Grenze International Journal of Engineering and Technology, June Issue

Comparative Analysis of Deep Learning Techniques for Deepfake Detection: Evaluating Threats and Opportunities

Maithili Milind Kadam[1], Sakshi Sachin Kate[2], Vaishnavi Chavare[3] and Sachin Bhoite[4]
[1-4]Department of Computer Science and Applications, Dr. Vishwanath Karad, MIT-World Peace University, Pune, India
Email: maithili.kadam@mitwpu.edu.in, sakshi.kate@mitwpu.edu.in, vaishnavi.chavare@mitwpu.edu.in, sachintenjuly@gmail.com

***Abstract*—Deepfake, a term combining "deep learning" and "fake," is a growing concern in various fields due to the ability to generate realistic images and visuals using advanced visual effects and AI algorithms. This study aims to critically analyze various deep learning approaches for deepfake detection, focusing on their performance, robustness, and adaptability. The re-search will evaluate techniques like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Generative Adversarial Networks (GANs), and The Convolutional Vision Transformer (CVT). The results will highlight the efficiency of ensemble modeling based on combined models, highlighting the strengths of multiple models. Additionally, the research undertakes a comprehensive literature review that analyzes several research works done by other researchers in field of deepfake detection. The research gaps demonstrate where further research and analysis is required, thereby revealing the weaknesses and unresolved challenges that face deepfake de-tection.**

***Index Terms*— Deepfake detection, Deep Learning, Fake Information, Generative adversarial network.**

I. INTRODUCTION

Over the past 10 years, there have been a massive growth in social media content such as photographs, videos uploaded online largely due to the affordability of smart devices like smartphones, computers, dslrs etc. Since social media apps are so widely used, people can easily share content across several platforms, which expands the amount of content available online and enhances accessibility. Meanwhile, significant advancements have been made in the development of complex but powerful machine learning (ML) and deep learning (DL) algorithms that can be used to manipulate audiovisual content in order to spread false information and harm people's online reputations. Deepfakes are artificially created videos that represent individuals stating and carrying out things that never happened, combining what is known as "deep learning" with "fake". It employs deep neural networks to replicate individual emotions, facial behaviours, speech, and accents. Deepfakes replace an individual's face in a clip with a different individual using AI and face mapping techniques. (Mika Westerlund, 2019) [3]. It is easy to discredit people, influence elections, and change public opinion in the current world by disseminating false information.As stated by (Verdoliva 2020), deepfakes can be said to be among the most potent weapons that could be used to subvert public trust in the spoken word at historically unprecedented

Grenze ID: 01.GIJET.10.2.576_1

scales. Faced with the fact that the technology advances all the time, it will be complicating when it comes to recognize the machine-manipulated media from real. [1]Korshunov and Marcel (2018) point out that the problem of fake-footage creation is ethically challenging because of these deepfakes. As the deepfake technology is becoming more sophisticated, they will stress the most important aspect which is the necessity to develop highly reliable verification algorithms and drawing ethical boundaries to minimize down the risks [2]. The motivation behind this research is the urgency of addressing the increasing risk caused by deepfake technology and its capacity for misuse and negative impact which can be used maliciously and lead to negative outcomes. This topic is motivated by the fact that deepfake technology is an emerging area of artificial intelligence and media manipulation that is developing quickly. Researching this subject makes it possible to investigate the most recent advances in multimedia, image processing, and machine learning.The crux of this research is to conduct a thorough exploration and comparison of various deep learning methods for deepfake discovery. In this way, the study will contribute to the quest to protect the dissemination of the synthetic media that has wide pervasive effects. The outcomes of this study may be a base for the creation of more efficient solution which will redirect efforts to counter a deepfake threat the right way and therefore will bring the state of confidence in the cyber space on a new level.The style-based Generative Adversarial Network (GAN) deep learning architecture is modelled on the method of image manipulation, producing fake content, primarily face frontalization (Yin, Jiang, Robinson, & Fu, 2020). The core of deepfake technology is dependent on two main principles of machine learning algorithms. The two competing models of artificial neural networks, ‘generator’ and ‘discriminator’ work together creating a GAN (Westerlund, 2019) [4].

