International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 07 | July - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Long Distance Attention-Based on the Fake Footage Detection

[1] SPOORTHI B M, [2] SHRUTHI M T

[1]Assistant Professor , Department of MCA ,BIET, Davangere
[2]Student, Department of Master of Computer Applications, BIET, Davangere

ABSTRACT

Over the span of late numerous years, quick headway in PC based knowledge, simulated intelligence, and significant learning has achieved new strategies and different devices for controlling sight and sound. Anyway the development has been generally used in true applications, for instance, for entertainment and tutoring, etc, malignant clients enjoy furthermore taken benefit of them for unlawful or detestable purposes. For example, first class and reasonable fake accounts, pictures, or sounds have been made to spread duplicity and declaration, incite political disunity and scorn, or even hassle and blackmail people. The controlled, first class and sensible accounts have become alluded to actually as Deep fake. Various approaches have since been depicted in the composition to deal with the issues raised by Deepfake. To give a revived blueprint of the assessment works in Deepfake area, we lead a precise composing overview (SLR) in this paper, summarizing 112 critical articles from 2018 to 2020 that presented various methods. We separate them by social event them into four one of a kind orders: significant learning- based techniques, old style man-made intelligence based methodologies, statistical techniques, and blockchain-based systems. We furthermore survey the introduction of the ID capacity of the various methods with respect to different datasets and assume that the significant learning-based methodologies beat various procedures in Deepfake acknowledgment. Keywords : manipulating multimedia, legitimate applications.

1. INTRODUCTION

The notable advances in artificial neural network (ANN) based technologies play an essential role in tampering with multimedia content. For example, AI-enabled software tools like Face App [1], and Fake App [2] have been used for realistic-looking face swapping in images and videos. 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, Deep fake. 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 word was named after an anonymous Redd it user in late 2017, who applied deep learning methods for replacing a person's face in pornographic videos using another person's face and created photo-realistic fake videos. To generate such counterfeit videos, two neural networks: (i) a generative network and (ii) a discriminative network with a Face Swap technique were used [3], [4]. The generative network creates fake images using an encoder and a decoder. The discriminative network defines the authenticity of the newly generated images. The combination of these two networks is called Generative Adversarial Networks (GANs), proposed by Ian Good fellow . Based on a yearly report [6] in Deep fake, DL researchers made several related breakthroughs in generative modeling. 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] to transform images and videos into different styles. Another group of scholars from the University of Washington proposed a method to synchronize the lip movement in video with a speech from another source [9]. Finally, in November 2017, the term Deep fake" emerged for sharing porn videos, in which celebrities' faces were swapped with the original ones. In January 2018, a Deepfake creation service was launched by various websites based on some 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. Rossler et al. introduced a vast video dataset to train the media forensic and Deep fake detection tools called Face Forensic [11] in March 2018. After a month, researchers at Stanford University published a method, Deep video portraits" [12] that enables photo-realistic re- animation of portrait videos. UC Berkeley researchers developed another approach [13] for transferring a person's body movements to another person in the video. NVIDIA introduced a style-based generator architecture for GANs [14] for synthetic image generation. According to [6] report, Google search engine could find multiple web pages that contain Deep fake related videos (see Figure 1).We found the following additional information from this report [6]:

_ The top 10 pornographic platforms posted 1,790C Deep fake videos, without concerning pornhub.com, which has removed 'Deep fakes' searches.

_ Adult pages post 6,174 Deep fake videos with fake video content.

_ 3 New platforms were devoted to distributing Deep fake pornography.

_ In 2018, 902 articles were published in arXiv, including the keyword GAN either in titles or abstracts.

