University “St. Kliment Ohridski”
Bitola
Faculty of Information and
Communication Technology - Bitola
Republic of North Macedonia

PROCEEDINGS
15th International Conference on
APPLIED INTERNET AND INFORMATION TECHNOLOGIES
AIIT 2025

AIIT International Conference

Bitola, November 7, 2025

University “St. Kliment Ohridski” Bitola
Faculty of Information and Communication Technology - Bitola
Republic of North Macedonia

PROCEEDINGS
15th International Conference on
APPLIED INTERNET AND INFORMATION TECHNOLOGIES

AIIT 2025

November 7, 2025 Bitola

Proceedings publisher and organizer of the conference:
University "St. Kliment Ohridski", Bitola, Faculty of Information and Communication Technology – Bitola, Republic of North Macedonia

For publisher:
Blagoj Ristevski, PhD, Full Professor, Dean of the
Faculty of Information and Communication Technologies,
University "St. Kliment Ohridski", Bitola, North Macedonia

Proceedings editors:
Kostandina Veljanovska, PhD
Željko Stojanov, PhD

Conference Chairmans:
Blagoj Ristevski, University "St. Kliment Ohridski", Faculty of Information and Communication Technologies, Bitola, Republic of N. Macedonia – chair
Kostandina Veljanovska, University "St. Kliment Ohridski", Faculty of Information and Communication Technologies, Bitola, Republic of N. Macedonia – co-chair
Željko Stojanov, University of Novi Sad, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia – co-chair

Technical preparation of the proceedings:

Kostandina Veljanovska, PhD
Marija Apostoloska Kondoska, MSc
Darko Pajkovski, MSc

Cover design:
Kostandina Veljanovska, PhD
Hristina Dimova Popovska, MSc

e-Proceedings
ISBN 978-608-5003-06-8

CIP - Каталогизација во публикација

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

004-049.8(062)

INTERNATIONAL conference on applied internet and information technologies AIIT 2025 (15 ; 2025 ; Bitola, Republic of North Macedonia)
Proceedings / 15th International conference on applied internet and information technologies AIIT 2025, November 7 2025, Bitola, Republic of North Macedonia ; [editors Kostandina Veljanovska, Zeljko Stojanov]. - Bitola : University "St. Kliment Ohridski", Bitola Faculty of information and communication technologies, 2025. - 477 стр. : илустр. ; 30 см
Библиографија кон трудовите
ISBN 978-608-5003-06-8

а) Информатичка технологија -- Примена -- Собири
COBISS.MK-ID 67608325

Introduction

As organizing partners of 15th International Conference on Applied Internet and Information Technologies AIIT 2025, we warmly welcome all participants, researchers, and colleagues joining us from various countries and universities, united by our shared commitment to advancing knowledge in the fields of computer science, applied Internet, and information technologies.

The AIIT conference has become a long-standing tradition of excellence and collaboration, co-organized by the Faculty of Information and Communication Technologies – Bitola, University "St. Kliment Ohridski," and the Technical Faculty "Mihajlo Pupin" – Zrenjanin, University of Novi Sad, Serbia. Over the past fifteen years, this partnership has fostered not only strong academic cooperation but also genuine friendship among our institutions and scholars.

This year's conference proudly continues that tradition, bringing together innovative research, diverse perspectives, and new insights into technologies that are shaping our digital future. The Scientific Program Committee once again faced the demanding task of selecting the highest-quality papers from more than sixty submissions spanning a wide range of topics—including Artificial Intelligence, Immersive Technologies, Mathematical Simulations, Data Science and Big Data Analytics, Knowledge and IT Management, Cybersecurity, Software Engineering, Data Mining, Digital Transformation, Behavioral Economics and Business, Social Engineering, Digital Humanities, Augmented Humanity, and Hybrid Intelligence. This ensures that the program reflects both scientific rigor and creative originality.

We would like to express our sincere gratitude to all reviewers for their dedicated work, as well as to the members of the Organizing Committee for their professionalism, commitment, and enthusiasm in preparing this event.

We are confident that these proceedings will provide an enriching and thought-provoking reading experience.

Conference chairs:

Blagoj Ristevski, University "St. Kliment Ohridski", Faculty of Information and Communication Technologies, Bitola, Republic of N. Macedonia (chair)

Kostandina Veljanovska, University "St. Kliment Ohridski", Faculty of Information and Communication Technologies, Bitola, Republic of N. Macedonia (co - chair)

Željko Stojanov, University of Novi Sad, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia (co – chair)

MAIN ORGANIZERS:

Faculty of Information and Communication Technologies - Bitola
University "St. Kliment Ohridski" University - Bitola
NORTH MACEDONIA
http://fikt.uklo.edu.mk/

Technical Faculty "Mihajlo Pupin" Zrenjanin
University of Novi Sad SERBIA
http://www.tfzr.uns.ac.rs/

ORGANIZATION PARTNERS:

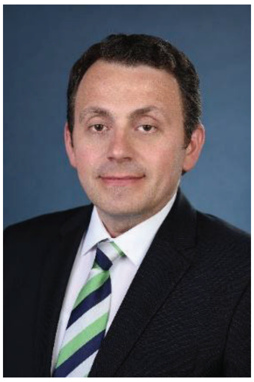
Faculty of Computer Science
Irkutsk National Research Technical University
Institute of Informational Technologies and Data Analysis
Irkutsk, RUSSIA
http://www.istu.edu/

Matrosov Institute for System Dynamics and Control Theory of Siberian Branch of Russian Academy of Sciences, Irkutsk, RUSSIA
http://idstu.irk.ru/

Irkutsk State Transport University (IrGUPS)
Irkutsk, RUSSIA
https://www.irgups.ru/

Faculty of Engineering South-west
University "Neophyte Rilsky"-Blagoevgrad
BULGARIA
http://www.swu.bg/

Conference Chairs



Blagoj Ristevski, University "St. Kliment Ohridski", Faculty of Information and Communication Technologies, Bitola, Republic of N. Macedonia (chair)

