

DeepFake Face Detection Using Advanced Deep Learning Techniques

- 1. Gorla.UdayPavan**, B.Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY,udaypavan377@gmail.com
- 2. Thirumani. Naga Durga**, B.Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY,thirumaninagadurga@gmail.com
- 3. Narina.Jagadeesh Kumar**, B.Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY,kumarjagadeesh1908@gmail.com
- 4. Gollakoti.S.V.Manikanta**, B.Tech, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY,gollakotimanikanta@gmail.com
- 5. Ms. Siva SyamalaKorupuri**, M. Tech, Assistant Professor, Department of CSE, DNR COLLEGE OF ENGINEERING AND TECHNOLOGY,syamalakorupuri@gmail.com

Abstract: With a particular emphasis on the rapidly expanding field of deep fakes, this in-depth analysis explores the ever-changing terrain of deep learning applications. Innovations in domains such as computer vision, natural language processing, and machine learning have resulted from deep learning's seamless integration. Nevertheless, there is now serious cause for alarm about the proliferation of deep fakes, which are highly edited movies and photos. There are serious dangers in the online world due to the evil uses of this technology, which include revenge porn, financial frauds, celebrity impersonations, and false news. Famous people, politicians, and other popular personalities are easy prey for Deep Fake Detection. By using a variety of deep learning algorithms, such as InceptionResnetV2, VGG19, CNN, and Xception, this study thoroughly evaluates the creation and identification of deep fakes. Xception stands out as the most accurate algorithm in the assessment, which was carried out on a Kaggle deep fake dataset. The need for strong detection techniques to protect society from possible repercussions is growing as the number of harmful applications of deep fakes increases.

Xception, CNN, Deep Learning, InceptionResnetV2, and VGG19 are some of the index phrases.

I. INTRODUCTION

The use of deepfake technology, which is powered by sophisticated machine learning algorithms, has made it possible to effortlessly superimpose one person's appearance onto another, resulting in very lifelike fake films and photographs. As a result, many are worried that deepfakes may be used for evil, such as disseminating false information or influencing public opinion.

Scientists and engineers have begun using deep learning techniques to combat this rising danger by creating deepfake detection tools. The use of deep learning, and more specifically CNNs and RNNs, has shown potential for detecting deepfake content's artifacts and small discrepancies. These detection methods seek to differentiate between real and altered material by using the capabilities of neural networks to recognize intricate patterns and attributes.

Methods for detecting deepfakes have been refined thanks to a number of research efforts. Most notably, H. Li et al.'s study presented a deep learning-based approach to detect edited facial emotions in films by means of facial action units (Li et al., 2020). In addition, Rossler et al. (2019) suggested analyzing blinking patterns and small head movements using deep learning to find anomalies that may be deepfake material. The importance and urgency of tackling the issues presented by this quickly developing technology are underscored in this introduction, which delves into the growing area of deepfake detection using deep learning. The following sections explore various approaches, developments, and difficulties related to deepfake detection, providing insight into the continuous endeavors to protect digital media's authenticity in a world where artificial intelligence-generated manipulations are prevalent.

In light of the rising problem of deep fakes, or doctored films and pictures, this research investigates the potential uses of deep learning to combat this issue. The study highlights the necessity for strong detection techniques in light of the increasing harmful usage in false news, frauds, and privacy breaches. It investigates several algorithms on a Kaggle deep fake dataset, including InceptionResnetV2, VGG19, CNN, and Xception. Deep fakes, which are films and photos that have been successfully manipulated, are becoming more common and constitute a serious danger in many areas, such as the spread of disinformation and privacy breaches. In

light of the critical need of understanding and preventing the harmful uses of deep fakes, this research highlights the immediate necessity of creating efficient detection methods.

II. LITERATURE SURVEY

[9]Concern over deepfake's potential for harmful usage has intensified in response to its meteoric rise in popularity. To combat this, research on deepfake detection has become in importance. Even while DeepfakeDetection and FaceForensics++ are two of the most powerful datasets out now, they aren't always representative of real-world situations since they use movies with volunteer actors in controlled circumstances. This study fills that need by introducing the WildDeepfake dataset, which contains 7,314 face sequences extracted from 707 deepfake films that were retrieved from the internet in their entirety. When compared to earlier datasets, WildDeepfake attempts to capture the variety and intricacy of deepfakes that are really present online. Since the dataset does not adhere to regulated conditions or commonly used deepfake software, its unique composition presents a greater challenge to deepfake detection techniques. The authors show that WildDeepfake is more challenging and has worse detection performance after doing a thorough examination of baseline detection networks on both conventional datasets and it. Using attention masks on both real and fake faces, the article presents two Attention-based Deepfake Detection Networks (ADDNets) to improve detection capabilities. The suggested ADDNets show promise for fighting real-world deepfake threats by being empirically successful on both well-known datasets and, most importantly, the more difficult WildDeepfake dataset. To keep up with the ever-changing nature of deepfake material on the internet, our study adds to the growing body of research on effective detection systems.