_ 25 Papers published on this subject, including non-peer reviews, are investigated, and DARPA funded 12 of them. 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. To address such threats, the field of Deep fake detection has attracted considerable attention from academics and experts during the last few years, resulting in many Deep fake detection techniques. There are also some efforts on surveying selected literature focusing on either detection methods or performance analysis. However, a more comprehensive overview of this research area will be beneficial in serving the community of researchers and practitioners by providing summarized information about Deep fake in all aspects, including available datasets, which are noticeably missing in previous surveys. Toward that end, we present a systematic literature review (SLR) on Deep fake detection in this paper. We aim to describe and analyze common grounds and the diversity of approaches in current practices on Deep fake

detection. Our contributions are summarized as follows:

We perform a comprehensive survey on existing literature in the Deep fake domain. We report current tools, techniques, and datasets for Deep fake detection-related research by posing some research questions. We introduce a taxonomy that classifies Deep fake 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 Deep fake detection methods using different measurement metrics. We highlight a few observations and deliver some guidelines on

Deep fake detection that might help future research and practices in this spectrum. The remainder of the paper is organized as follows: Section II presents the review procedure by defining interest research questions. In Section III, we thoroughly discuss the findings from different studies. Section IV summarizes the overall observations of the study, and we present the challenges and limitations in Section V. Finally, Section VI concludes the paper.

2. LITERATURE REVIEW

II. RELATED This paper explores the efficacy of attention mechanisms, particularly long-distance attention, in detecting deepfake videos. The authors review various 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 analyzing the strengths 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 concludes that these methods 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 use 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 findings underscore the effectiveness of these methods in distinguishing authentic videos from deepfakes.

3. MODULE DESCRIPTION

3.1 MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as

Login, Train & Test Data Sets, View Videos Datasets Trained and Tested Accuracy in Bar Chart,

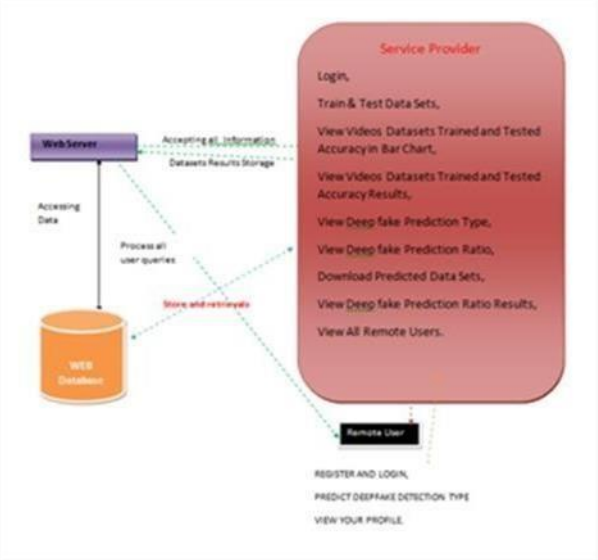
View Videos Datasets Trained and Tested Accuracy Results, View Deep fake Prediction Type, View Deep fake Prediction Ratio, Download Predicted Data Sets, View Deep fake Prediction Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT DEEPFAKE DETECTION TYPE,VIEW YOUR PROFILE.



4. METHODOLGY

Dataset Preparation:

Selection of datasets containing both real and deepfake videos. Preprocessing steps l like frame extraction, alignment and normalization.

Feature Extraction:

Extracting relevant features from frames or sequences.

Use of techniques such as CNNs (Convolutional Neural Networks) for image-based features and RNNs (Recurrent Neural Networks) or transformer for sequence-based features.

Long Distance Attention Mechanism:

Explanation of how long-distance attention is applied to the feature extraction process.

Integration of attention mechanisms (possibly self-attention or other variants) to capture dependencies across frames or sequences that span longer distances.

Classifier Training:

Training a classifier (could be CNNs, RNNs, transformers, or a combination) on the extracted features. Supervised learning approach where labels indicate whether a video is real or a deepfake.

Attention Mechanisms:

Description of the specific attention mechanisms used, possibly Transformer-based architectures like BERT or similar models adapted for video analysis.

Focus on how these mechanisms help in capturing long-range dependencies crucial for identifying inconsistencies in deepfake videos.

Deep Learning Models:

Detailed explanation of the deep learning architectures employed (CNNs, RNNs, Transformers). Modifications or adaptations made to these models to suit the task of deepfake detection.

Loss Functions and Optimization:

Specification of the loss functions used during training (e.g., binary cross- entropy).

Optimization techniques like stochastic gradient descent (SGD), Adam, or variants that are effective for training deep neural networks.

