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.2024.0707137 |

Detection of Deepfake Videos using Long Distance Attention

Adil Pasha T A[1], Praveen K S[2]

Student, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: With the rapid progress of deepfake techniques in recent years, facial video forgery can generate highly deceptive video contents and bring severe security threats. And detection of such forgery videos is much more urgent and challenging. Most existing detection methods treat the problem as a vanilla binary classification problem. In this paper, the problem is treated as a special fine-grained classification problem since the differences between fake and real faces are very subtle. It is observed that most existing face forgery methods left some common artifacts in the spatial domain and time domain, including generative defects in the spatial domain and inter-frame inconsistencies in the time domain. And a spatial-temporal model is proposed which has two components for capturing spatial and temporal forgery traces in global perspective respectively. The two components are designed using a novel long distance attention mechanism. The one component of the spatial domain is used to capture artifacts in a single frame, and the other component of the time domain is used to capture artifacts in consecutive frames. They generate attention maps in the form of patches. The attention method has a broader vision which contributes to better assembling global information and extracting local statistic information. Finally, the attention maps are used to guide the network to focus on pivotal parts of the face, just like other fine-grained classification methods. The experimental results on different public datasets demonstrate that the proposed method achieves the state-of the- art performance, and the proposed long distance attention method can effectively capture pivotal parts for face forgery.

KEY WORDS: Automation, real-time updates, inventory management, transaction processing, customer and supplier relations, user accounts, advanced analytics, integration, scalability, security, user-friendly interface

I. INTRODUCTION

A Digital Twin is a real-time digital replica of a physical system that accurately reflects its features. The DT environment involves the formation of a clone of the tangible object to perform simulations in the virtual space. Grieves and Vickers [1] first proposed the idea of performing simulations with a clone in a virtual environment in 2002, and National Aeronautics and Space Administration (NASA) in 2010 referred to the method as a DT [2]. The DT concept was developed to make it possible to reap the benefits of paradigms like Industry 4.0 and the industrial Internet of Things (IIOT). The idea is to make every product or process-related data source and control interface description accessible through a single interface for automatic communication establishment and auto-discovery. Without specific knowledge of each component, developers and engineers can determine, design, and construct the required interfaces, integrations, and communication links by analyzing the DTs of the incorporated components [3]. The devices may eventually be able to locate and communicate with one another without the need for a human engineer to stand in between them. With the assistance of DTs, this kind of auto-discovery and auto-established communication may eventually make IOT more scalable for currently unimaginable applications. The numerous fields in which DT technology is being studied are manufacturing, construction, healthcare, and space industries. IOT and mobile devices have recently been added to the DT technology’s application range. For instance, autonomous driving can be achieved in a vehicular environment, and precise and detailed remote medical treatment can be carried out in a medical environment.

The proposal system's goals include:

- 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 highlight a few observations and deliver some guidelines on Deepfake detection that might help future research and practices in this spectrum
- 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.

II. LITERATURE SURVEY

In [22], the consistency of the biological signs are measured along with the spatial and temporal [23]_[25] directions to use various landmark [26] points of the face (e.g., eyes, nose, mouth, etc.) as unique features for authenticating the legitimacy of GANs generated videos or images. Similar characteristics are also visible in Deepfake videos, which can be discovered by approximating the 3D head pose [27]. In most cases, facial expressions are associated initially with the head's movements. Habeeba et al. [88] applied MLP to detect Deepfake video with very little computing power by exploiting visual artifacts in the face region. As far as the performance concern in machine learning based Deepfake methods, it is observed that these approaches can achieve up to 98% accuracy in detecting Deepfakes. However, the performance entirely relies on the type of dataset, the selected features, and the alignment between the train and test sets. The study can obtain a higher result when the experiment uses a similar dataset by splitting it into a certain level of ratio, for example, 80% for a train set and 20% for a test set. The unrelated dataset drops the performance close to 50%, which is an arbitrary assumption. Zhang et al. [33] introduced a GAN simulator that replicates collective GAN-image artifacts and feeds them as input to a classifier to identify them as Deepfake. Zhou et al. [34] proposed a network for extracting the standard features from RGB data, while [35] proposed a similar but generic resolution. Besides, in [36]_[38], researchers proposed a new detection framework based on physiological measurement, for example, Heartbeat. At first, the deep learning-based method was proposed in [40] 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 [41].

