Kais Dai[1], Jesús Alonso[2], and Javier Gutiérrez-Meana[3]

[1]Tree Technology S.A., C. San Francisco, 2, 33003 Oviedo, Asturias, Spain | *kais.dai@treelogic.com*
[2]Tree Technology S.A., C. San Francisco, 2, 33003 Oviedo, Asturias, Spain | *jesus.alonso@treelogic.com*
[3]Tree Technology S.A., C. San Francisco, 2, 33003 Oviedo, Asturias, Spain | *javier.gutierrez@treetk.com*

Abstract

This paper introduces an innovative document verification system that leverages artificial intelligence techniques to simplify the onboarding process of electronic identity solutions. The system uses images of identity documents captured via smartphones to identify and detect any potential manipulation or alterations present within the documents. It addresses the wide variety of document types and versions, and the variability in image quality due to different smartphone cameras and lighting conditions. The technological stack used for identity document verification includes optical character recognition (OCR) libraries, machine-readable zone (MRZ) check, image key-points for copy-move forgery detection, and advanced machine learning algorithms for character manipulation detection. The paper also describes the dataset used for training and validation, consisting of genuine identity documents and simulated forged documents. The verification module includes an image quality check, a copy-move forgery detection, an imitation forgery detector, and a global forgery scoring endpoint. This system provides a comprehensive approach for real-time verification of valid identity documents, which has been tested across five European countries, offering a transparent and secure framework to detect forged identity documents.

Keywords: electronic ID, ID documents, forgery detection, machine learning, copy-move forgery, imitation forgery.

Cite paper as: Dai, K., Alonso, J., Gutiérrez-Meana, J., (2025). A Machine Learning Framework for Forgery Detection in Digital ID Documents - Letter, *Journal of Innovation Management*, 13(2), XVI-XXV.; DOI: https://doi.org/10.24840/2183-0606_013.002_L003

1 Introduction

The work presented in this paper was developed as part of the IMPULSE project (Impact of Blockchain and Artificial Intelligence to Improve Electronic Identities), which aims to provide an electronic identity (eID) solution based on disruptive technologies, with a focus, among other aspects, on simplicity and ease of adoption. Following this philosophy, the onboarding process that will lead to the generation of the eID avoids time-consuming paperwork and only requires the capture of pictures/video of the users and their physical Identity (ID) cards/passports by means of their smartphones. The main concern of this approach, especially considering that only photos of the selected ID documents will be provided – and not the ID cards themselves – is the risk of document manipulation, which makes validation and forgery detection essential.

When proof of identity became mandatory to conduct administrative proceedings, the need for forgery detection on ID documents appeared. The first detection methods, relying on document experts' knowledge with no automatic aid (Centeno et al., 2019), were prone to failure and it was relatively easy to bypass controls. With the appearance of Computer Vision (CV) and

Machine Learning (ML) techniques, algorithms of ever-growing sophistication have become key for the differentiation between tampered and genuine documents. The improved methodology and technological advancements have led to a cat-and-mouse game being played between authorities – implementing more effective security measures – and counterfeiters – taking advantage of the newest developments for their own interest. Therefore, forgery detection is still a hot topic nowadays to prevent crime while avoiding the potential harm to citizens and strengthening the global economy. Thankfully, cutting-edge Artificial Intelligence (AI) techniques provide a toolset to make these detections more accurate than ever.

Despite these improvements, the implementation of ID document verification systems within the European Union and European Free Trade Association is neither easy nor straightforward. One of the main challenges consists in the broad range of coexisting document types and versions (European Council, 2024). To begin with, some countries issue national ID cards, whereas others do not and rely on the use of passports, driving licenses or digital certificates for the same purpose. Moreover, apart from the fact that designs and layouts are different for each nationality, in most cases they have been updated every few years, incorporating the latest security measures. Consequently, a significant number of citizens own legacy, but still valid, versions of their documents. The project for which this document verification module has been developed, with its 6 case studies in 5 different European countries, has leveraged the common features of the variations and adapted to their differences.