Prof. Dr. Blagoj Ristevski is a Full Professor at the Faculty of Information and Communication Technologies (FICT) at the University "St. Kliment Ohridski" - Bitola, where he currently serves as Dean. He holds a PhD in Technical Sciences from the Faculty of Electrical Engineering and Information Technologies, Institute of Computer Science and Informatics, at Ss. Cyril and Methodius University in Skopje. His research interests span Databases, Data Science, Data Mining, Big Data Analytics, Bioinformatics, Computer Graphics, and Cybersecurity. Prof. Ristevski has supervised numerous BSc, MSc, and PhD theses and has led several international research projects. He has served on the management committees of multiple COST actions, reviewed for numerous high-impact journals, and evaluated project proposals for the Horizon 2020 and Horizon Europe programs. Prof. Ristevski is also a senior member of IEEE.

Kostandina Veljanovska, University "St. Kliment Ohridski", Faculty of Information and Communication Technologies, Bitola, Republic of N. Macedonia (co – chair)

Kostandina Veljanovska, Ph.D. completed her education at the University "Sts. Kiril i Metodi", Skopje (BSc in Computer Science), at the University of Toronto, Toronto (MASc in Applied Engineering) and got her MSc and also her PhD in Technical Sciences at the University "St. Kliment Ohridski", Bitola, R. Macedonia. She has completed postdoc in Artificial Intelligence at the Laboratory of Informatics, Robotics and Microelectronics at the University of Montpellier, Montpellier, France. She worked as a Research assistant at the Faculty of Applied Science, University of Toronto, Canada. She also, worked at research team for Constraints, Learning and Agents at LIRMM, University of Montpellier. Currently, she works as a Full Professor in Artificial Intelligence and Systems, Computer Science and Computer Engineering at the Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" - Bitola and serves as a Vice-dean for Science and Collaboration. Her research work is focused on artificial intelligence, machine learning techniques, intelligent systems and human - computer interaction. She participated in several international and domestic scientific projects. She has published numerous scientific papers in the area of interest, as well as several monographic items. She is a reviewing referee for well-known publishing house, journals with significant impact factor in science and also, member of editorial board of several international conferences.

Željko Stojanov, University of Novi Sad, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia (co – chair)

Željko Stojanov, Ph.D. received PhD degree in Computer science and applied informatics at University of Novi Sad, Serbia. He works as a full professor at University of Novi Sad, Technical Faculty "Mihajlo Pupin" Zrenjanin, Serbia. His research interests are in the fields of software engineering, software architecture, software life cycle, business informatics, learning and knowledge management, engineering education, and human aspects of software engineering. He is author of scientific papers published in refereed journals and in the proceedings of international conferences. He participated in several research and industrial projects at national and international levels. He has over fifteen years of experience working with small software companies as a consultant in the fields of software development, software maintenance and software process improvement.

Organizing Committee

Chairs

Kostandina Veljanovska (President), Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Željko Stojanov, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia (vice-president)

Members

Blagoj Ristevski, Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Ivana Berković, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Višnja Ognjenović, Technical Faculty "Mihajlo Pupin" Zrenjanin, Serbia
Eleonora Brtka, Technical Faculty "Mihajlo Pupin" Zrenjanin, Serbia
Dalibor Dobrilovic, Technical Faculty "Mihajlo Pupin" Zrenjanin, Serbia
Dragica Radosav, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Biljana Radulovic, Technical Faculty "Mihajlo Pupin" Zrenjanin, Serbia
Božidar Milenkovski, Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Ljubica Kazi, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Snežana Savoska, Faculty of Information and Communication Technologies - Bitola,N. Macedonia
Vladimir Brtka, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Zoltan Kazi, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Siniša Mihajlović, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Velibor Premčevski, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Nikola Rendevski , Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Aleksandra Stojkov, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Maja Gaborov, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Milica Mazalica, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Igor Vecštejn, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Marko Blažić, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Vuk Amižić, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Natasa Blazeska-Tabakovska, Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Jovana Borovina, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Dalibor Šeljmeši, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Mimoza Bogdanoska Jovanovska, Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Vladimir Šinik, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Nadežda Ljubojev, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Marina Blažeković Toshevski, Faculty of Information and Communication Technologies - Bitola, N. Macedonia
Hristina Dimova Popovska, Faculty of Information and Communication Technologies, University "St.Kliment Ohridski" - Bitola, N. Macedonia
Darko Pajkovski, Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" - Bitola, N. Macedonia
Marija Apostoloska Kondoska, Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" - Bitola, N. Macedonia
Milcho Prisagjanec, Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" - Bitola, N. Macedonia
Ilche Dimovski, Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" - Bitola, N. Macedonia
Zoran Pavlovski, Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" - Bitola, N. Macedonia
Vladimir Karuović, Technical faculty "Mihajlo Pupin", Zrenjanin, Serbia
Evgeny Cherkashin, Institute of System Dynamic and Control Theory SB RAS, Russia
Anastasia Popova, Matrosov Institute for System Dynamics and Control Theory of the Siberian Branch of the Russian Academy of Sciences, Russia
Filip Tsvetanov, South-west University "Neophyte Rilsky", Faculty of Engineering, Blagoevgrad, Bulgaria