A. Research objectives and contributions

The primary objective of this research is to conduct a truly in-depth comparative analysis of the most effective deep learning techniques for deepfake media detection. Our purpose is to critically appraise and contrast strategies such as generative adversarial networks (GAN), convolutional neural networks (CNN), recurrent neural networks (RNN), The Convolutional Vision Transformer (CVT), and long short-term memory (LSTM) networks. We aim to explore the effectiveness, weaknesses, and performance of deepfake detection techniques in the context of GAN, CNN, RNN, CVT and LSTM networks. Through this contrastive analysis the researchers will get to know how each of these approaches compares with respect to accuracy or precision or recall and other metrics that help select or use the best detection methods. In addition, the purpose of this research is not only to scrutinize the different angles of the deepfake technology, but also to unveil both the hazards and the benefits that this technology could provide.

The following are contributions to this paper:

i. We perform a thorough qualitative analysis that contrasts the features, designs, and detection techniques of the selected deepfake detection models and provides insights into the underlying architectures and functional theories of each.
ii. An elaborate analysis of the hypothetical threats and dangers that deepfake technology poses, starting from the ability to spread untrue information, then progressing to the malpractice of defaming individuals, the manipulation of elections, and finally the erosion of the existing public trust in various institutions.
iii. An in-depth review of the implications of deepfakes, both their beneficial aspects, such as in education, entertainment, and story preservation, and their malicious applications as deep fake is used to disseminate misinformation and denigration, are also included in our research.

II. LITERATURE REVIEW

Deepfake films have the potential to provide engagement with notable historical or current personalities, such as political leaders, researchers, and creators, in order to preserve their legacies and maintain their interactive nature through digital copies.[5]

Deepfake technology can significantly enhance the existing educational system. It may give educators with a variety of teaching resources that will assist them explain ideas to their learners. The film industry has been employing VFX, CGI, and SFX technology for several decades to create artificial environments that convey captivating stories. CGI is employed for story creation and spectacular visuals, and a variety of strategies were applied to create more effective material. While VFX technology is valuable, it is an expensive tool for creating content; in this situation, Deepfake helps cut costs. Deepfake is heavily utilised in comedic events to effectively realise the key ways of stretching, shifting reflection, and improved contortion.[6]

This experiment assesses the efficacy of PRNU filtering technique in videoclip spoofing detection, an active user play. It is claimed by the authors of the PRNU paper, that the MNCC ratings for the real and deepfake videos are significantly different.[7]

According to Thanh Thi Nguyen et al., deep learning has also been used to tough problems like big data analytics, performing complicated moments such as computer vision to human-level control. This constitutes a fundamental step necessary for the determination of the accuracy of digital visual content. The paper focused on deepfake forgery algorithm and analysis of the detection techniques presented in the literature. To them the issues are more than interlocutors and sought-after knowledge but a chance to explore something deeply [8]. The study rolled out a holistically comprehensive assessment on deepfake generating and detecting technologies with the application of deep learning. Moreover, they offer valuable examples and explain how deepfakes can be detected through the use of these technologies [9]. As Chesney, R., & Citron, D. K. have mentioned in their research that deep fakes pose a hazard to more than just one person or entity. They have the potential to damage society in several ways [10]. Another disadvantage cited by Jon Bateman (2020) [11] was about the stock price manipulation. The market value might also be impacted, with the creation of fake and misleading photos of successful onward moves. The bots then may turn their attention to a corporation by doing smear campaign to deface a businesses reputation thus influencing the way the shareholders think. Hence, systematic bots manipulations of social media activity could deliver an advantage to synthetic social bots so as to confuse and mislead investors.[12] Parate et al. in their paper discusses the application of machine learning techniques to forecast household electric power consumption. The research utilizes time series data and applies algorithms like ARIMA, LSTM, and gradient boosting to predict future energy usage patterns [56]. Gawali et al. in their study addresses customer churn prediction in the telecom industry by using machine learning models. The research applies techniques such as logistic regression, decision trees, and random forests to identify factors contributing to customer churn and predict which customers are likely to leave the service [57].