[17]By focusing on the consistency of source characteristics inside forged photos, this work presents a novel method for deepfake detection. Even after passing through sophisticated deepfake production procedures, unique source traits may still be detected and identified, according to the underlying theory. For the purpose of extracting and identifying these source characteristics indicative of deepfake manipulation, the suggested approach, known as pair-wise self-consistency learning (PCL), uses ConvNets for representation learning. To enhance PCL training, a new method of image synthesis called the inconsistency image generator (I2G) is used. This method produces training data that is heavily annotated. The models built in this paper demonstrate significant advancements in deepfake detection, as confirmed by extensive testing on seven well-known datasets. The average Area Under the Curve (AUC) in the in-dataset assessment goes up from 96.45% to 98.05%, which is better than the state-of-the-art performance. In addition, the AUC increases from 86.03% to 92.18% in the cross-dataset examination. These results highlight the effectiveness of the suggested method, showing that it can improve the precision and consistency of deepfake detection models on various datasets. Ongoing attempts to strengthen defenses against the propagation of fraudulent deepfake material benefit greatly from the research's insightful techniques and contributions.

[24]In light of the significant difficulty caused by the widespread use of false movies, especially those produced by sophisticated generative adversarial networks, this study presents a fresh method for identifying deepfake videos. By making use of the cutting-edge Attribution-Based Confidence (ABC) measure, the suggested approach may function independently of either the training data or the validation data and the calibration model. The ABC metric allows inference to be based just on the availability of the trained model, unlike previous techniques. A deep learning model is trained using only original films in this process. Then, the ABC measure is used to identify whether a video is real or not. With confidence values greater than 0.94, this measure sets a threshold for original videos and provides confidence values. The ABC measure offers a simple and effective way to tell real movies from edited ones, opening up a potential new direction for deepfake detection that doesn't need large training or validation datasets. The unique addition of this research is the way it uses the ABC measure in a novel way, demonstrating how well it can differentiate between real and deepfake films. This method is a great asset to the fight against the fast development of misleading video alteration methods since it relies on attribution-based trust.

[28]By showing that adversarial perturbations may fool conventional detectors, this study fixes a serious flaw in deepfake detection systems. In both whitebox and blackbox settings, the research uses the Fast Gradient Sign Method and the Carlini and Wagner L2 norm approach to generate adversarial perturbations that greatly improve deepfake pictures, leading to a sharp drop in detection accuracy. When presented with disturbed deepfakes, detectors' performance dropped to less than 27% accuracy, in contrast to over 95% accuracy on undamaged deepfakes. Two possible improvements to deepfake detectors are also explored in the research. To increase resistance to input perturbations, we first investigate Lipschitz regularization, which limits the detector's gradient relative to the input. With a notable 10% improvement in accuracy in the blackbox situation, this regularization enhances the identification of disturbed deepfakes. The Deep Image Prior (DIP) defense is presented secondly; it employs generative convolutional neural networks to unsupervisedly eliminate disturbances. In some instances, the DIP defense maintains a 98% accuracy rate on a 100-image subset; in others, it achieves 95% accuracy on altered deepfakes that first fooled the detector. This study provides useful

insights into possible ways for strengthening the robustness of deepfake detectors against adversarial assaults. It highlights the necessity of protecting these systems from developing adversarial threats. on page 34 To address the growing problem of deepfake movies created by sophisticated tools like Generative Adversarial Networks (GANs), this research presents DeepfakeStack, a powerful deep ensemble-based learning method for video manipulation detection. There is an urgent need for strong countermeasures due to the fact that deepfake technology has many illegal uses, including misleading propaganda, cybercrimes, and political campaigns. Using state-of-the-art deep learning models, DeepfakeStack has developed an all-inclusive method for identifying altered material. By merging a number of state-of-the-art classification models into an ensemble, DeepfakeStack generates an upgraded composite classifier. The experimental findings show that DeepfakeStack is the best classifier, surpassing the competition with a remarkable AUROC score of 1.0 and an accuracy of 99.65% in deepfake identification. These results show that the suggested technique works and make DeepfakeStack a good tool for creating deepfake detectors in real time, which can protect against many illegal uses of hyper-realistic multimedia. This study adds significantly to the current body of knowledge on the subject of creating cutting-edge technology to combat the growing threats posed by the fraudulent alteration of audio and video material.