Program Committee

Madhusudan Bhatt, R.D. National College, University of Mumbai, India
Amar Kansara, Parth Systems LTD, Navsari, Gujarat, India
Narendra Chotaliya, H. & H.B. Kotak Institute of Science, Rajkot, Gujarat, India
Zeljko Jungic, ETF, University of Banja Luka, Bosnia and Herzegovina
Saso Tamazic, Univerisity of Ljubljana, Slovenia
Marijana Brtka, Centro de Matemática, Computação e Cognição, Universidade Federal do ABC, São Paulo, Brazil
Zoran Cosic, Statheros, Split, Croatia
Istvan Matijevics, Institute of Informatics, University of Szeged, Hungary
Slobodan Lubura, Faculty of electrical engineering, University of East Sarajevo, Bosnia and Herzegovina
Edit Boral, ASA College, New York, NY, USA
Dana Petcu, West University of Timisoara, Romania
Marius Marcu, "Politehnica" University of Timisoara, Romania
Aleksej Stevanov, South-west University "Neophyte Rilsky", Faculty of Engineering, Blagoevgrad, Bulgaria
Petar Apostolov, South-west University "Neophyte Rilsky", Faculty of Engineering, Blagoevgrad, Bulgaria
Filip Tsvetanov, South-west University "Neophyte Rilsky", Faculty of Engineering, Blagoevgrad, Bulgaria
Francesco Flammini, School of Innovation, Design and Engineering, Division of Product Realisation, Mälardalen University, Eskilstuna, Sweden
Deepak Chahal, Jagan Institute of Management Studies (JIMS, Rohini Sector-5), New Delhi, India
Abdel-Badeeh M. Salem, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt
Dragan Peraković, University of Zagreb, Faculty of Transport and Traffic Sciences, Zagreb, Croatia
Gordana Jotanović, University of East Sarajevo, Faculty of Transport and Traffic Engineering, Doboj, Bosnia and Herzegovina
Goran Jauševac, University of East Sarajevo, Faculty of Transport and Traffic Engineering, Doboj, Bosnia and Herzegovina
Dinu Dragan, Faculty of technical Sciences, University of Novi Sad, Serbia
Gururaj Harinahalli Lokesh, Department of IT, Manipal Institute of Technology, Bengaluru, India
Ertuğrul AKBAŞ, Esenyurt University, Istanbul, Turkiye

CONTENT

Plenary Papers

Regular papers

Deepfake Video Detection: How Far Have We Gone?

Zoran Kotevski

University "St. Kliment Ohridski" - Bitola, Faculty of Information and Communication Technologies, Studentska bb, Bitola, North Macedonia

zoran.kotevski@uklo.edu.mk

Abstract:
The increasing sophistication and accessibility of Deepfake technology, which leverages advanced deep learning models to create realistic manipulated videos, poses a significant and escalating threat to information integrity, personal privacy, and public discourse. We may already be at a point where Deepfake videos are indiscernible from real, and in recent years we witness extensive efforts to develop robust and generalizable Deepfake detection methods. This research provides a review of the latest Deepfake video detection models and architectures, and discusses the key technical aspects that are still considered under-researched or represent major open challenges in this field.

Keywords:
Deepfake video detection, Artificial intelligence, Deep learning

1. Introduction

Deepfake technology leverages advanced deep learning models like Generative Adversarial Networks (GANs) and Autoencoders to manipulate or synthesize realistic video content. While initially developed for benign purposes, Deepfakes have been largely exploited for malicious activities, necessitating effective detection mechanisms. The origins of what we now call Deepfake can be traced back to the academic research in the 1990s when basic machine learning techniques were used to swap faces in static images [1], while the term Deepfake was coined in 2017 [2] by a Reddit user named "deepfakes". The technology gained increased attention after 2010 with the significant advancements in machine learning, the availability of large datasets, and the power of new computing resources. The biggest breakthrough in deep learning fostering Deepfakes was presented by Goodfellow et al. [3] with the introduction of GANs, which enabled the next generation of highly sophisticated image, video, and audio Deepfakes.

According to Global Cyber Alliance report [4] from May 2025, we are witnessing an explosion of Deepfake fraud incidents, with North America seeing a 1,740% increase, the Asia-Pacific region up by 1,530%, and Europe experiencing a 780% increase in 2022 alone. McAfee research from April 2024 [5] revealed that 53% of respondents say Artificial Intelligence (AI) has made it harder to spot online scams. The alarming expansion rate of Deepfake threats is confirmed by the United Kingdom Government study [6], published in February 2025, which reveals that the number of Deepfakes shared on content platforms alone is projected to surge to 8 million in 2025, up from just half a million in 2023. Deepfake statistics by Zero Threat [7] from June 2025 state that in the first quarter of 2025 alone, there was a 19% increase in Deepfake incidents compared to the total in 2024. This is particularly concerning when we take into account the fraud from February 2024 [8] when a finance worker at a multinational firm in Hong Kong was tricked into paying out 25 million USD to fraudsters using Deepfake technology to pose as the company's chief financial officer in a video conference call.

Deepfake detection is critically important for several reasons, primarily because of the profound ethical, social, and political threats posed by the malicious use of this technology. While Deepfakes have some harmless applications such as in filmmaking, their potential for harm far outweighs their benign uses. In response to these potentially harmful consequences of Deepfakes, Deepfake detection has emerged as a critical area of research and development. Significant research regarding Deepfake detection has been published in recent years, but more research is needed, since Deepfake fraudsters seem to be a step ahead. In this research we review the latest achievements in the field of Deepfake detection, and we aim to offer valuable insights in order to provide information for performance enhancements of Deepfake detection metods. Section 2 of this research presents Deepfake detection techniques, methods and models, while Section 3 gives an overview of the most widely used datasets created for training and evaluation of Deepfake detection methods. Section 4 provides a review on the latest Deepfake detection research, and Section 5 discusses the open challenges in the field. Section 6 concludes the paper with the summary of contribution.

2. Deepfake detection techniques, methods and models

Deepfake detection methods are classified into three main categories: visual-based methods, audio-based methods and multi-modal methods that combine the visual and audio part and simultaneously explore both signals [9]. Visual-based methods scrutinize the video frames for spatial and temporal inconsistencies that are often imperceptible to the naked eye. They are the most common form of Deepfake detection and employ several different approaches. Artifact-based detection approach focuses on the low-level imperfections or the digital fingerprints such as face inconsistency artifacts or up-sampling artifacts [10]. Audio-based methods are typically deployed to detect Deepfake in speech synthesis or voice conversion [11]. Speech synthesis focuses on generating entirely new speech from textual input, while voice conversion involves modifying the vocal characteristics of a source speaker to mimic a target speaker's voice. Multi-modal Deepfake detection method combines the analysis of both audio and video streams, by looking for inconsistencies between what is seen and what is heard [12]. These methods can provide a more robust and more accurate detection of Deepfakes.