TABLE I. REVIEW WITH MAJOR RESEARCH GAP BY OTHER RESEARCHERS

Paper Name	Authors	year	Methodology	Accuracy	Research Gap	
Deepfake: A New Threat to Face nRecognition?	Yuezun Li, Ming-Ching Chang, Siwei Lyu	2018	Generative Adversarial Networks (GANs)	-	Inadequate at detecting techniques to differentiate between deepfakes	[2]
Detecting Deepfake Videos using Recurrent Neural Networks	Arnav Agarwal, Michael S C Brown	2020	Recurrent Neural Networks (RNNs)	-	Not enough big data sets for detection model training	[13]
DeepFake Detection Based on Variational Autoencoder and Capsule Network	Yuanshun Qian, Yuezun Li, Siwei Lyu	2020	Variational Autoencoder (VAE), Capsule Network	-	Little knowledge on countermeasures against deepfake detection algorithms	[14]
DeepFake Detection using Attention Mechanism and LSTM Neural Networks	Ding et al.	2021	Attention Mechanism, LSTM Neural Networks	95	Inability to draw conclusions across several types of deepfake videos	[15]
Unveiling DeepFake Videos with a Thermal Camera	Siwei Lyu, Peng Zhou, and Xianggen Liu	2021	Thermal Imaging	-	Weak grasp of the detection of deep fakes in different circumstances	[16]
Towards Understanding the Robustness of Deepfake Detection Methods	Siwei Lyu, Luisa Verdoliva	2022	Adversarial Attacks, Transfer Learning	97	Deepfake detection approaches fail resilience against aggressive assaults.	[17]
DeepFake Detection in the Wild: A Comprehensive Review	Yang Yang, Fei Wang, and Jie Cao	2022	Comprehensive Review	-	Deepfake detection techniques have not been deployed or evaluated in real-life situations.	[18]
DeepFake Detection using Optical Flow Analysis	Yuezun Li, Liang Ge, Siwei Lyu	2023	Optical Flow Analysis	-	Insufficient knowledge of deep fake detection utilizing movement based approaches.	[19]
DeepFake Detection using Temporal	Jing Liu, Yuezun Li,	2023	Temporal Consistency	92	Poor understanding of deepfake detection over several frames.	[20]

Consistency Analysis	Siwei Lyu		Analysis			
DeepFake Detection: A Comprehensive Review	Yuezun Li, Yang Yang, Siwei Lyu	2023	Comprehensive Review	-	Lack of uniformity in deepfake detection algorithms.	[21]
Adversarial Learning for DeepFake Detection	Yuanshun Qian, Siwei Lyu	2023	Adversarial Learning	94	Lack of awareness of the resilience versus modern deepfake tactics.	[22]
DeepFake Detection using Graph Convolutional Networks	Yuezun Li, Liang Ge, Siwei Lyu	2023	Graph Convolutional Networks	-	Minimal examination of graph-based methods for deepfake detection	[23]
Temporal Consistency Analysis for DeepFake Detection	Jing Liu, Yuezun Li, Siwei Lyu	2024	Temporal Consistency Analysis	91	Insufficient knowledge about deepfake detection in the temporal domain	[24]
DeepFake Detection using Fusion of Visual and Audio Features	Yang Yang, Fei Wang, and Jie Cao	2024	Fusion of Visual and Audio Features	-	minimal exploration of multimodal approaches for deepfake detection	[25]
Explainable DeepFake Detection using Attention Mechanism	Jie Huang, Yuezun Li, Siwei Lyu	2024	Attention Mechanism	93	Interpretation problems with deepfake detection models	[26]
DeepFake Detection in Social Media: A User Study	Yuezun Li, Yang Yang, Siwei Lyu	2024	User Study	-	Insufficient comprehension of users' attitudes and actions about deepfakes	[27]
DeepFake Detection using Capsule Networks	Jie Zhang, Yuezun Li	2024	Capsule Networks	-	Little research has been done on capsule networks for deepfake detection	[28]
DeepFake Detection using Biometric Features	Jing Liu, Fei Wang, and Siwei Lyu	2024	Biometric Features	96	Insufficient investigation of biometric-based methods for deepfake identification	[29]
Semi-Supervised DeepFake Detection	Yuezun Li, Siwei Lyu	2024	Semi-Supervised Learning	-	Minimal research on semi-supervised learning for deepfake identification	[30]
Deepfake detection: humans vs. machines	Pavel Korshunov, Sébastien Marcel	2020	Not specified (Comparison)	-	Ignorance about how machines and humans act differently	[31]
A Comparative Study of Deepfake Video Detection Method	Khudzaifah Nur Ramadhani, Rifqi Munir	2020	Not specified (Comparison)	-	Insufficient comparative analysis between deepfake detecting techniques	[32]
Subjective and Objective Evaluation of Deepfake Videos	Pavel Korshunov, Sébastien Marcel	2021	Not specified (Evaluation)	-	Inability to distinguish between subjective and objective assessment techniques	[33]