III. METHODOLOGY

i) Proposed Work:

By taking a holistic approach and making use of state-of-the-art deep learning algorithms, the suggested solution hopes to counter the growing danger of deep fakes. Our system uses DeepFace, InceptionResnetV2, CNN, and Xception algorithms for thorough assessment on a Kaggle deep fake dataset. Building a reliable system to identify altered information from genuine content is a top priority. The system's goal is to help shed light on the creation and dissemination of deep fakes by analyzing their complexities. The dataset offers a varied array of situations for efficient training and testing, and the integration of many methods guarantees a detailed analysis. The possible social effects of false news, impersonations, and privacy breaches may be mitigated by this holistic strategy, which aims to improve the overall accuracy and reliability of deep fake detection. To protect our online environment from the malicious use of deep fake technologies, the suggested solution is an important first step.

ii) Architecture of the System:

Several steps make up the architecture of the system used to identify deepfakes. These steps include importing the movies, cutting them into frames, using an image data generator, exploratory data analysis (EDA) with data visualization, and scaling the images. The system then uses Xception, InceptionResNetV2, VGG19, CNN, and other deep learning algorithms to ensure accurate identification after EDA. At the outset, the system slices deepfake films into individual frames using a segmentation algorithm. By breaking down the movie into its individual frames, we may examine possible modifications in more detail. Data visualization tools are used in the next EDA step to learn about the frames' properties, which helps to comprehend the dataset better. Standardizing frame size by picture scaling improves model generalizability. To further enhance the dataset, add variances, and make the model more robust, an image data generator is also used. At its heart, the design is based on using well-known deep learning algorithms for picture categorization, including InceptionResNetV2, VGG19, CNN, and Xception. Separate algorithms analyze the frames and add to the total detection accuracy by extracting unique characteristics. Finally, we compare these algorithms' detection performance using measures like recall, F1-score, specificity, sensitivity, MAE, and MSE, among others. This all-inclusive system design guarantees a methodical and efficient method of deepfake detection by using a mix of preprocessing, exploratory analysis, and cutting-edge deep learning algorithms to boost the system's total effectiveness.

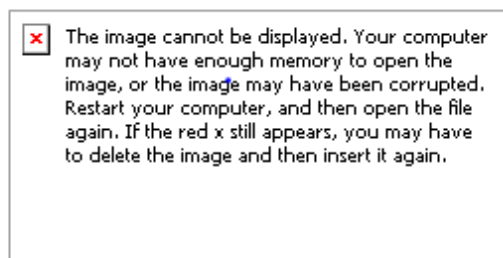


Fig 1 System Architecture

iii) Dataset collection:

A Kaggle deepfake dataset is a great tool for developing deepfake detection models since it contains a wide variety of both real and fake videos. When it comes to dealing with the difficulties brought up by deepfake technology, the curated datasets available on the data science and machine learning competition site Kaggle are ideal. The first step in gathering datasets is to go to Kaggle's deepfake dataset repository. This repository usually has a ton of movies that display both real and altered material. This labelled dataset is ideal for supervised learning methods since each video has been painstakingly tagged to indicate its legitimacy. For the model to be reliable and applicable in a wide range of situations, the dataset includes many characters, settings, and situations. Because of the cooperative spirit of Kaggle, users often pool their resources to improve the quality and use of datasets by preparing and supplementing them. With ground truth labels at their fingertips, researchers can easily train and test deepfake detection algorithms, comparing their models to a standard dataset.

iv) Image Processing: When it comes to creating successful computer vision models, image processing is essential, especially for deepfake detection and similar applications. Image Resizing and Image Data Generator are two essential methods used in this context for processing images. To make sure that deep learning models use consistent input data, picture resizing is used to change the size of photos to a common format. When working with photos of different resolutions, resizing is crucial for avoiding computational inefficiencies and ensuring a smooth integration into neural network designs. Finding a happy medium between processing speed and maintaining important visual information is much easier with its assistance. Image Data Generator, in contrast, is a method for increasing model resilience and dataset variety by the introduction of input data changes. The random transformations that fall within this category include rotating, zooming, and horizontally flipping. Image Data Generator is essential for deepfake detection because it trains models to handle variances and alterations in video frames that really occur in the real world. All of these image processing methods work together to help provide the groundwork for a solid deepfake detection system. Image Data Generator improves the model's generalizability by adding variability, Image Resizing makes ensuring that input dimensions are consistent, and finally, Image Resizing improves the model's capability to distinguish real content from altered visual data. Taken together, these methods provide the deep learning model the tools it needs to deal with the complex, ever-changing visual inputs it will see in the actual world.