Existing System

In [22], the consistency of the biological signs are measured along with the spatial and temporal [23]_[25] directions to use various landmark [26] points of the face (e.g., eyes, nose, mouth, etc.) as unique features for authenticating the legitimacy of GANs generated videos or images. Similar characteristics are also visible in Deepfake videos, which can be discovered by approximating the 3D head pose [27]. In most cases, facial expressions are associated initially with the head's movements. Habeeba et al. [88] applied MLP to detect Deepfake video with very little computing power by exploiting visual artifacts in the face region. As far as the performance concern in machine learning based Deepfake methods, it is observed that these approaches can achieve up to 98% accuracy in detecting Deepfakes. However, the performance entirely relies on the type of dataset, the selected features, and the alignment between the train and test sets. The study can obtain a higher result when the experiment uses a similar dataset by splitting it into a certain level of ratio, for example, 80% for a train set and 20% for a test set. The unrelated dataset drops the performance close to 50%, which is an arbitrary assumption. Zhang et al. [33] introduced a GAN simulator that replicates collective GAN-image artifacts and feeds them as input to a classifier to identify them as Deepfake. Zhou et al. [34] proposed a network for extracting the standard features from RGB data, while [35] proposed a similar but generic resolution. Besides, in [36]_[38], researchers proposed a new detection framework based on physiological measurement, for example, Heartbeat. At first, the deep learning-based method was proposed in [40] 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 [41].

Proposed System

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. We highlight a few observations and deliver some guidelines on Deepfake detection that might help future research and practices in this spectrum.

III. SYSTEM DESIGN

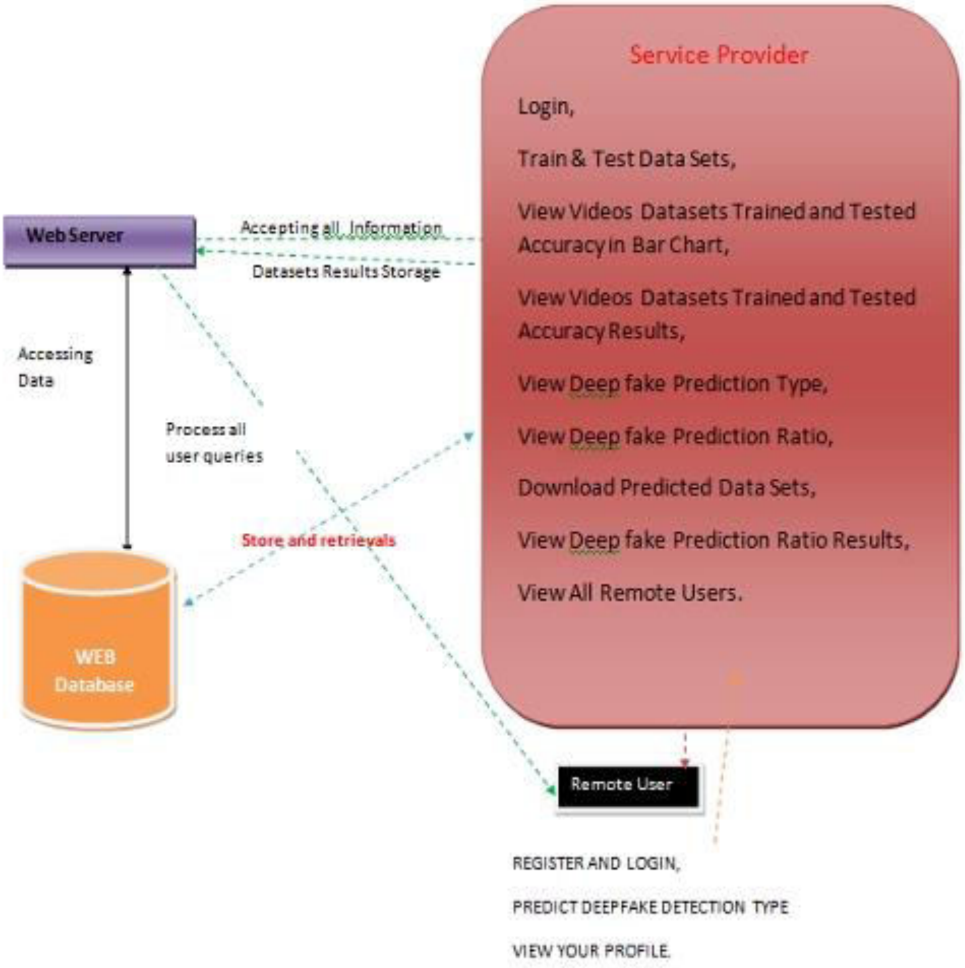
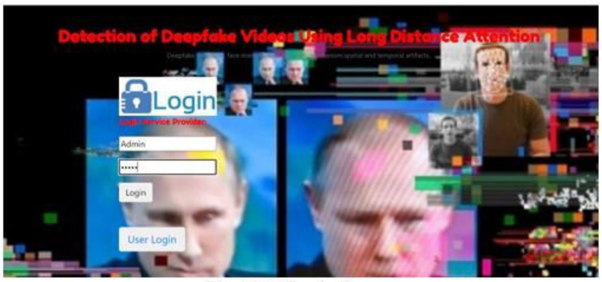