Evaluation Performance Metrics:

Metrics used to evaluate the model's performance, such as accuracy, precision, recall, and possibly area under the ROC curve (AUC).

Comparison with existing methods or benchmarks to demonstrate the effectiveness of the proposed approach.

5. RESULTS

This systematic literature review (SLR) 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.

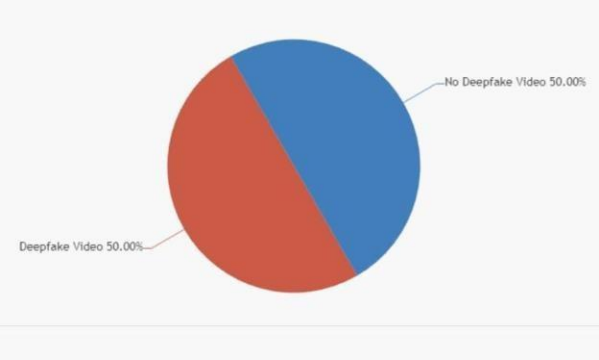
- The FF++ dataset is the most frequently employed in experiments.

- Convolutional Neural Network (CNN)

models constitute a significant portion of the detection models.

- Detection accuracy is the most commonly used performance metric.

- 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.



6. CONCLUSION

This systematic literature review (SLR) provides a comprehensive analysis of the latest methods for detecting deepfakes, examining 112 studies from early 2018 to late 2020. It reveals that deep learning approaches, especially Convolutional Neural Networks (CNNs), are the most commonly used techniques for detecting deepfakes, with the FF++ dataset being the most frequently utilized. Detection accuracy is highlighted as the primary performance metric. The experimental findings demonstrate that deep learning techniques are highly effective and generally surpass non-deep learning models in performance. However, deepfake detection continues to be a challenging task due to the fast-paced advancements in technology and the widespread availability of deepfake tools. This SLR is a valuable resource for researchers, offering insights to develop more effective detection methods and countermeasures against deepfakes.

7. REFERENCE

[1] Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu,

D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative Adversarial Nets,” in Advances in Neural Information Processing Systems, vol. 27, Montreal, CANADA, 2014.

[2] D. P. Kingma and M. Welling, “Auto-Encoding Variational Bayes,” 2014.

[3] T. Karras, T. Aila, S. Laine, and J. Lehtinen, “Progressive Growing of GANs for Improved Quality, Stability, and Variation,” in International Conference on Learning Representations, Vancouver, Canada, 2018.

[4] Q. Duan and L. Zhang, "Look More Into Occlusion: Realistic Face Frontalization and Recognition With BoostGAN," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 1, pp. 214–228, 2021.

[5] "deepfake" http://www.github.com/ deepfakes/ Accessed September 18, 2019.

[6] "fakeapp," http://www.fakeapp.com/ Accessed February 20, 2020.

[7] "faceswap" http://www.github.com /MarekKowalski/ Accessed September 30, 2019.

[8] F. Matern, C. Riess, and M. Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations," in IEEE Winter Applications of Computer Vision Workshops, Waikoloa, USA, 2019, pp. 83–92.

[9] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "Mesonet: a Compact Facial Video Forgery Detection Network," in IEEE International Workshop on Information Forensics and Security, Hong Kong, China, 2018, pp. 1–7.

[10] X. Yang, Y. Li, H. Qi, and S. Lyu, "Exposing GAN-Synthesized Faces Using Landmark Locations," in Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 2019, p. 113–118.

[11] D.-T. Dang-Nguyen, G. Boato, and F. G. De Natale, "Discrimination between computer generated and natural human faces based on asymmetry information," in Proceedings of the 20th European Signal Processing Conference, Bucharest, Romania, 2012, pp. 1234–1238.

[12] E. Sabir, J. Cheng, A. Jaiswal, W. AbdAlmageed, I. Masi, and P. Natarajan, "Recurrent Convolutional Strategies for Face Manipulation Detection in Videos," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Los Angeles, USA, June 2019.

[13] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Two-Stream Neural Networks for Tampered Face Detection," in IEEE Conference on Computer Vision and Pattern Recognition Workshops, Honolulu, USA, 2017, pp. 1831–1839.