e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707242 |

Enhancing Deepfake Video Detection with Long-Distance Attention Mechanisms

Akshitha Annapurna T, Prof. Rajeshwari N

MCA Student, Department of Computer Application, Bangalore Institute of Technology, Bangalore, India

Assistant Professor, Department of Computer Application, Bangalore Institute of Technology, Bangalore, India

ABSTRACT: Rapid advancements in AI, machine learning algorithms, and deep learning over the past few years led to the development of new methods and tools for altering multimedia. Despite the fact the technology have mainly been utilized for good reasons, including entertainment and education, unscrupulous people have nonetheless taken advantage of it for illegal or sinister ends. For instance, realistic-seeming, high-quality phony films, pictures, or sounds have been produced with the intention of propagandizing false information, inciting hatred and political unrest, or even harassing and blackmailing individuals. Recently, the highly-reproduced, lifelike, and altered videos have come to be known as Deepfake. Since then, a number of strategies have been detailed in the literature to address the issues brought up by Deepfake. In this study, we undertake a systematic literature review (SLR) to provide an updated overview of the research efforts in Deepfake detection. We summarize 112 relevant papers from 2018 to 2020 that presented a range of techniques. And differentiate it into four more groups for analysis. Methods based on deep learning, methods based on conventional machine learning, methods based on statistics, and approaches based on blockchain. We also assess how well the different algorithms recognize patterns on different datasets, and we find that deep learning-based make it work better than other Deepfake detection.

KEYWORDS: manipulating multimedia, legitimate applications.

I.INTRODUCTION

The significant developments in artificial neural network (ANN)-based technologies are crucial for manipulating multimedia content. For example, realistic-looking face swapping in photos and videos has been achieved with AI-enabled software applications such as Face App [1] and Fake App [2].This swapping mechanism allows anyone to alter the front look, hairstyle, gender, age, and other personal attributes. The propagation of these fake videos causes many anxieties and has become famous under the hood, Deepfake. The term ``Deep fake'' is derived from ``Deep Learning (DL)'' and ``Fake,'' and it describes specific photo-realistic video or image contents created with DL's support. This phrase was given its name in honor of an anonymous Reddit user who, in late 2017, used deep learning techniques to make photo-realistic phony movies by utilizing someone else's face to replace the person's in pornographic videos. Two neural networks were used to create these fake videos: a generative network and a discriminative network that employed the Face Swap approach [3], [4]. The generative network uses an encoder and a decoder to produce artificial visuals. The newly generated images' legitimacy is determined by the discriminative network. Ian Goodfellow introduced the concept of Generative Adversarial Networks (GANs), which are essentially these two networks together. Researchers in Deep Fake (DL) achieved numerous relevant achievements in generative modelling, as reported in an annual report [6]. For example, computer vision researchers proposed a method known as Face2Face [7] for facial re-enactment.This method transfers facial expressions from one person to a real digital 'avatar' in real-time. In 2017, researchers from UC Berkeley presented Cycle GAN [8] eventually, in November 2017, the term "deep fake" surfaced for the uploading of pornographic videos in which the faces of celebrities were replaced with their real ones. A Deepfake creation service was introduced in January 2018 by a number of websites with funding from private sponsors. After a month, several websites, including Gfycat [10], Pornhub, and Twitter, banned these services. However, considering the threats and potential risks in privacy vulnerabilities, the study of Deep fake emerged super-fast. In March 2018, Rossler et al. released a large video dataset for media forensic and deep fake detection techniques dubbed Face Forensic .Apart from Deep fake pornography, there are many other malicious or illegal uses of Deep fake, such as spreading misinformation, creating political instability, or various cybercrimes. In response to these dangers, the subject of Deepfake detection has garnered significant attention from specialists and scholars in recent years, leading to the development of numerous Deepfake detection algorithms. Additionally, some efforts are being made to examine a subset of the literature with an emphasis on performance analysis or detection techniques. However, a more comprehensive overview of this research area will be beneficial in serving the community of researchers and

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707242 |

practitioners by providing summarized information about Deep fake in all aspects, including available datasets, which are noticeably missing in previous surveys. In order to do such, in this study we provide a systematic literature review (SLR) on Deep fake detection. Our goal is to outline and examine the commonalities as well as the variety of methods used in contemporary deepfake detection strategies.