Another difficulty stems from the device used to capture the document pictures. The smartphone ecosystem has grown into a vast landscape of manufacturers, vendors, brands, models, generations and operating system versions. Accordingly, smartphone cameras have highly heterogeneous features, offering different resolutions, lenses, sensors and technologies. To these hardware-related issues we need to add the variations in illumination of the locations where the pictures are taken. The result is a considerable variability in image color, sharpness, document positioning and metadata, which must be treated with digital image processing techniques.

2 Related Work

Despite extensive research in image forensics (Gill, Garg & Doegar, 2017), the focus on detecting forgeries within images of identification documents (Gayer, Ershova & Arlazarov, 2023) remains limited. However, advancements in this niche area are gaining traction due to the critical importance of ensuring the integrity and authenticity of identity documents.

One promising development is in the detection of copy-move forgery (Verma et al., 2024), a specific type of image tampering where a part of the image is copied and pasted on another part. In the context of ID documents, this forgery technique may be used to alter the image by reproducing some characters and respecting the utilized fonts and size. Hence, the objective of this verification process is to detect similar regions of the same image. Several copy-move forgery detection (CMFD) techniques have been employed in the current research. (Chen, Yan & Lyu, 2020) relied on extracting distinctive features from the image, such as key-points or texture descriptors, and matching them to detect regions that exhibit similarity indicative of copy-move forgery. In (Gurunlu & Ozturk, 2022), a block-based method involved partitioning the image into blocks of pixels and comparing them to identify duplicated blocks. Various similarity metrics, such as correlation coefficients or Euclidean distances, were utilized to assess the resemblance between blocks and detect instances of forgery. Furthermore, in (Zare Mehrjardi et al., 2023), a hybrid approach combining both feature-based and block-based methods was proposed. A genetic

algorithm identifies suspected forgery blocks using matched keypoints as the fitness function, followed by simulated annealing to refine the detection of accurate forgery blocks.

Another significant method for manipulating ID documents is imitation or insertion forgery. This involves replicating the font, size, color, and other morphological characteristics of the text on ID documents to introduce fake or manipulated data. Due to the available means, imitation forgery is always imperfect, leaving deviations in size, skewness and rotation with respect to the official text. This forgery detection method aims to detect traces left by the tampering process, thus obtaining evidence that the ID document is not legitimate. Similarly, (Greiner & Tuba, 2023) introduces forgery detection classifiers, comprising both size-dependent and size-independent models, leveraging support vector machine (SVM) techniques to determine if the document is forged or not. These models utilize features such as local binary pattern (LBP), kurtosis, and skewness of pixel values. Additionally, (Ranjan et al., 2018) outlines a comprehensive methodology for detecting imitation forgeries in digital images. This approach entails enhancing image quality through histogram equalization, noise reduction via median filtering, and image segmentation using K-means clustering. Feature extraction employs the Gray Level Co-occurrence Matrix (GLCM) for texture analysis, followed by training two models: initially, a linear kernel SVM, succeeded by an Artificial Neural Network (ANN) which demonstrated superior performance.

In the context of ID documents, a high importance is given to the Machine-readable-zone (MRZ) field. The latter encapsulates personal data and represents a security code which is included in all ID documents. The MRZ code needs to follow the specifications and minimum-security standards set out in International Civil Aviation Organization (ICAO) document number 9303 (International Civil Aviation Organization, 2021). Once read, the MRZ code is translated into a dictionary with all relevant information available on the ID document (ID card or passport). This information is used to verify the format and structure of the extracted data to ensure it adheres to the standards set for MRZ encoding, such as ISO/IEC 7501 (International Organization for Standardization, 2008). Subsequently, perform checksum validation on key fields within the MRZ, such as the document number and the date of birth, by applying algorithms specified in international standards. Further verifications may be conducted based on the specific document type and the regulations of the issuing country.