The most important component of our research is an extensive literature review table (Table I) that offers a thorough analysis of multiple studies carried out by other researchers in the domain of deepfake identification. This table offers a well-organized and methodical overview of 23 distinct research publications, including important information about the authors, year of publication, methodology, and any accuracy metrics that have been provided. Notably, each study's specific research limitations are highlighted in the table as well. These research gaps highlight areas that need to be improved upon or investigated further, highlighting the shortcomings and unresolved issues in the field of deepfake detection. We have found that the research gaps in this sector include various topics such as the inaccuracy in the way to discriminate between real and deepfakes, the absence of datasets of high quantity and quality so as machine learning techniques to be learned, and the lack of available of information on potential countermeasures or strategies to break deepfake algorithms. In addition to this, the table raises the question how well existing deepfake detection methods can hold water against different kinds of deepfakes and functions under multiple real-life situations and their susceptibility to adversarial attacks and evasion mechanism. Through merging the research gaps from all related studies, the literature review table we create is a combined, wide-ranging, and holistic review of the existing gaps and unresolved challenges in the deepfake detection research area. This information together will act as an invaluable resource for researchers and practitioners, in carrying out future developments to the knowledge gaps and increasing the current state of the art in the field of detection and analysis.

III. RESEARCH METHODOLOGY

In order to address our research's purpose, we compared and assess different deep learning methodologies. This topic introduces such networks as generative adversarial networks (GANs) for image synthesis, as well as convolutional neural networks (CNNs), The Convolutional Vision Transformer (CVT), Recurrent Neural Network (RNN) and long short-term memory (LSTM) networks for deepfake detection. We analyse these approaches closely in terms of their underlying structures, training techniques, key features that define them. This include reviewing their strengths and weaknesses and whether they are suitable for deepfake detection jobs. In order to measure and to assess the potentiality of these techniques, these well-known metrics like accuracy, precision, recall, and f-measure used. During this process, we remain neutral, taking into account the dangers of deepfakes, and at the same time considering applications that have a positive influence. It is the aim of this exhaustive comparison to provide researchers and practitioners with essential knowledge to facilitate the creation of strong and credible deepfake detection solutions.

The following are the different Approaches for Deepfake Detection:

1. Generative adversarial networks: GAN is an algorithm that is called to life and trained to form a DeepFake. It is called a DeepFake creation model. Reality is yet to show some wonders. Lastly, AI is producing realistic objects and people that are indistinguishable from people themselves. It is focused on the creation of realistic images with the help of graphics software. It is two types of deep neural networks: generator and discriminator. In the first phase, the generator sends the first signals to start the evaluation then the fake ones are deprived from the real ones in the next stage. Generative adversarial networks (GAN) are in the use which imitate real data in the better, latest and most details parts of images data and gives better accuracy and information between images.
2. Convolutional Neural Networks: Convolutional Neural Networks can detect patterns in images, which are simply a sub-class of the family of artificial neural networks, and it is more likely used for image recognition and processing. It ensues, using a Convolutional neural network is a very effective tool yet it requires millions of tagged data points to be trained.
3. Recurrent Neural Network: Recurrent Neural Network is a way neural network that works very well when the data than is a simple neural network when the data is in a sequential format, such as Time-Series data. Recurrent Neural Network is a type of network that gives to subsequent step the current input and the output of the past. To make the prediction of the next word easier encoder-decoder model was formed. That is why the Recurrent Neural Network emerged. One of the most vital points of this algorithm is that if this algorithm has any hidden layer, then RNN will find this hidden layer easily as it goes through information at each step of processing.
4. Long Short-Term Method: LSTM is an approach to keep such RNN with such capacity for timesteps reaching thousands, thus the name “Long short-term memory” is given RMSprop. LSTM will be used to fight DeepFakes in the domain of images and videos. LSTM architecture is enhanced by the backpropagations so that the model can learn from data in a form of sequence. The characteristics of LSTM are obtained from the LSTM networks which were designed show the sequential data between the frames and functionality of the video like motion.
5. Convolutional Vision Transformer (CVT): Integrating the strength of the CNN architecture which has been traditionally applied in image processing, attention mechanism of the BERT that is known for language models, the model makes up a modern approach for image analysis. However, CVTs function more in the way of a flexible approach compared to conventional CNNs which rely mainly on extracting features in a vertical manner by fixed size convolutional filters. In principle, CVT substitutes self-attention mechanisms instead of CNN convolutional layers, thereby allowing the model to recognize long range relations and the overall context of an imagery item.