Our contributions are summarized as follows:
We do a thorough analysis of the body of work already written in the Deepfake field. We report current tools, techniques, and datasets for Deepfake detection-related research by posing some research questions.

We introduce a taxonomy that classifies Deepfake detection techniques in four categories with an overview of different categories and related features, which is novel and the first of its kind.

We conduct an in-depth analysis of the primary studies' experimental evidence. Also, we use distinct measuring parameters to assess the effectiveness of different Deepfake detecting techniques. We draw attention to a few findings and provide some recommendations on Deepfake detection that may be useful for further studies and applications in this area. The remaining sections of the document are arranged as follows: By defining research issues of interest, Section II outlines the review process. We go into great detail about the results from several research in Section III. The study's general observations are compiled in Section IV, and in Section V, we outline the difficulties and constraints. The paper is finally concluded in Section VI.

II. LITERATURE REVIEW

This paper explores the efficacy of attention mechanisms, particularly long-distance attention, in detecting deepfake videos. The authors review numerous deep learning models that incorporate attention layers and evaluate their performance on publicly available deepfake datasets. The findings suggest that attention mechanisms significantly improve the detection accuracy by focusing on subtle inconsistencies across frames. Transformers, known for their attention-based architecture, have shown promise in various domains, including deepfake detection. This survey provides a comprehensive overview of recent research employing transformer networks to identify deepfake videos. By analysing the advantages and limitations of different transformer models, the authors highlight key advancements and potential areas for further research. The paper surveys recent advancements in deepfake detection, focusing on methods utilizing long-distance attention. The authors discuss various techniques, including self-attention and cross-attention, and their application in capturing temporal dependencies in video sequences. The study accomplishes that these approaches are highly effective in improving detection rates. This review examines the role of attention mechanisms in deepfake detection, emphasizing the use of long-distance attention. The authors present a taxonomy of attention-based models and evaluate their performance on standard benchmarks. The review highlights the importance of capturing long-range dependencies for effective deepfake detection.The survey provides an in-depth analysis of various deepfake detection techniques, with a focus on methods employing attention mechanisms. By reviewing both classical and state-of-the-art approaches, the authors identify the strengths of attention-based models in detecting subtle manipulations in video content. This paper investigates the usage of long-distance attention in developing robust deepfake detection systems. The authors review multiple studies that implement attention layers to capture long-range dependencies across video frames. The results highlight how well these techniques work to separate real videos from deepfakes.

III. METHODOLOGY OF PROPOSED SURVEY

We perform a comprehensive survey on existing literature in the Deepfake domain. We report current tools, techniques, and datasets for Deepfake detection-related research by posing some research questions.We introduce a taxonomy that classifies Deepfake detection techniques in four categories with an overview of different categories and related features, which is novel and the first of its kind. We perform a thorough examination of the experimental evidence from the primary research. Additionally, we use several assessment measures to assess the effectiveness of different Deepfake detection techniques. We highlight a few observations and deliver some guidelines on Deepfake detection that might help future research and practices in this spectrum.

Existing System:
Introduced a GAN simulator that replicates collective GAN-image artifacts and feeds them as input to a classifier to identify them as Deepfake proposed a network for extracting the standard features from RGB data, while proposed a similar but generic resolution. Besides, in researchers proposed a new detection framework based on physiological measurement, for example, Heartbeat.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707242 |

At first, the deep learning-based method was proposed in for Deepfake video detection. Two inception modules, (i) Meso-4 and (ii) MesoInception-4, were used to build their proposed network. In this technique, the mean squared error (MSE) between the actual and expected labels is used as the loss function for training. An enhancement of Meso-4 has been proposed in the system.

Proposed Methodology:
We perform a comprehensive survey on existing literature in the Deepfake domain. We report current tools, techniques, and datasets for Deepfake detection-related research by posing some research questions.

We introduce a taxonomy that classifies Deepfake detection techniques in four categories with an overview of different categories and related features, which is novel and the first of its kind.

We conduct an in-depth analysis of the primary studies' experimental evidence. Also, we evaluate the performance of various Deepfake detection methods using different measurement metrics.