3 Technological Stack

The objective of this paper is to present the ID documents verification service. This verification module allows to assess whether a photograph of an ID document sent by a user corresponds to a genuine document (in other words, it has not been forged) and effectively belongs to that user, in the framework of the onboarding process.

The ID document verification module uses state-of-the-art optical character recognition (OCR) libraries, based on Long Short-Term Memory (LSTM) neural networks (https://tesseract-ocr.github.io/) (Jaided AI, 2024). OCR is the conversion of the text shown in images into machine-encoded characters. In this context, OCR is used to compare the information contained in the ID documents to the one provided by the users and to locate characters on the document pictures.

Other pieces of the technological stack are worth commenting on as well (Figure 1). The machine-readable zone (MRZ) follows a standardized format for verification by authorities. Specialized software extracts and compares it to other document information. Furthermore, different features are considered to compare intra-documents similarities at pixel and character levels. In this context, image key-points detect copy-move forgeries (textual areas of the pictures copied and pasted in a different location). Last, but not least, advanced ML algorithms are deployed to detect

manipulation of characters. The resulting models depart from the morphology of characters read by OCR to detect outliers. This module returns a forgery probability and highlights suspicious regions within the image. It acts as a security barrier against counterfeiters, ensuring only genuine ID holders can proceed with the eID mobile app onboarding. This state-of-the-art, AI-based technological stack will allow this eID service to provide an onboarding process that is at the same time simple, fast, secure, compliant with the General Data Protection Regulation (GDPR) (https://gdpr-info.eu/) and transparent for users, but robust in the background and heavily resilient against attempts of citizens with suspicious intentions to sign up using fake or false IDs.

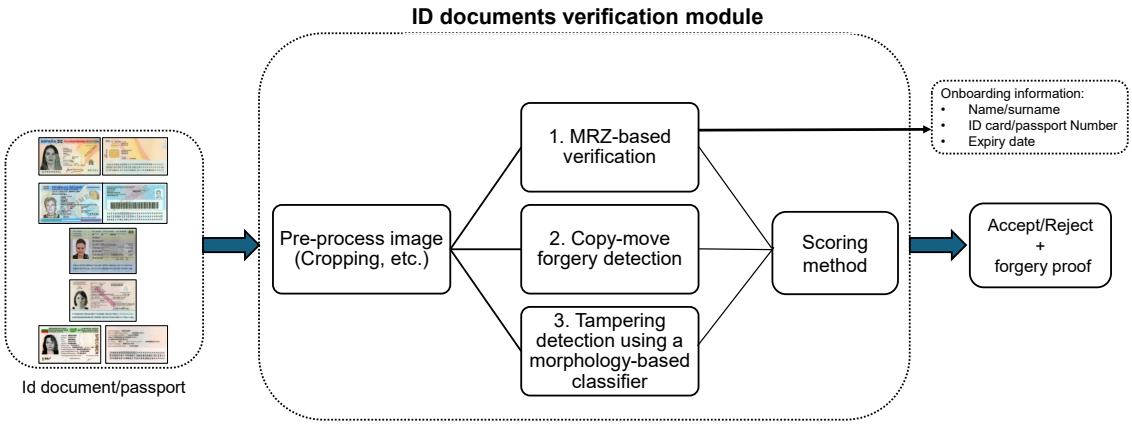

Figure 1. ID documents forgery detection pipeline.

4 Dataset

The dataset used to train and evaluate the forgery detection models is composed of images of real ID documents, 72 ID cards (front and back side photographs) and 32 passports (only photographs of the bio-data page) that were kindly provided by volunteer members of the project consortium (in Spain, Iceland, Denmark, Bulgaria and Italy). This was made with all the guarantees for privacy of their personal information, in accordance with the applicable regulation (as in GDPR) and after having signed an informed consent.