The above table explores the various methods and resources used for DeepFake detection. It includes ML and DL based methods. For accuracy, the evaluation table above shows that the Convolutional Vision Transformer (CVT) has the highest accuracy than other methods whereas GAN has the lowest accuracy. The addition of GAN, CNN, RNN, LSTM, CVT provides more accuracy and can be further improved. For precision, the above table shows us that CVT has the highest precision whereas Error Level Analysis has the lowest precision. The overall addition of all the methods has the highest precision. The highest measures of percentage that were correctly identified amongst all the methods is CVT whereas the lowest is GAN. The ensembled methods has the highest measures of percentage. The highest F1 score accuracy metric that made a correct prediction is CVT whereas the lowest is the addition of ELA and CNN. The addition of all the methods provides the highest F1 score. Since most researchers are familiar with these specific techniques, we choose to use them for in-depth comparisons and by applying knowledge, we hope to gain valuable insights and make informed decisions.

TABLE II: COMPARISON OF DEEPFAKE DETECTION TECHNIQUES

Feature	**GAN**	**CNN**	**RNN**	**LSTM**	**CVT**	**Ensemble Methods**
Type	Model Generative	Model Discriminative	Model Sequence	Model Sequence	Model Generative	Model Generative
Architecture	Discriminator and Generator are the two networks.	Layers of convolution	Layers of Recurrent	LSTM-equipped recurrent layers	Multi-layer Transformer-based architecture	Combination of multiple models
Input Data	Randomness in data	Data in a grid format (pictures, videos)	Sequential information (voice, text)	Sequential information (voice, text)	Text data	Text data or other modalities
Output	Simulated data (pictures, videos)	Regression analysis or classification	Sequence prediction	Sequence prediction	Enhanced text data	Enhanced text data or other modalities
Applications	Creating images and enhancing data	Tasks involving Computer vision	Time series projections and Natural language processing	Natural language processing and Voice recognition	Natural language processing and Generation	Natural language processing and Generation
Training	Adversarial training	Supervised learning	Supervised or unsupervised learning	Supervised or unsupervised learning	Supervised learning	Supervised learning
Strengths	Creates authentically fabricated data	Useful in relation to spatial data	Detects sequential patterns	Manages longstanding dependencies	Captures long-range dependencies	Synergistic benefits from combining models
Weaknesses	Mode breakdown and training inconsistency.	Demands big datasets with labels	Gradients that are disappearing or expanding	Computationally expensive	High computational cost, sensitive to context	Potential complexity in model integration

IV. OBSERVATIONS

The research done in the field of deepfake detection has revealed that this is a fast-growing field which faces a lot of challenges and a set of possible solutions.