Service Provider
Login,
Train & Test Data Sets,
View Videos Datasets Trained and Tested Accuracy in Bar Chart,
View Videos Datasets Trained and Tested Accuracy Results,
View Deep fake Prediction Type,
View Deep fake Prediction Ratio,
Download Predicted Data Sets,
View Deep fake Prediction Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT DEEPFAKE DETECTION TYPE
VIEW YOUR PROFILE.

Figure 1: System Architecture

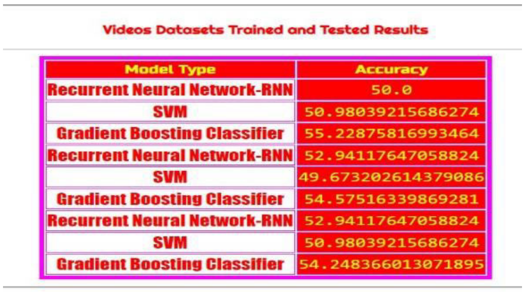
IV. RESULTS AND OUTCOMES

Implementation

Screen Shots



Login Page



Videos Datasets Trained and Tested Results

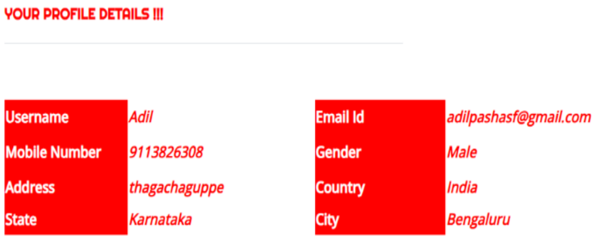
Model Type	Accuracy
Recurrent Neural Network-RNN	50.0
SVM	50.98039215686274
Gradient Boosting Classifier	55.22875816993464
Recurrent Neural Network-RNN	52.94117647058824
SVM	49.673202614379086
Gradient Boosting Classifier	54.57516339869281
Recurrent Neural Network-RNN	52.94117647058824
SVM	50.98039215686274
Gradient Boosting Classifier	54.248366013071895

Test result

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

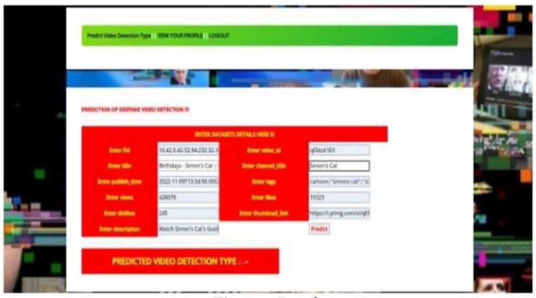
| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707137 |



YOUR PROFILE DETAILS !!!

Username	Adil	Email Id	adilpashasf@gmail.com
Mobile Number	9113826308	Gender	Male
Address	thagachaguppe	Country	India
State	Karnataka	City	Bengaluru



PREDICTION OF DEEFAKE VIDEO DETECTION !!!

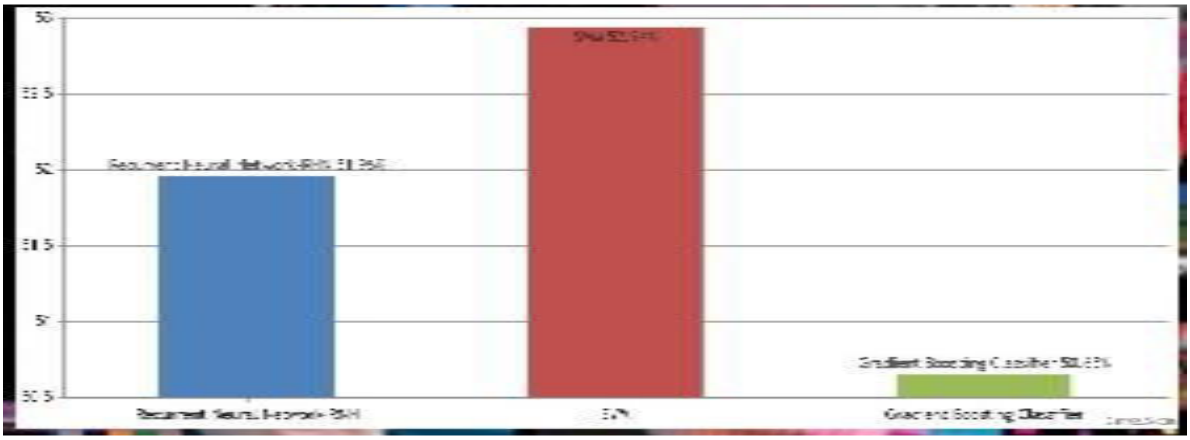
ENTER DATASETS DETAILS HERE !!