Regarding the models employed, at the forefront of the fight against Deepfakes is the same technology used to generate Deepfakes, i.e. deep learning models, particularly Convolutional Neural Networks (CNNs) [13]. CNNs have demonstrated remarkable capabilities in identifying the artifacts and inconsistencies that are left behind by generative algorithms and excel at learning complex spatial and temporal features. These models are trained on vast datasets of real and fake media, learning to recognize the signs of manipulation. The most popular CNN architectures that have been adapted for Deepfake detection include XceptionNet [14], ResNet [15], VGG16 [16], and Densenet121 [17].

While CNNs excel at analyzing individual frames, Deepfake videos often exhibit inconsistencies over time, for which Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTM) [18] are frequently used. RNNs and their more advanced variant, LSTMs, are designed to process sequential data, making them ideal for capturing these temporal anomalies. They can analyze the flow of frames in a video to detect unnatural motion and flickering, inconsistent head poses and facial expressions. RNNs and LSTMs are often used in conjunction with CNNs, where the CNN extracts spatial features from each frame, and the RNN/LSTM analyzes the sequence of these features.

In recent years, Transformers [19] are used as well. They rely on self-attention mechanisms instead of recurrence. As such, they have become the dominant architecture for many sequence-processing tasks, particularly in natural language processing, due to their superior handling of long-range dependencies and greater parallelizability. RNNs are adequate for applications that require computational efficiency and real-time processing.

3. Datasets

The quality and refinement of the Deepfake detection models is critically dependent the quality, the diversity, and the complexity of the training and testing datasets. Over the past several years, a number of key datasets have emerged, each contributing uniquely to the research landscape by providing a benchmark for performance evaluation and the generalizability of new Deepfake detection methods.

FaceForensics++ [20] is one of the most widely used and foundational datasets for deepfake detection. It consists of 1000 original video sequences that have been manipulated with four automated face manipulation methods: Deepfakes, Face2Face, FaceSwap and NeuralTextures. The dataset is available in different compression levels (raw, high quality, and low quality) to simulate the effects of video compression on social media platforms, which is a significant challenge for detection models. FaceForensics++ has been instrumental in benchmarking the performance of a wide range of Deepfake detection models and has served as a standard for academic research in the field.

DFDC dataset [21] was created for a global competition launched by Facebook in partnership with Microsoft, Amazon Web Services and academics. The DFDC dataset is the largest face swap video dataset, with more than 100 thousand video clips. The main contribution of the DFDC dataset is that it pushed the boundaries of Deepfake detection by providing a large-scale, diverse, and challenging benchmark that reflects the complexity of detecting Deepfakes in real-world environments.

The Celeb-DF dataset [22], developed by Li et al., aimed to address one key limitation of earlier datasets i.e. the presence of easily detectable visual artifacts. It consists of 590 original videos of celebrities sourced from YouTube and 5,639 corresponding Deepfake videos. Many detection models that performed well on older datasets have shown a significant drop in accuracy when tested on Celeb-DF. Celeb-DF raised the bar for Deepfake detection research by providing a more realistic and more challenging benchmark that reflects the advancements in Deepfake generation technology.

Deepfake-TIMIT [23], developed by Korshunov and Marcel, is one of the earlier Deepfake datasets and is particularly notable for its focus on audio-visual Deepfakes. It is one of the smallest collections, comprising only 620 videos with swapped faces while retaining the original audio, making it useful for research into both video-based and audio-based detection methods. Deepfake-TIMIT was an important early contribution to the field, particularly for researchers interested in the audio-visual aspects of Deepfake detection.

Recognizing the growing threat of multimodal Deepfakes, in 2021 the FakeAVCeleb dataset, by Khalid et al. [24], was created to facilitate the development of detection methods that can analyze both audio and video. FakeAVCeleb is based on the VoxCeleb2 dataset [25], and besides Deepfake videos, this dataset contains corresponding synthesized audio created using advanced text-to-speech and voice conversion models. FakeAVCeleb is a crucial resource for the development of robust, multimodal Deepfake detection systems that are necessary to combat the next generation of sophisticated forgeries.

DeeperForensics-1.0 dataset, by Jiang et al. [26], was designed to solve a critical problem that many detection models that worked well in laboratory settings, have failed when faced with real-world videos that have imperfections. It's a large-scale dataset containing 60 thousand videos, providing a vast amount of data for training. The core contribution of DeeperForensics-1.0 is that it pushes the research community to create Deepfake detectors that are not just accurate, but practical and resilient in the messy, unpredictable environment of the real world.

The OpenForensics dataset, by Le et al. [27] includes various media types, such as images, videos and audio, which allows for a broader range of forensic studies. The manipulations are designed to be realistic and challenging to detect, reflecting real-world scenarios. OpenForensics is a foundational dataset that helps to counter the threat of disinformation and manipulated content by providing the necessary resources to build and validate the next generation of forensic technologies.