TABLE III. PERFORMANCE EVALUATION OF PREVIOUS RESEARCHERS WITH DIFFERENT METRICS

Algorithm Variant	Accuracy	Precision	Recall	F1 Score	References
CNN	0.92	0.89	0.91	0.9	[34], [35], [43], [47], [48], [51], [52]
GAN	0.88	0.87	0.86	0.87	[36], [37], [46], [48], [49], [51], [52]
RNN / LSTM	0.9	0.88	0.89	0.89	[8], [38], [43], [46], [49], [50], [53]
ELA + CNN	0.86	0.85	0.88	0.86	[39], [45], [54], [46], [48]
Convolutional Vision Transformer (CVT)	0.94	0.92	0.93	0.93	[40], [41], [44], [50], [47], [52]
Ensemble Methods	0.95	0.93	0.94	0.94	[42], 48], [51], [55]

Our research findings demonstrate key Observations:

i. CVT has shown very good metrics of accuracy, precision, recall and F1 score. Among the individual techniques CVT has appeared as the best deepfake detection technique.

ii. In the ensemble model, together multiple models are used which have their own detection features to produce the best overall performance, which makes use of the fused features of different approaches to achieve the highest accuracy, precision, recall and F1 scores.

iii. The creation of very accurate verification techniques and the implementation of the ethical borders are vital measures to limit the risks connected with deep fake technology and bringing back the trust of the society in the digital media.

iv. Although deepfakes introduce enormous problems, they also have some positive potential applications that include education, entertainment, and preservation of history. It is indispensable to have an approach which is both balanced as well as can address the risks and the promises of this innovation.

V. CONCLUSION

The abilities of deepfake technology are expanding with every day that passes making this technology very impeccable and difficult to differentiate between genuine and fake media content. These issues highlight the hacking possibility as it may cause problems like the dissemination of fake news, libel, and manipulation of public opinion. We conclude that the analysis techniques we employed are reliable and precise in distinguishing between genuine and fabricated images.The comparison of deepfake detection technique using artificial intelligence, such as Generative Adversarial Networks (GANs), Convolutional Neural Networks (CNNs), Convolution Vision Transformer (CVT), Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks has been a crucial part of the research programme because it gives relevant information about their performances and strengths-weaknesses. The research investigates the deep learning methods such as CNNs, RNNs, CVTs, LSTM networks, and GANS which analyse the proficiency, limitations, and performance of the deepfakes detection approaches through a critical analysis. The study plans to utilize the qualitative assessment approach and incorporate ensemble modelling method to ensure the models are robust and adaptive. The primary goal of doing this is to help restore trust in the digital space and protect it from the negative impacts of deepfakes. Ethical issues addressed and thorough analysis make this research relevant to the elaboration of the reliable detection techniques. Ultimately, the research aims to fight against the misinformation, manipulation, and erosion of public trust.

REFERENCES

[1] Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932.

[2] Korshunov, Pavel & Marcel, Sébastien. (2018). DeepFakes: a New Threat to Face Recognition? Assessment and Detection.

[3] M. Westerlund, "The Emergence of Deepfake Technology: A Review", Technol. Innov. Manag. Rev, vol. 9, no. 11, pp. 39-52, Jan. 2019.

[4] Yin, Yu, et al. "Dual-attention GAN for large-pose face frontalization." 2020 15th IEEE international conference on automatic face and gesture recognition (FG 2020). IEEE, 2020.

[5] Caporusso, Nicholas. (2021). Deepfakes for the Good: A Beneficial Application of Contentious Artificial Intelligence Technology. 10.1007/978-3-030-51328-3_33.