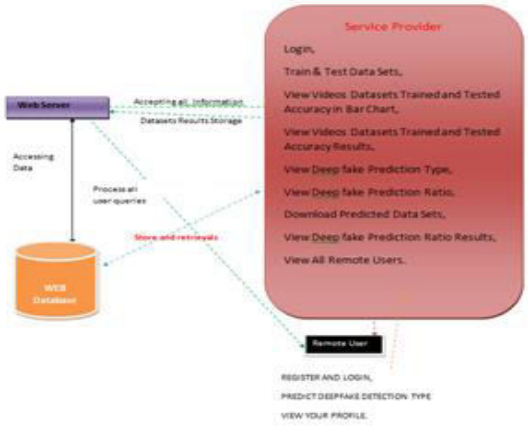


Fig 1. Service provider

Service Provider
The Service Provider must enter a valid user name and password to log in to this module. Once he logs in successfully, he can perform several tasks like logging in, training and testing data sets, View the trained and tested accuracy of the video datasets in a bar chart; view the results of the training and testing of the accuracy of the video datasets; view the type and ratio of the deep fake prediction; download the predicted data sets; view the results of the deep fake prediction ratio; and view all remote users.

View and Permit Users
The administrator can see a list of all enrolled users in this module. In this, the administrator may see user information such name, email address, and address, and they can also approve people.

Remote Operator
There are n numbers of users present in this module. Prior to beginning any operations, the user must register. The user's information is saved in the database after they register. Upon successful registration, he must use his permitted user name and password to log in. Following a successful login, the user will perform certain tasks like PREDICT, REGISTER AND LOGIN, DEEPFAKE DETECTION TYPE, and VIEW YOUR PROFILE.

IV. RESULTS AND ANALYSIS

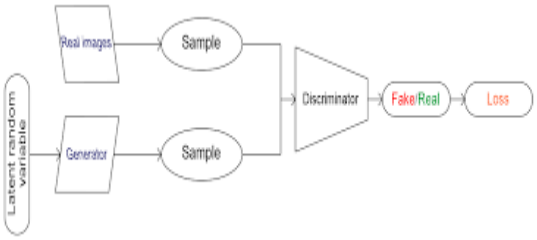
This comprehensive overview of the literature presents various state-of-the-art methods for detecting deepfakes, covering 112 studies published from early 2018 to late 2020. It outlines fundamental techniques and evaluates the efficacy of different detection models.
Key findings include:
-Deep learning-based methods are predominantly used for deepfake detection.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707242 |

- The FF++ dataset is the utmost frequently employed in experiments.
- Convolutional Neural Network (CNN) models constitute a significant portion of the detection models.
- The performance metric that is most frequently utilized is detection accuracy.



Experimental results show that deep learning techniques are effective in detecting deepfakes, generally outperforming non-deep learning models. Despite rapid advancements in multimedia technology and the proliferation of tools and applications, deepfake detection still faces many challenges. This SLR aims to provide a valuable resource for the research community in developing effective detection methods and countermeasures.

V.CONCLUSION

This comprehensive overview of the literature presents an extensive analysis of various state-of-the-art methods for detecting deepfakes, covering 112 studies from early 2018 to late 2020. It highlights that deep learning-based methods, particularly Convolutional Neural Networks (CNNs), are predominantly used for deepfake detection, with the FF++ dataset being the most frequently employed. Detection accuracy is identified as the most common performance metric. According to the experimental data, deep learning methods perform better than non-deep learning models and are quite effective. Deepfake detection continues to be difficult despite major breakthroughs since deepfake tools are widely available and technological advancements happen quickly. This systematic literature review is an invaluable tool for academics as it offers useful insights for creating detection strategies and countermeasures against deepfakes.

VI. FUTURE WORK

Future enhancements in the field of Deepfake detection can be anticipated across several dimensions, driven by advancements in technology and the evolving sophistication of Deepfake creation methods. One promising direction is the development of hybrid detection systems that combine the strengths of deep learning-based techniques with classical machine learning and statistical methods to enhance accuracy and robustness. These hybrid models can leverage the comprehensive feature extraction capabilities of deep learning alongside the interpretability and efficiency of classical approaches. Another potential enhancement lies in the integration of real-time detection systems capable of identifying Deepfake content instantaneously. This would involve optimizing algorithms for speed without compromising accuracy, making them suitable for deployment in live-streaming scenarios and social media platforms.