4. Latest research in Deepfake detection

In recent years, tremendous amount of research is focused on the development of effective Deepfake detection methods, techniques and algorithms. For Example, Cozzolino at al. [28] introduced an approach, named ID-Reveal, with an underlying CNN architecture that comprises a facial feature extractor, a temporal network and a GAN. Trained using VoxCeleb2 dataset, ID-Reveal shows improvement of more than 15% in terms of accuracy for facial reenactment on high compressed videos, compared to other state-of-the-art models. Wodajo and Atnafu [29] introduced a method to detect Deepfake videos by leveraging a Convolutional Vision Transformer (CvT), combining the strengths of CNNs and Vision Transformers (ViT). The model was trained and tested using DFDC dataset and achieved accuracy of 91.5 %, but performed poorly on the FaceForensics++ FaceShifter dataset. Gu et al. [30] proposed a method for Deepfake video detection by focusing on spatiotemporal inconsistency. The model uses CNN and employs a temporal modeling paradigm that analyzes the differences between adjacent frames in both horizontal and vertical directions. The model was trained on four public datasets: FaceForensics++, Celeb-DF, DFDC and WideDeepfake [31], and it have shown that it outperforms state-of-the-art competitors. Zhang et al. [32] introduced a Spatiotemporal Dropout Transformer (STDT). The research addresses the challenge that existing Deepfake detection methods, which often focus on single frames, fail to recognize inconsistencies across multiple frames. It was evaluated on FaceForensics++, DFDC and Celeb-DF datasets. The tests show that this approach outperforms 25 other state-of-the-art Deepfake detection methods. Ge et al. [33] proposed a Latent Pattern Sensing (LPS) model that uses a self-supervised predictive learning mechanism to train its feature extractors. Experiments on three public benchmarks (FaceForensics++, DFDC and Celeb-DF) show that the LPS model outperforms 12 other state-of-the-art methods. Zhang et al. [34] proposed a two-stage clustering process method. This approach was tested on FaceForencisc++ and their own dataset and it has shown to perform similarly to state-of-the-art detectors. Gu et al. [35] present a model that addresses a key limitation in many Deepfake detection methods, which is their failure to capture the subtle local motions and inconsistencies between adjacent video frames. The experiments showed this method outperformed the state-of-the-art model competitors on four popular benchmark dataset, i.e. FaceForensics++, Celeb-DF, DFDC and WildDeepfake. Liu, Wang and Wang [36] introduced a novel pipeline called Cross-Domain Local Forensics (XDLF). The framework also leverages four high-level forgery-sensitive local regions of a face, such as the eyes and mouth, to further enhance its detection capabilities. The conducted experiments on FaceForensics++, Celeb-DF and DFDC datasets have shown that the proposed method is superior over many state-of-the-art approaches on cross-dataset generalization. Deng, Suo and Li [37] propose a detection method using the EfficientNet-V2 network. The study utilizes two major datasets, FaceForensics++ and the newer $FFIW_{10K}$ [38], to train and validate the model. The proposed model demonstrated superior performance, achieving a validation accuracy of 97.9% on the FaceForensics++ dataset and 93.0% on the $FFIW_{10K}$ dataset. This surpassed the accuracy of existing networks like XceptionNet on the FaceForensics++ dataset. Xu et al. [39] introduced a method that addresses the issue that existing video-based Deepfake detectors are often computationally intensive. The research integrates a strategy named Thumbnail layout (TALL) with the Swin Transformer [40] to create an efficient and effective method called TALL-Swin. Experiments on Face Forensics++, Celeb-DF, DFDC, and DeeperForensics-1.0 show that TALL-Swin outperforms the state-of the-art approaches. Elpeltagy et al. [41] proposed a new system for detecting Deepfake videos by analyzing both visual frames and audio. For visual frames, the system uses an upgraded XceptionNet model to extract spatial features. Evaluated on the FakeAVCeleb dataset, it has shown superiority over the existing state-of-the-art approaches. Ciamarra et al. [42] presents a method for detecting Deepfake videos by identifying "temporal surface frame anomalies". The tests performed on FaceForensics++ dataset show that this methodology can achieve significant performance in detection accuracy.

Many other research efforts introduce novel Deepfake detection methods, such as Borade et al. [43], combining three distinct models: ResNet50, EfficientNetB7, and EfficientNetAutoAttB4 to design a robust, adaptable to the unique Deepfake detection mechanism that requires minimal computing power. Choi et al. [44] propose an approach to Deepfake video detection by analyzing the "temporal changes of style latent vectors" in generated videos in a framework that uses a module named StyleGRU, trained with contrastive learning, and includes a style attention module to detect both visual and temporal artifacts. Lu at al. [47] presented a method for detecting Deepfake videos by using a technique called Long-Distance Attention, to identify the subtle differences between real and fake faces that are often left as common artifacts in both the spatial and temporal domains, while Roy et al. [48] proposed a Deepfake video detection system that uses a combination of 3D CNNs and attention mechanisms. Zhai et al. [49] introduces the Dual-stream Frequency-Spatial Fusion (DFSF) network, an approach for Deepfake detection that improves generalization and robustness. The method addresses the limitations of detectors that focus only on spatial or frequency artifacts, which often fail against new forgery techniques or compressed videos. Hu et al. [50] propose Delocate, a two-stage model designed to improve the detection and localization of Deepfake videos, particularly those from unknown sources with randomly tampered areas, while Yan et al. [51] present a "plug-and-play" framework for Deepfake video detection, aimed to improve the model's ability to generalize to new, unseen manipulation techniques and datasets. Balara, Machova and Mach [52] explore the use of a variety of CNN based architectures to detect Deepfakes, particularly those depicting human faces. Satwika et al. [53] introduced a Deepfake video detection system that combines an EfficientNet model, which is a cutting-edge CNN architecture, and a LSTM network to analyze both spatial and temporal features of a video. Pawar et al. [54] proposed a real-time system designed to combat the spread of manipulated video content on social media. They develop a social media platform with an integrated AI-based CNN detection engine to identify Deepfakes during the upload process, and report detection accuracy between 85 and 90%. Nigade et al. [55] presented a framework for detecting Deepfake videos by combining two powerful machine learning techniques: ResNet50v2 and LSTM networks. The hybrid model, leveraging both spatial and temporal analysis, was trained on a combined dataset of real and fake videos (FaceForensics++, Celeb-DF, and DFFD).

All the presented Deepfake detection methods have been evaluated on one or more datasets, and the results presented show high effectiveness and accuracy, but there are still challenges that need to be addressed, which is discussed in the following section.