The dataset of images of ID documents described above is only composed of real, valid ID documents. Thus, it contains no image of tampered or forged documents used for unauthorized purposes. To fill this gap, we developed a generator of simulated forged ID documents, to serve as positive forgery examples in the validation of the forgery detection models. This simulator can perform operations of resizing, moving, rotating, copy-moving and inserting characters into images of genuine ID documents.

5 Forgery Detection Modules

The verification module is equipped with an image quality check endpoint which plays a crucial role in verifying the quality of ID document photographs. By employing detectors for blurry images, dark images, and high reflections of holograms, it tests whether the provided image meets

the necessary quality standards. Depending on the results, appropriate Application Programming Interface (API) call responses guide users to either proceed or upload a new photo.

Copy-move forgery detection identifies regions within ID document images that have been copied and pasted. By employing Scale-Invariant Feature Transforms (SIFT) -based key point extraction (Teerakanok & Uehara, 2019) and Density-Based Clustering (DBSCAN) (Campello et al., 2020; Kriegel et al., 2011), potential tampering pairs are identified. The forgery proof image highlights the locations of copy-move forger. Regions where elements have been duplicated or manipulated within the same image, are marked using lines or other visual indicators. By providing visual evidence of potential tampering, public administration representatives may gain a deeper understanding of the specific areas that raise concern. The copy-move forgery detection also provides a score later aggregated into the global forgery score.

An example of the forgery proof image is depicted in Figure 2. A copy-move forgery has been detected using our verification tool. The red line indicates both source (number *5* copied from field *validez* which stands for the expiry date in the Spanish specimen of the ID card) and destination of the tampering.

Figure 2. Forgery proof image

The imitation forgery detector locates text which has been tampered by imitating the characteristics (font, color, position, etc.) of the original text of the ID document (Bertrand et al., 2013). The detector works by applying OCR to extract the sub-image of every character in the document and carefully crafting features from it (such as size, color, skewness and alignment), together with the nationality and the document type (ID document or passport). Then, a one-class Support Vector Machine (SVM) classifier (Chen, Zhou & Huang, 2001), trained on all the character features extracted from our dataset, is applied, detecting every character that deviates enough from the ones in the training set to constitute a forgery suspicion. A forgery proof image is also returned. It encloses these suspicious regions within rectangles, making them easily distinguishable.

The global forgery scoring module integrates results from MRZ-based, copy-move, and morphology detectors, using adaptive thresholds per nationality to evaluate document authenticity. This initial version averages scores from these detectors and face recognition, considering both sides of ID documents. Future development aims to optimize weight assignments for each method via gradient descent, minimizing binary classification errors across a dataset of five ID document types.

6 Results and Conclusion

By providing the public administration representatives with a proof image that highlights suspicious elements, we empower them to verify the authenticity of the ID documents and make informed decisions. It ensures that the system's decisions are not perceived as arbitrary or opaque, but rather because of a comprehensive analysis of potential tampering indicators.

The evaluation was conducted using a dataset of 103 genuine ID documents, including ID cards from Spain (52), Bulgaria (15), and Italy (4), as well as passports from Iceland (22) and Denmark (10). Since ID cards contain both a front and back side, the dataset includes 174 genuine images, with 142 images from ID cards (71 front-side and 71 back-side) and 32 images from passports (one biodata page per passport). To assess the system's performance, a forgery simulation module generated manipulated versions of these genuine images, resulting in 348 forged images across different forgery types. Two types of forgeries were simulated: copy-move forgery and morphology-based forgery. These transformations introduced realistic variations that closely resemble real-world forgery techniques, increasing the complexity of the detection task.

Accuracy results corresponding to each forgery detection technique are depicted in Table 1.

Table 1. Test data and Accuracy results.

Forgery Detection Technique	Test Data	Accuracy
Copy-Move Forgery Detection	348 images (174 genuine + 174 forged)	92%
Morphology Forgery Detection	209 images (35 genuine + 174 forged)	89.04%
MRZ Detection & Reading Module	103 images (back-side ID cards + passport biodata)	98.41%

For copy-move forgery detection, the system was tested on 348 images, comprising 174 genuine images and 174 forged images, where the forged images were generated by modifying both the front and back sides of ID cards as well as the biodata pages of passports. The module achieved an accuracy of 92%, demonstrating its ability to detect localized character manipulations effectively.