REFERENCES

1. Sailasya, G., & Kumari, G. L. A. (2021). Analyzing the performance of stroke prediction using ML classification algorithms. International Journal of Advanced Computer Science and Applications, 12(6).
2. Devaki, A., & Rao, C. G. (2022, February). An Ensemble Framework for Improving Brain Stroke Prediction Performance. In 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) (pp. 1-7). IEEE.
3. Ghannam, A., & Alwidian, J. A Predictive Model of Stroke Diseases using Machine Learning Techniques.
4. Akter, B., Rajbongshi, A., Sazzad, S., Shakil, R., Biswas, J., & Sara, U. (2022, January). A machine learning approach to detect the brain stroke disease. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 897-901). IEEE.
5. Sathya Sundaram., Pavithra.K., Poojasree.V, & Priyadharshini.S. (2020). STROKE PREDICTION USING MACHINE LEARNING: a review. International Advanced Research Journal in Science, Engineering and Technology, DOI: 10.17148/IARJSET.2022.9620.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707242 |

6. Rishabh Gurjar, Sahana H K , Neelambika C , Sparsha B Sathish , Ramys S (2022). Stroke Risk Prediction Using Machine Learning Algorithms: International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)doi : https://doi.org/10.32628/CSEIT2283121.
7. Tazin, T., Alam, M. N., Dola, N. N., Bari, M. S., Bourouis, S., & Monirujjaman Khan, M. (2021). Stroke disease detection and prediction using robust learning approaches. Journal of healthcare engineering, 2021.
8. https://www.kaggle.com/datasets/zzettrkalpakbal/full- filled-brainstroke-dataset
9. LaValley, M. P. (2008). Logistic regression. Circulation, 117(18), 2395-2399.
10. Quinlan, J. R. (1996). Learning decision tree classifiers. ACM Computing Surveys (CSUR), 28(1), 71-72.
11. Petkovic, D., Altman, R., Wong, M., & Vigil, A. (2018). Improving the explainability of Random Forest classifier–user centered approach. In Pacific symposium on biocomputing 2018: proceedings of the pacific symposium (pp. 204-215).
12. Chen, P. H., Lin, C. J., & Schölkopf, B. (2005). A tutorial on ν-support vector machines. Applied Stochastic Models in Business and Industry, 21(2), 111-136.
13. Yang, F. J. (2018, December). An implementation of naive bayes classifier. In 2018 International conference on computational science and computational intelligence (CSCI) (pp. 301-306). IEEE.
14. Ali, P. U. S., & Ventakeswaran, D. C. J. (2011). Improved evidence theoretic kNN classifier based on theory of evidence. International Journal of Computer Applications, 15(5), 37-41.
15. Islam, R., Debnath, S., & Palash, T. I. (2021, December). Predictive Analysis for Risk of Stroke Using Machine Learning Techniques. In 2021 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2) (pp. 1-4). IEEE.
16. Borugadda, P., Lakshmi, R., & Sahoo, S. (2023). Transfer Learning VGG16 Model for Classification of Tomato Plant Leaf Diseases: A Novel Approach for Multi-Level Dimensional Reduction. Pertanika Journal of Science & Technology, 31(2).
17. Yadav, Shubham and Patwa, Anuj and Rane, Saiprasad & Narvekar, Chhaya. (2019). Indian Traffic Sign Board Affirmation and Driver Prepared Structure Using artificial intelligence. Overall Journal of Applied Sciences and Smart Developments. 1. 1-10. 10.24071/ijasst.v1i1.1843.
18. Anushree A., S., Kumar, H., Iram, I., &Divyam, K. (2019). Modified Announcement Revelation System by the Vehicles.
19. S. Harini, V. Abhiram, R. Hegde, B. D. D. Samarth, S. A. Shreyas and K. H. Gowranga, "A savvy driver prepared system for vehicle traffic using picture area and affirmation methodology," 2017 second IEEE Overall Social event on Late Examples in Equipment, Information and Correspondence Development (RTEICT), Bangalore, India, 2017, pp. 1540-1543, doi: 10.1109/RTEICT.2017.8256856.
20. C. Wang, "Investigation and Usage of Traffic Sign Disclosure and Affirmation Considering Significant Learning," 2018 Worldwide Gathering on Robots and Clever Structure (ICRIS), Changsha, China, 2018, pp. 150-152, doi: 10.1109/ICRIS.2018.00047.
21. M A Muchtar etal2017J. Phys.: Conf. Ser. 801 012010
22. Y. Yuan, Z. Xiong and Q. Wang, "VSSA-NET: Vertical Spatial Progression Thought Association for Traffic Sign Acknowledgment," in IEEE Trades on Picture Dealing with, vol. 28, no. 7, pp. 3423-3434, July 2019, doi: 10.1109/TIP.2019.2896952.
23. S. Huang, H. Lin and C. Chang, "An in-vehicle camera structure for traffic sign area and affirmation," 2017 Joint seventeenth World Congress of Worldwide Feathery Systems Alliance and ninth Overall Gathering on Fragile Figuring and Brilliant Structures (IFSA-SCIS), Otsu, Japan, 2017, pp. 1-6, Doi: 10.1109/IFSA-SCIS.2017.8023239.
24. Bi, Z., Yu, L., Gao, H. et al. Further created VGG model-based compelling traffic sign affirmation for safe driving in 5G circumstances. Int. J. Mach. Learn. & Cyber. (2020).
25. Chuanwei Zhang et al., Focus on Traffic Sign Affirmation by Improved Lenet-5 Estimation, Overall Journal of Model Affirmation and Man-made thinking, doi:0.1142/S0218001420550034
26. Han, C., Gao, G. & Zhang, Y. Continuous little traffic sign acknowledgment with refreshed speedier RCNN. Multimed Gadgets Appl 78, 13263-13278 (2019). https://doi.org/10.1007/s11042-018-6428-0
27. H. S. Lee and K. Kim, "Simultaneous Traffic Sign Distinguishing proof and Cutoff Evaluation Using Convolutional Mind Association," in IEEE Trades on Astute Transportation Structures, vol. 19, no. 5, pp. 1652-1663, May 2018, doi: 10.1109/TITS.2018.2801560.
28. R. Qian, Y. Yue, F. Coenen and B. Zhang, "Traffic sign affirmation with convolutional mind network considering max pooling positions," 2016 twelfth Worldwide Gathering on Normal Estimation, Cushy Structures and Data Divulgence (ICNC-FSKD), Changsha, China, 2016, pp. 578-582, doi: 10.1109/FSKD.2016.7603237.
29. A. Pon, O. Adrienko, A. Harakeh and S. L. Waslander, "A Different evened out Significant Designing and More modest than typical pack Assurance Procedure for Joint Traffic Sign and Light Disclosure," 2018 fifteenth Social