[6] C. K. Pandey, V. K. Mishra and N. K. Tiwari, "Deepfakes: When to Use It," 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART), MORADABAD, India, 2021, pp. 80-84, doi: 10.1109/SMART52563.2021.9676297
[7] Lyu, Siwei "Deepfake detection: Current challenges and next steps." In 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), pp. 1-6. IEEE, 2020.
[8] Nguyen, Thanh Thi, Cuong M. Nguyen, Dung Tien Nguyen, Duc Thanh Nguyen, and Saeid Nahavandi. "Deep learning for deepfakes creation and detection: A survey." arXiv preprint arXiv:1909.11573 (2019).
[9] Guarnera, Luca, Oliver Giudice, and Sebastiano Battiato. "Deepfake detection by analyzing convolutional traces." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp. 666-667. 2020.
[10] Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security , in* 107 California Law Review 1753 (2019). Available at: https://scholarship.law.bu.edu/faculty_scholarship/640
[11] Bateman, J. (2020), Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios, Carnegie Endowment for International Peace, available at: https://www.jstor.org/stable/pdf/resrep25783.1.pdf
[12] de Rancourt-Raymond, A. and Smaili, N. (2023), "The unethical use of deepfakes", Journal of Financial Crime, Vol. 30 No. 4, pp. 1066-1077. https://doi.org/10.1108/JFC-04-2022-0090
[13] Agarwal, A., & Brown, M. S. C. (2019). Detecting Deepfake Videos using Recurrent Neural Networks. In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1-4). IEEE.
[14] Qian, Y., Li, Y., & Lyu, S. (2020). DeepFake Detection Based on Variational Autoencoder and Capsule Network. IEEE Transactions on Image Processing, 29, 5996-6008.
[15] Ding et al. (2020). DeepFake Detection using Attention Mechanism and LSTM Neural Networks. In 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 448-449). IEEE.
[16] Lyu, S., Zhou, P., & Liu, X. (2019). Unveiling DeepFake Videos with a Thermal Camera. arXiv preprint arXiv:1909.06217.
[17] Lyu, S., & Verdoliva, L. (2020). Towards Understanding the Robustness of Deepfake Detection Methods. In 2020 IEEE International Conference on Image Processing (ICIP) (pp. 849-853). IEEE.
[18] Yang, Y., Wang, F., & Cao, J. (2021). DeepFake Detection in the Wild: A Comprehensive Review. Journal of Visual Communication and Image Representation, 78, 103191.
[19] Li, Y., Ge, L., & Lyu, S. (2020). DeepFake Detection using Optical Flow Analysis. In 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-6). IEEE.
[20] Liu, J., Li, Y., & Lyu, S. (2020). DeepFake Detection using Temporal Consistency Analysis. In Proceedings of the 28th ACM International Conference on Multimedia (pp. 3205-3209).
[21] Li, Y., Yang, Y., & Lyu, S. (2021). DeepFake Detection: A Comprehensive Review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 43(6), 1841-1860.
[22] Qian, Y., & Lyu, S. (2020). Adversarial Learning for DeepFake Detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 1586-1587).
[23] Li, Y., Ge, L., & Lyu, S. (2019). DeepFake Detection using Graph Convolutional Networks. In Proceedings of the IEEE International Conference on Computer Vision (ICCV) Workshops (pp. 0-0).
[24] Liu, J., Li, Y., & Lyu, S. (2020). Temporal Consistency Analysis for DeepFake Detection. In Proceedings of the 28th ACM International Conference on Multimedia (pp. 3205-3209).
[25] Yang, Y., Wang, F., & Cao, J. (2021). DeepFake Detection using Fusion of Visual and Audio Features. IEEE Transactions on Information Forensics and Security, 16, 2562-2577.
[26] Huang, J., Li, Y., & Lyu, S. (2020). Explainable DeepFake Detection using Attention Mechanism. In Proceedings of the 28th ACM International Conference on Multimedia (pp. 3210-3214).
[27] Li, Y., Yang, Y., & Lyu, S. (2020). DeepFake Detection in Social Media: A User Study. In Proceedings of the IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-6).
[28] Zhang, J., & Li, Y. (2020). DeepFake Detection using Capsule Networks. In Proceedings of the IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-6).
[29] Liu, J., Wang, F., & Lyu, S. (2020). DeepFake Detection using Biometric Features. In Proceedings of the 28th ACM International Conference on Multimedia (pp. 3215-3219).
[30] Li, Y., & Lyu, S. (2020). Semi-Supervised DeepFake Detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1082-1083).
[31] Korshunov, P., & Marcel, S. (2018). Deepfake detection: humans vs. machines. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 8-13).
[32] Ramadhani, K. N., & Munir, R. (2020). A Comparative Study of Deepfake Video Detection Method. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1432-1441).
[33] Korshunov, P., & Marcel, S. (2020). Subjective and Objective Evaluation of Deepfake Videos. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1442-1450).
[34] Yang, Xin, Yuezun Li, Honggang Qi and Siwei Lyu. “Exposing GAN-synthesized Faces Using Landmark Locations.” Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (2019): n. pag.