5. Discussion

The research community has made significant accomplishments in the fight against the increasingly sophisticated Deepfake generation models, but several aspects are still considered under-researched or represent major open challenges in the field. Here are some of the key areas of Deepfake detection that are not yet thoroughly researched.

The Deepfake detectors are usually trained and evaluated on a single or multiple datasets, such as FaceForensics++, DeeperForensics-1.0, Celeb-DF etc., and are proven to be quite effective. But, they are rarely tested on in-the-wild Deepfakes and often fail when tested on Deepfakes generated by unseen architectures or from different datasets. Little work exists on universal detectors that can handle video, audio, and multimodal Deepfakes equally well. There is also a lack of models that can generalize effectively across different Deepfake generation architectures and across various video platforms which have different compression algorithms. A big research challenge would be the development of Deepfake detectors that can identify unknown manipulation techniques without requiring retraining, i.e a universal detection method that doesn't rely on specific, known artifacts but instead learns to recognize the fundamental properties of real media.

Another issue is that the majority of Deepfake detection methods, especially the older ones, are concentrated on the visual domain only. However, Deepfakes are increasingly a multimodal phenomenon, incorporating manipulated audio and video, thus some of the newer research has begun to explore multi-modal detection (combining video, audio, and even text), but the fusion of these data streams in Deepfake detection approaches is far from perfected. Developing sophisticated fusion architectures that can effectively analyze and find inconsistencies between different data modalities is a challenging task. More research is needed to understand how artifacts from different modalities interact and how to develop detectors that can identify these combined manipulations.

One emerging critical area is the adversarial attacks [56] on Deepfake detectors. Deepfake creators are beginning to deliberately design their fakes to fool detection algorithms, by adding imperceptible noise to the Deepfakes that is specifically crafted to confuse the detector. Developing detectors robust to adversarial perturbations and intentional obfuscation is a challenging matter for future research.

Most advanced detection models require significant computational power, making them impractical for real-time applications on standard hardware. They are often too slow and resource-intensive to be deployed on mobile devices or for large-scale, real-time social media monitoring. Developing lightweight, efficient models that can run on consumer-grade hardware or even on edge devices is an important research challenge that needs to be addressed.

Deep learning models are often “black boxes”, providing a binary output (real or fake) without a clear explanation for their decision. This lack of interpretability is a major barrier to using Deepfake detection in high-stakes applications like journalism, legal proceedings, or law enforcement. The research field needs to expand to more reliable techniques to attribute a Deepfake to the specific generative model or software that created it, as well as to ensure the integrity of a suspected Deepfake as it is collected and analyzed for forensic purposes, making the findings admissible in legal proceedings. Research into human-interpretable forensic cues needs further research as well.

A promising area of research involves detecting Deepfakes at the hardware [57] and sensor level, because every camera sensor has a unique noise pattern, known as Photo-Response Non-Uniformity (PRNU). Research is needed to develop robust methods that can detect inconsistencies in these fingerprints to identify manipulated images and videos, as well as on the use of non-traditional sensors, such as thermal or depth sensors, to capture information that is difficult to convincingly synthesize with current Deepfake generation techniques.

Furthermore, social media platforms perform re-encoding to the videos, and add noise during this process that often degrades or erases subtle forensic traces. Therefore robust Deepfake detection methods under heavy video compression are needed. Most research focuses on face-swapping, but Deepfakes are expanding to AI-generated art, text, and even full-body synthetic avatars, hence Unified detection frameworks for diverse synthetic media are required. As the creation of synthetic media becomes increasingly sophisticated and accessible, the field of Deepfake detection must evolve beyond its current paradigms. By exploring these under-researched technical areas, the research community can work towards building a more resilient and trustworthy information ecosystem.

6. Conclusion

In this research, we have surveyed the latest achievements in the Deepfake detection domain, examining various approaches. These methods have demonstrated significant progress in identifying manipulated content, leveraging advances in CNNs, self-supervised learning, and hybrid models that integrate audio, video, and textual cues. But despite these achievements, critical research gaps still remain. Adversarial resilience against imperceptible perturbations is still in its infancy, limiting real-world robustness. Cross-domain generalization beyond benchmark datasets, especially for unseen generation algorithms, requires more universal frameworks. The challenge of deploying lightweight, low-latency detectors on edge devices has not been fully addressed. Explainability is another frontier that current detectors lack transparent, forensic-grade reasoning for end users and legal contexts. Detection in compressed or degraded media and non-visual Deepfakes demand dedicated research as well.

Future work should prioritize the integration of adversarial defense mechanisms, domain-adaptive training strategies and efficient model architectures tailored for mobile and embedded platforms. Developing interpretable forensic cues alongside end-to-end detection pipelines will bridge the gap between automated analysis and human verification. Multimodal, cross-resolution frameworks that maintain high accuracy under compression and noise will be essential for real-world adoption. Addressing these challenges will not only fortify our defenses against evolving Deepfake threats but also pave the way for more transparent and trustworthy digital media ecosystems.

References:

[1] George, A. Shaji, and AS Hovan George. “Deepfakes: the evolution of hyper realistic media manipulation.” Partners Universal Innovative Research Publication 1, no. 2 (2023): 58-74.

[2] Tina Brooks, Princess G., Jesse Heatley, Jeremy J., Scott Kim, Samantha M., Sara Parks, Maureen Reardon, Harley Rohrbacher, Burak Sahin, Shani S., James S., Oliver T., Richard V. “Increasing Threat of Deepfake Identities”. US Department of Homeland Security Report (2021).

[3] Goodfellow, Ian J., Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. “Generative adversarial nets.” Advances in neural information processing systems 27 (2014).

[4] Megan Cruse. “Seeing Isn’t Believing - Staying Safe During the Deepfake Revolution”. Global Cyber Alliance (2025). globalcyberalliance.org

[5] McAfee Corporation. “McAfee Study Reveals Peoples’ Deep Concerns About the Impact of AI-Generated Deepfakes During Critical Election Year”, (2024). www.mcafee.com

[6] UK Government Case Study. “Innovating to detect deepfakes and protect the public”. (2025) www.gov.uk [7] Zero Threat - Trends and Statistics. “Deepfakes & AI Phishing in 2025: Alarming Stats You Can’t Ignore”.
(2025) zerothreat.ai

[8] Kathleen Magramo, “Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’”. CNN Article (2024).