For morphology forgery detection, the model was trained using 80% of the 174 genuine images (i.e., 139 images) with a one-class SVM approach for anomaly detection. The testing phase was conducted on the remaining 20% of the genuine images (i.e., 35 images) along with 174 forged images generated by the morphology forgery simulator, leading to a total of 209 test images. The system achieved an accuracy of 89.04%, successfully identifying document modifications involving character shape, size, and brightness alterations.

Additionally, the MRZ detection and reading module, evaluated on 103 images (71 back-side ID card images and 32 passport biodata pages), achieved an overall accuracy of 98.41%, ensuring reliable verification of machine-readable zones across different document types. These results underscore the improved effectiveness of the system in detecting document forgery across both ID cards and passports.

The high accuracy of the MRZ-related module highlights its reliability, while the refinements in the copy-move detection technique enhance the system's ability to detect localized manipulations. The morphology detection module further strengthens the system's capacity to identify more complex forgeries. By achieving consistently high detection rates across different document structures and forgery types, the system demonstrates its adaptability and robustness in real-world scenarios.

A major limitation of this study is the absence of publicly available datasets specifically designed for ID document forgery detection. This restricts the ability to conduct direct benchmarking

and comparative evaluations, as general-purpose forgery datasets do not adequately represent the distinct features and complexities of ID documents. Moreover, the generation of synthetic datasets, while helpful for training, cannot fully replicate the complexity of real-world forgery cases. This limitation underscores the need for future collaborative efforts to establish shared datasets and evaluation protocols specific to this application. Additionally, the reliance on MRZ validation as part of the verification stack further complicates comparative analysis. The MRZ module is specialized for ID document verification and cannot be readily applied to other forgery detection use cases. This specialization, while enhancing the system's capability to detect ID-specific forgeries, limits its direct comparability with general forgery detection systems.

A holistic approach for the automatic and real-time verification of valid ID documents has been developed for six different European countries as part of the onboarding process of this innovative eID solution. It relies on state-of-the-art AI techniques and provides a transparent and secure framework to detect forged ID documents.

The ongoing work, yet to be validated, focuses on the integration of statistical-based methodologies to augment the forgery detector capabilities. This integration encompasses several techniques, including JPEG Compression Analysis (Wang et al., 2022), which investigates the influence of JPEG compression artifacts on forgery detection. Error Level Analysis (ELA) (Chandana et al., 2024) is also being explored to discern the inconsistencies in error levels induced during image manipulation.

Our future research trajectory will also extend to encompass advancements in detecting image splicing (Meena & Tyagi, 2021), further enhancing the detector's capability to identify various forms of image manipulation and forgery. Furthermore, future work will explore the use of federated learning (KhoKhar et al., 2022) to address privacy concerns while enhancing the system's capabilities. This approach allows decentralized training of models using real ID cards without the need to store or share sensitive data centrally. Federated learning enables devices to compute model updates locally, with only these updates transmitted to the central system and being aggregated there. By ensuring that personal data remains on users' devices, this privacy-preserving methodology complies with regulations such as GDPR while leveraging authentic ID documents to improve detection performance. Implementing this framework could significantly advance the system's accuracy and robustness without compromising user privacy.

Acknowledgement

This work received funding from the European Union's Horizon 2020 research and innovation programme under the IMPULSE project (grant agreement No 101004459).