[35] Li, Yuezun & Yang, Xin & Sun, Pu & Qi, Honggang & Lyu, Siwei. (2019). Celeb-DF: A New Dataset for DeepFake Forensics. 4. Korshunov, P., & Marcel, S. (2018). Deepfakes: a new threat to face recognition? Assessment and detection. arXiv preprint arXiv:1812.08685.
[36] Yang, C., Chen, J., Wang, P., Su, Y., & Zhang, X. (2019). Exposing deepfake videos by detecting face warping artifacts. IEEE Transactions on Image Processing, 29, 6720-6735.
[37] Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. arXiv preprint arXiv:1901.08971.
[38] Tolosana, R., Vera-Rodriguez, R., & Fierrez, J. (2020). DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. Information Fusion, 64, 131-148. https://doi.org/10.1016/j.inffus.2020.06.014
[39] Karras, T., Aila, T., Laine, S., & Lehtinen, J. (2018). Progressive growing of GANs for improved quality, stability, and variation. arXiv preprint arXiv:1710.10196. https://doi.org/10.48550/arXiv.1710.10196
[40] Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., ... & Houlsby, N. (2021). An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. arXiv preprint arXiv:2010.11929. https://doi.org/10.48550/arXiv.2010.11929
[41] Carion, N., Massa, F., Synnaeve, G., Usunier, N., Kirillov, A., & Zagoruyko, S. (2020). End-to-end object detection with transformers. arXiv preprint arXiv:2005.12872. https://doi.org/10.48550/arXiv.2005.12872
[42] X. Wu, R. He, Z. Sun and T. Tan, "A Light CNN for Deep Face Representation With Noisy Labels," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2884-2896, Nov. 2018, doi: 10.1109/TIFS.2018.2833032.
[43] Zhang, X., Sugrim, S., & Farid, H. (2019). Detecting deepfake videos with steganalysis. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 32-36).
[44] Chen, J., Wu, Y., Wang, P., & Liu, S. (2021). Deepfake Detection with Temporal Convolutional Networks. arXiv preprint arXiv:2104.13410
[45] Wang, Z., & Farid, H. (2020). Detecting deepfake videos in the wild. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 32-36).
[46] Güera, D., Redón, A., & Escrivà, V. (2020). Deepfake Detection with Capsule Networks. In International Conference Image Analysis and Recognition (pp. 39-47). Springer, Cham.
[47] Wang, Y., Liu, X., Yu, D., & Zhu, S. (2019). Deepfake Detection Based on Multimodal Convolutional Neural Networks. IEEE Transactions on Information Forensics and Security, 15, 3452-3466.
[48] Hussain, M., & Muhammad, K. (2021). Deepfake detection using ensemble learning with machine learning and deep learning classifiers. Neural Computing and Applications, 1-15.
[49] Choi, I., Kim, H., Kim, J., & Lee, S. (2020). Deepfake Detection using Ensemble of CNN-based and LSTM-based Features. arXiv preprint arXiv:2006.05926.
[50] Lee, J., Kim, J., Kim, J., & Moon, H. (2019). Deepfake detection using neural network and data augmentation. Multimedia Tools and Applications, 78, 27051-27065.
[51] Zhang, Y., & Jiang, C. (2020). A novel deep learning method for deepfake detection. Journal of Visual Communication and Image Representation, 71, 102812.
[52] Wang, Z., & Bovik, A. (2019). Deepfake detection: a review. Signal Processing: Image Communication, 82, 115811.
[53] Yang, Xin, Yuezun Li, Honggang Qi and Siwei Lyu. “Exposing GAN-synthesized Faces Using Landmark Locations.” Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (2019): n. pag.
[54] Rivera-Rovelo, J., Echegoyen, G., & Morales, A. (2020). Error level analysis and convolutional neural networks for deepfake detection. In 2020 IEEE Mexican Conference on Pattern Recognition (MCPR) (pp. 1-6). IEEE.
[55] Park, J., Kwak, N., & Kim, M. (2021). Ensemble Learning for Deepfake Detection: A Comprehensive Review. IEEE Access, 9, 7421-7435.
[56] Aaditi Parate, Sachin Bhoite “Individual Household Electric Power Consumption Forecasting using Machine Learning Algorithms”, International Journal of Computer Applications Technology & Research, pages 371 – 376 Volume 8, issue 09, September 2019, ISSN: 2319-8656.