[9] Alrashoud, Mubarak. “Deepfake video detection methods, approaches, and challenges”. Alexandria Engineering Journal 125 (2025): 265-277.

[10] Ma, Long, Zhiyuan Yan, Yize Chen, Jin Xu, Qinglang Guo, Hu Huang, Yong Liao, and Hui Lin. “From specificity to generality: Revisiting generalizable artifacts in detecting face deepfakes”. arXiv preprint arXiv:2504.04827 (2025).

[11] Zhang, Bowen, Hui Cui, Van Nguyen, and Monica Whitty. “Audio deepfake detection: What has been achieved and what lies ahead”. Sensors (Basel, Switzerland) 25, no. 7 (2025): 1989.

[12] Salvi, Davide, Honggu Liu, Sara Mandelli, Paolo Bestagini, Wenbo Zhou, Weiming Zhang, and Stefano Tubaro. “A robust approach to multimodal deepfake detection”. Journal of Imaging 9, no.

6 (2023): 122.

[13] Abbasi, Maryam, Paulo Váz, José Silva, and Pedro Martins. “Comprehensive Evaluation of Deepfake Detection Models: Accuracy, Generalization, and Resilience to Adversarial Attacks”. Applied Sciences 15, no. 3 (2025): 1225.

[14] Chollet, François. “Xception: Deep learning with depthwise separable convolutions”. In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1251-1258. 2017.

[15] He, Kaiming, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. "Deep residual learning for image recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770-778. 2016.

[16] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." arXiv preprint arXiv:1409.1556 (2014).

[17] Huang, Gao, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q. Weinberger. "Densely connected convolutional networks." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 4700-4708. 2017.

[18] Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." Neural computation 9, no. 8 (1997): 1735-1780.

[19] Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. "Attention is all you need." Advances in neural information processing systems 30 (2017).

[20] Rossler, Andreas, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, and Matthias Nießner. "Faceforensics++: Learning to detect manipulated facial images." In Proceedings of the IEEE/CVF international conference on computer vision, pp. 1-11. 2019.

[21] Dolhansky, Brian, Joanna Bitton, Ben Pflaum, Jikuo Lu, Russ Howes, Menglin Wang, and Cristian Canton Ferrer. "The deepfake detection challenge (dfdc) dataset." arXiv preprint arXiv:2006.07397 (2020).

[22] Li, Yuezun, Xin Yang, Pu Sun, Honggang Qi, and Siwei Lyu. "Celeb-df: A large-scale challenging dataset for deepfake forensics." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 3207-3216. 2020.

[23] Korshunov, Pavel, and Sébastien Marcel. "Deepfakes: a new threat to face recognition? assessment and detection." arXiv preprint arXiv:1812.08685 (2018).

[24] Khalid, Hasam, Shahroz Tariq, Minha Kim, and Simon S. Woo. "FakeAVCeleb: A novel audio-video multimodal deepfake dataset." arXiv preprint arXiv:2108.05080 (2021).

[25] Chung, Joon Son, Arsha Nagrani, and Andrew Zisserman. "Voxceleb2: Deep speaker recognition." arXiv preprint arXiv:1806.05622 (2018).

[26] Jiang, Liming, Ren Li, Wayne Wu, Chen Qian, and Chen Change Loy. "Deeperforensics-1.0: A large-scale dataset for real-world face forgery detection." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 2889-2898. 2020.

[27] Le, Trung-Nghia, Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen. "Openforensics: Large-scale challenging dataset for multi-face forgery detection and segmentation in-the-wild." In Proceedings of the IEEE/CVF international conference on computer vision, pp. 10117-10127. 2021.

[28] Cozzolino, Davide, Andreas Rössler, Justus Thies, Matthias Nießner, and Luisa Verdoliva. "Id-reveal: Identity-aware deepfake video detection." In Proceedings of the IEEE/CVF international conference on computer vision, pp. 15108-15117. 2021.

[29] Wodajo, Deressa, and Solomon Atnafu. "Deepfake video detection using convolutional vision transformer." arXiv preprint arXiv:2102.11126 (2021).

[30] Gu, Zhihao, Yang Chen, Taiping Yao, Shouhong Ding, Jilin Li, Feiyue Huang, and Lizhuang Ma. "Spatiotemporal inconsistency learning for deepfake video detection." In Proceedings of the 29th ACM international conference on multimedia, pp. 3473-3481. 2021.

[31] Zi, Bojia, Minghao Chang, Jingjing Chen, Xingjun Ma, and Yu-Gang Jiang. "Wilddeepfake: A challenging real-world dataset for deepfake detection." In Proceedings of the 28th ACM international conference on multimedia, pp. 2382-2390. 2020.

[32] Zhang, Daichi, Fanzhao Lin, Yingying Hua, Pengju Wang, Dan Zeng, and Shiming Ge. "Deepfake video detection with spatiotemporal dropout transformer." In Proceedings of the 30th ACM international conference on multimedia, pp. 5833-5841. 2022.