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707242 |

occasion on PC and Robot Vision (CRV), Toronto, ON, Canada, 2018, pp. 102-109, doi: 10.1109/CRV.2018.00024.

30. Saha S., Islam M.S., Khaled M.A.B., Tairin S. (2019) A Successful Traffic Sign Affirmation Approach Using a Shrewd Significant Cerebrum Association Decision Plan. In: Abraham A., Dutta P., Mandal J., Bhattacharya A., Dutta S. (eds) Emerging Progressions in Data Mining and Information Security. Advances in Shrewd Structures and Enrolling, vol 814. Springer, Singapore. https://doi.org/10.1007/978-981-13-1501-5_74
31. A. Welzel, A. Auerswald and G. Wanielik, "Accurate camera-based traffic sign limitation," seventeenth Worldwide IEEE Social event on Shrewd Transportation Structures (ITSC), Qingdao, China, 2014, pp. 445-450, doi: 10.1109/ITSC.2014.6957730.
32. M. Karaduman and H. Eren, "Deep learning-based traffic direction sign detection and determining driving style," 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 2017, pp. 1046-1050, doi: 10.1109/UBMK.2017.8093453.
33. E. Winarno, W. Hadikurniawati and R. N. Rosso, "Location based service for presence system using haversine method," 2017 International Conference on Innovative and Creative Information Technology (ICITech), Salatiga, Indonesia, 2017, pp. 1-4, doi: 10.1109/INNOCIT.2017.8319153.
34. Pal R, Ghosh A, Kumar R, et al. public health crisis of road traffic accidents in India: Risk factor assessment and recommendations on prevention on the behalf of the Academy of Family Physicians of India. J Family Med Prim Care.2019;8(3):775-783. doi: 10.4103/jfmpc.jfmpc_214_18

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com