7 References

Bertrand, R., Gomez-Krämer, P., Terrades, O. R., Franco, P., & Ogier, J. M. (2013, August). A system based on intrinsic features for fraudulent document detection. In *2013 12th International conference on document analysis and recognition* (pp. 106-110). IEEE. https://doi.org/10.1109/ICDAR.2013.29

Chandana, S., Nagarathna, C. R., Amrutha, A., & Jayasri, A. (2024, January). Detection Of Image Forgery Using Error Level Analysis. In *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)* (pp. 1-5). IEEE. https://doi.org/10.1109/IITCEE59897.2024.10467523

Campello, R. J., Kröger, P., Sander, J., & Zimek, A. (2020). Density-based clustering. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10*(2), e1343. https://doi.org/10.1002/widm.1343

Centeno, A. B., Terrades, O. R., Canet, J. L., & Morales, C. C. (2019). Identity Document and banknote security forensics: a survey. *arXiv preprint arXiv:1910.08993*. https://doi.org/10.48550/arXiv.1910.08993

Chen, H., Yang, X., & Lyu, Y. (2020). Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm. *IEEE Access*, *8*, 36863-36875. https://doi.org/10.1109/ACCESS.2020.2974804

Chen, Y., Zhou, X. S., & Huang, T. S. (2001, October). One-class SVM for learning in image retrieval. In *Proceedings 2001 international conference on image processing (Cat. No. 01CH37205)* (Vol. 1, pp. 34-37). IEEE. https://doi.org/10.1109/ICIP.2001.958946

European Council. (2024). PRADO - Public Register of Authentic Identity and Travel Documents Online. Retrieved from https://www.consilium.europa.eu/prado/en/prado-start-page.html

Gayer, A., Ershova, D., & Arlazarov, V. V. (2023). An accurate approach to real-time machine-readable zone detection with mobile devices. *International Journal on Document Analysis and Recognition (IJDAR)*, *26*(3), 321-334. https://doi.org/10.1007/s10032-023-00435-w

Gurunlu, B., & Ozturk, S. (2022). Efficient approach for block-based copy-move forgery detection. In *Smart Trends in Computing and Communications: Proceedings of SmartCom 2021* (pp. 167-174). Springer Singapore. https://doi.org/10.1007/978-981-16-4016-2_16

Gill, N. K., Garg, R., & Doegar, E. A. (2017, July). A review paper on digital image forgery detection techniques. In *2017 8th International conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICCCNT.2017.8203904

Greiner, G., & Tuba, E. (2023, November). Detecting Image Forgery Using Support Vector Machine and Texture Features. In *International Conference on Intelligent Data Engineering and Automated Learning* (pp. 529-537). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-48232-8_48

International Civil Aviation Organization. (2021). Doc 9303: Machine Readable Travel Documents, Part 1: Introduction (8th ed.). Retrieved from https://www.icao.int/publications/Documents/9303_p1_cons_en.pdf

International Organization for Standardization. (2008). ISO/IEC 7501-1:2008: Identification cards — Machine readable travel documents — Part 1: Machine readable passport. Retrieved from https://www.iso.org/standard/45562.html

Jaided AI. (2024, September 24). EasyOCR (Version 1.7.2) [Computer software]. https://www.jaided.ai/easyocr/

Kriegel, H. P., Kröger, P., Sander, J., & Zimek, A. (2011). Density-based clustering. *Wiley interdisciplinary reviews: data mining and knowledge discovery*, *1*(3), 231-240. https://doi.org/10.1002/widm.30

Meena, K. B., & Tyagi, V. (2021). Image splicing forgery detection techniques: A review. In *Advances in Computing and Data Sciences: 5th International Conference, ICACDS 2021, Nashik, India, April 23–24, 2021, Revised Selected Papers, Part II 5* (pp. 364-388). Springer International Publishing. https://doi.org/10.1007/978-3-030-88244-0_35

Ranjan, S., Garhwal, P., Bhan, A., Arora, M., & Mehra, A. (2018, May). Framework for image forgery detection and classification using machine learning. In *2018 2nd international conference on trends in electronics and informatics (ICOEI)* (pp. 1-9). IEEE. https://doi.org/10.1109/ICOEI.2018.8553924