[33] Ge, Shiming, Fanzhao Lin, Chenyu Li, Daichi Zhang, Weiping Wang, and Dan Zeng. "Deepfake

video detection via predictive representation learning." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 18, no. 2s (2022): 1-21.
[34] Zhang, Li, Tong Qiao, Ming Xu, Ning Zheng, and Shichuang Xie. "Unsupervised learning-based framework for deepfake video detection." IEEE Transactions on Multimedia 25 (2022): 4785-4799.
[35] Gu, Zhihao, Yang Chen, Taiping Yao, Shouhong Ding, Jilin Li, and Lizhuang Ma. "Delving into the local: Dynamic inconsistency learning for deepfake video detection." In Proceedings of the AAAI conference on artificial intelligence, vol. 36, no. 1, pp. 744-752. 2022.
[36] Liu, Zihan, Hanyi Wang, and Shilin Wang. "Cross-domain local characteristic enhanced deepfake video detection." In Proceedings of the Asian Conference on Computer Vision, pp. 3412-3429. 2022.
[37] Deng, Liwei, Hongfei Suo, and Dongjie Li. "Deepfake Video Detection Based on EfficientNet-V2 Network." Computational Intelligence and Neuroscience 2022, no. 1 (2022): 3441549.
[38] Zhou, Tianfei, Wenguan Wang, Zhiyuan Liang, and Jianbing Shen. "Face forensics in the wild." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 5778-5788. 2021.
[39] Xu, Yuting, Jian Liang, Gengyun Jia, Ziming Yang, Yanhao Zhang, and Ran He. "Tall: Thumbnail layout for deepfake video detection." In Proceedings of the IEEE/CVF international conference on computer vision, pp. 22658-22668. 2023.
[40] Liu, Ze, Yutong Lin, Yue Cao, Han Hu, Yixuan Wei, Zheng Zhang, Stephen Lin, and Baining Guo. "Swin transformer: Hierarchical vision transformer using shifted windows." In Proceedings of the IEEE/CVF international conference on computer vision, pp. 10012-10022. 2021.
[41] Elpeltagy, Marwa, Aya Ismail, Mervat S. Zaki, and Kamal Eldahshan. "A novel smart deepfake video detection system." International Journal of Advanced Computer Science and Applications 14, no. 1 (2023).
[42] Ciamarra, Andrea, Roberto Caldelli, and Alberto Del Bimbo. "Temporal surface frame anomalies for deepfake video detection." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 3837-3844. 2024.
[43] Shwetambari Borade, Nilakshi Jain, Bhavesh Patel, Vineet Kumar, Mustansir Godhrawala, Shubham Kolaskar, Yash Nagare, Pratham Shah, Jayan Shah. “Advancements in Video Deepfake Detection: Integration of ResNet50, EfficientNetB7, and Efficient NetAutoAtt B4 Models”. International Journal of Intelligent Systems And Applications In Engineering, IJISAE, 2024, 12(3), 1206–1212
[44] Choi, Jongwook, Taehoon Kim, Yonghyun Jeong, Seungryul Baek, and Jongwon Choi. "Exploiting Style Latent Flows for Generalizing Deepfake Video Detection Supplementary Material."
[45] Li, Lingzhi, Jianmin Bao, Hao Yang, Dong Chen, and Fang Wen. "Faceshifter: Towards high fidelity and occlusion aware face swapping." arXiv preprint arXiv:1912.13457 (2019).
[46] Nick Dufour and Andrew Gully. “Contributing Data to Deepfake Detection Research”. Google Research and Jigsaw (2019)
[47] Lu, Wei, Lingyi Liu, Bolin Zhang, Junwei Luo, Xianfeng Zhao, Yicong Zhou, and Jiwu Huang. "Detection of deepfake videos using long-distance attention." IEEE transactions on neural networks and learning systems 35, no. 7 (2023): 9366-9379.
[48] Roy, Ritaban, Indu Joshi, Abhijit Das, and Antitza Dantcheva. "3D CNN architectures and attention mechanisms for deepfake detection." In Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, pp. 213-234. Cham: Springer International Publishing, 2022.
[49] Zhai, Tianbo, Kaiyin Lu, Jiajun Li, Yukai Wang, Wenjie Zhang, Peipeng Yu, and Zhihua Xia. "Learning spatial-frequency interaction for generalizable deepfake detection." IET Image Processing 18, no. 14 (2024): 4666-4679.
[50] Hu, Juan, Xin Liao, Difei Gao, Satoshi Tsutsui, Qian Wang, Zheng Qin, and Mike Zheng Shou. "Delocate: Detection and localization for deepfake videos with randomly-located tampered traces." arXiv preprint arXiv:2401.13516 (2024).
[51] Yan, Zhiyuan, Yandan Zhao, Shen Chen, Mingyi Guo, Xinghe Fu, Taiping Yao, Shouhong Ding, Yunsheng Wu, and Li Yuan. "Generalizing deepfake video detection with plug-and-play: Video-level blending and spatiotemporal adapter tuning." In Proceedings of the Computer Vision and Pattern Recognition Conference, pp. 12615-12625. 2025.

[52] Balara, Viliam, Kristína Machová, and Marián Mach. "Detection of Visual Deepfakes using Deep Convolutional Networks." (2025).

[53] Satwika.M, Neha.K, Pranavya.A, Rishika.K, Siva Sankar Namani "Video Deepfake Detection Using EfficientNet and LSTM". International Research Journal of Innovations in Engineering and Technology (IRJIET), Volume 9, Issue 3, pp 148-154, 2025.

[54] Neha Pawar, Sanika Arekar, Sanika Gaikwad, Prajakta Teli, Ms. Amrapali Babar. "Cutting-Edge Real-Time System for the Detection of AI-Generated and Manipulated Video Content" International Journal of Research Publication and Reviews, Vol 6, Issue 7, pp 4569-4574, 2025

[55] Chaitali Nigade1, Shreya Sakare, Shruti Sakare, Mayuri Salunkhe, Nilofar Mulla. "Safeguarding Society: A DeepFake Video Detection Framework". International Journal of Innovative Research In Technology, Volume 12 Issue 1, 2025.

[56] Aneja, Shivangi, Lev Markhasin, and Matthias Nießner. "Tafim: Targeted adversarial attacks against facial image manipulations." In European Conference on Computer Vision, pp. 58-75. Cham: Springer Nature Switzerland, 2022.

[57] Kamrul Hasan, Nima Karimian, Sara Tehranipoor. "Combating Deepfakes: A Novel Hybrid Hardware- Software Approach". Silicon Valley Cybersecurity Conference (SVCC), 2024.