Enter Fid	10.42.0.42-52.94.232.32-1	Enter video_id	qEltozt1El
Enter title	Birthdays - Simon's Cat		Enter channel_title	Simon's Cat
Enter publish_time	2022-11-09T13:34:58.000	Enter tags	cartoon|"simons cat"|"si
Enter views	426078	Enter likes	19323
Enter dislikes	245	Enter thumbnail_link	https://i.ytimg.com/vi/qEl
Enter description	Watch Simon's Cat's Guid		Predict

PREDICTED VIDEO DETECTION TYPE : -->

Profile detail

Result



Bar Chart

V. CONCLUSION

This SLR presents various state-of-the-art methods for detecting Deep fake published in 112 studies from the beginning of 2018 to the end of 2020. We present basic techniques and discuss different detection models' efficacy in this work. We summarize the overall study as follows:
_ The deep learning-based methods are widely used in detecting Deep fake.
_ In the experiments, the FF++ dataset occupies the largest proportion.
_ The deep learning (mainly CNN) models hold a significant percentage of all the models.
_ The most widely used performance metric is detection accuracy.
_ The experimental results demonstrate that deep learning techniques are effective in detecting
Deep fake. Further, it can be stated that, in general, the deep learning models outperform the non-deep learning models. With the rapid progress in underlying multimedia technology and the proliferation of tools and applications, Deep fake detection still faces many challenges. We hope this SLR provides a valuable resource for the research community in developing effective detection methods and countermeasures.

REFERENCES

[1] FaceApp. Accessed: Jan. 4, 2021. [Online]. Available: https://www. faceapp.com/
[2] FakeApp. Accessed: Jan. 4, 2021. [Online]. Available: https://www. fakeapp.org/
[3] Oberoi. Exploring DeepFakes. Accessed: Jan. 4, 2021. [Online]. Available:https://goberoi.com/exploring-deepfakes-20c9947c22d9
[4] J. Hui. How Deep Learning Fakes Videos (Deepfake) and How to Detect it. Accessed:Jan. 4, 2021. [Online]. Available: https://medium. com/how-deep-learning-fakes-videosdeepfakes and-how-to-detect-itc0b50fbf7cb9
[5] I. Goodfellow, J. P. Abadie, M. Mirza, B. Xu, D. W. Farley, S. Ozair, A. Courville, and Y.Bengio, ``Generative adversarial nets," in Proc. 27th Int. Conf. Neural Inf. Process. Syst.(NIPS), vol. 2. Cambridge, MA, USA: MIT Press, 2014, pp. 2672_2680.

[6] G. Patrini, F. Cavalli, and H. Ajder, ``The state of deepfakes: Reality under attack,'' Deeptrace B.V., Amsterdam, The Netherlands, Annu. Rep. v.2.3., 2018. [Online]. Available: https://s3.eu-west- 2.amazonaws.com/rep2018/2018-the-state-of-deepfakes.pdf

[7] J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Niessner, ``Face2Face: Real-time face capture and reenactment of RGB videos,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016, pp. 2387_2395, doi: 10.1109/CVPR.2016.262.

[8] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, ``Unpaired image-to-image translation using cycle-consistent adversarial networks,'' in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Venice, Oct. 2017, pp. 2242_2251, doi: 10.1109/ICCV.2017.244.

[9] S. Suwajanakorn, S. M. Seitz, and I. K. Shlizerman, ``Synthesizing Obama: Learning lip sync from audio,'' ACM Trans. Graph., vol. 36, no. 4, p. 95, 2017.

[10] L. Matsakis. Arti_cial Intelligence is Now Fighting Fake Porn. Accessed: Jan. 4, 2021. [Online]. Available: https://www.wired.com/story/gfycatarti _cial-intelligence-deepfakes/

INNO SPACE
SJIF Scientific Journal Impact Factor

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com