Teerakanok, S., & Uehara, T. (2019). Copy-move forgery detection: A state-of-the-art technical review and analysis. *IEEE Access*, *7*, 40550-40568. https://doi.org/10.1109/ACCESS.2019.2907316

Verma, M., & Singh, D. (2024). Survey on image copy-move forgery detection. *Multimedia Tools and Applications*, *83*(8), 23761-23797. https://doi.org/10.1007/s11042-023-16455-x

Wang, M., Fu, X., Liu, J., & Zha, Z. J. (2022, October). Jpeg compression-aware image forgery localization. In *Proceedings of the 30th ACM International Conference on Multimedia* (pp. 5871-5879). https://doi.org/10.1145/3503161.354774

Zare Mehrjardi, F., Latif, A., & Sardari Zarchi, M. (2023). An Optimal Hybrid Method to Detect Copy-move Forgery. *Journal of AI and Data Mining*, *11*(3), 429-442. https://doi.org/10.22044/jadm.2023.13166.2453

KhoKhar, F. A., Shah, J. H., Khan, M. A., Sharif, M., Tariq, U., & Kadry, S. (2022). A review on federated learning towards image processing. *Computers and Electrical Engineering*, *99*, 107818. https://doi.org/10.1016/j.compeleceng.2022.107818

Biographies

Kais Dai. Dr. Kais Dai earned his Ph.D. in Information and Communication Technology from the University of Vigo (Spain) and is currently a Senior Data Scientist at Tree Technology. He has over 15 years of experience in artificial intelligence and machine learning, with expertise spanning predictive modelling, natural language processing, generative models, and optimisation using operational research. At Tree Technology, he designs and deploys end-to-end AI/ML solutions across various domains. Kais has served as technical lead in numerous national and European R&D initiatives, including IMPULSE (AI-based identity-document verification for digital identity) and PRELUDE (Prescient building operation utilising real-time data for energy dynamic optimisation), among others. He has also published several papers in international peer-reviewed conferences and journals.
ORCID: *https://orcid.org/0000-0003-3570-2769*
CRediT Statement: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Supervision, Ressources, Validation, Visualization, Writing – original draft, Writing – review & editing.

Jesús Alonso. Jesús Alonso earned an M.Sc. in Mathematics from the University of Alicante and an M.Sc. in Artificial Intelligence from the Technical University of Valencia. He is Head of Artificial Intelligence at Tree Technology, where he shapes the company's AI research agenda and leads the development of trustworthy AI solutions spanning machine learning and deep learning, NLP and generative models. Jesús has participated in several Horizon 2020 and Horizon Europe projects, including TRUST aWARE (privacy-enhancing NLP for software users), IMPULSE (AI-based identity-document verification for digital identity), AI-ARC (satellite-image analysis for iceberg detection) and CARAMEL (predictive modelling of cardiovascular-disease risk in menopausal women), serving as technical lead in some of them.
ORCID: *https://orcid.org/0000-0002-2678-0426*
CRediT Statement: Data curation, Formal analysis, Investigation, Methodology, Resources, Software, Validation, Writing - original draft.

Javier Gutiérrez-Meana. Dr. Javier Gutiérrez Meana (male) received his Telecommunication Engineering and PhD degree from the University of Oviedo in 2005 and 2010 respectively. As PhD candidate and R&D Engineer he participated in several R&D projects, being the author/co-author of multiple papers in peer-reviewed magazines and conferences. He worked as R&D Project Manager with a focus on EU programmes. Since 2020, he is R&D Manager at Tree Technology, where his activities include project management and elaboration of proposals in the field of ICT at national and international level. He was involved in many FP7, Eurostars-Eureka and Horizon 2020 projects, including IMPULSE (grant no. 101004459) and TRUST aWARE (grant no. 101021377) as Project Coordinator.
ORCID: *https://orcid.org/0009-0008-1091-1736*
CRediT Statement: Resources, Writing – Review & Editing, Supervision, Project administration, Funding acquisition.