v) Visualizing Data: One of the most important steps in deepfake detection is slicing films into frames. This allows for a detailed study of how the video was altered over time. When films are broken down into their constituent frames, data visualization tools come in handy for understanding the dataset's properties. Visual information retrieved from video frames is represented by a variety of graphical and statistical methods in this context, which is known as data visualization. To fully grasp the temporal dynamics of the dataset, methods including displaying optical flow patterns, showing histograms of pixel intensities, and frame length distributions are used. A histogram may help you spot trends or outliers linked to deepfake alterations by revealing changes in pixel values. Visualizations of time, such as motion heatmaps or frame-by-frame comparisons, help to identify anomalies or abnormalities produced by deepfake production. Visualizing the direction and intensity of motion between successive frames may be achieved by plotting optical flow vectors. This technique offers valuable insights on the dynamic elements of the video material. Researchers may also make advantage of interactive visualization tools to examine and mark individual frames, which helps to spot trends or outliers that might point to deepfake alterations. Using these data visualization tools, researchers may better understand the information and find ways to improve deepfake detection algorithms by revealing complex temporal patterns, abnormalities, and artifacts. Visualization enhances the deepfake detection system's interpretability and helps with model development decision-making.

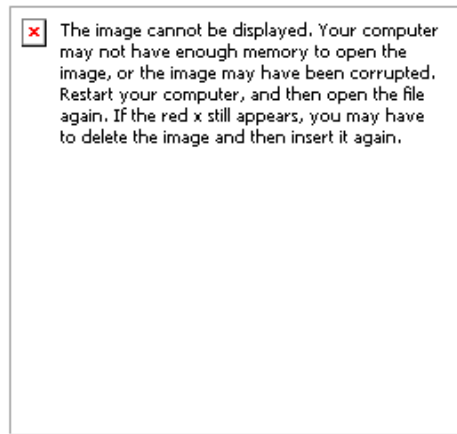


Fig 2 Data Visualization

vi) Algorithms:

InceptionResNetV2: The PrototypeThe deep structure and improved feature extraction capabilities of ResNetV2, a hybrid of Inception and ResNet architectures, are used. For the purpose of detecting minute visual clues that point to deepfake alterations in video frames, this model is perfect since it is so good at collecting complex patterns and hierarchical characteristics.

Chosen for its efficacy and simplicity, VGG19 has a simple design with tiny receptive fields that helps to capture both low-level and high-level characteristics. The fact that it can effectively identify deepfake patterns in single video frames makes it a great option.

One useful tool for collecting spatial information from picture data is a Convolutional Neural Network (CNN). For fast processing of individual frames during deepfake detection, this architecture—which is both lightweight and effective—is ideal.

A model that excels in understanding spatial hierarchies is Xception, thanks to its deep design and remarkable feature extraction capabilities. This model is well-suited for this project because of its depth, which increases its ability to catch complex patterns that are important for identifying alterations in video frames.

IV. EXPERIMENTAL RESULTS

Accuracy: A test's accuracy is defined by how well it distinguishes between healthy and sick samples. We can determine a test's accuracy by calculating the percentage of reviewed instances with true positives and true negatives. If we express this mathematically, we get: $Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$.

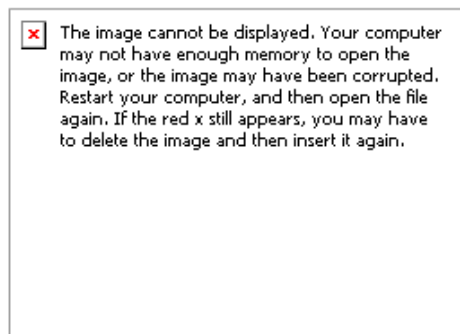
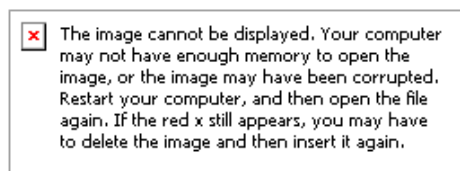


Fig 3 Accuracy comparison graph

Precision:

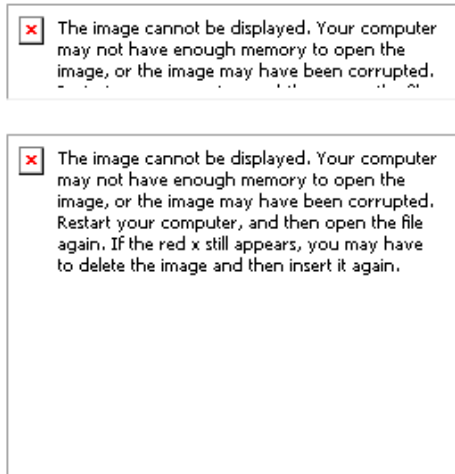


Fig 4 Precision comparison graph

Recall:

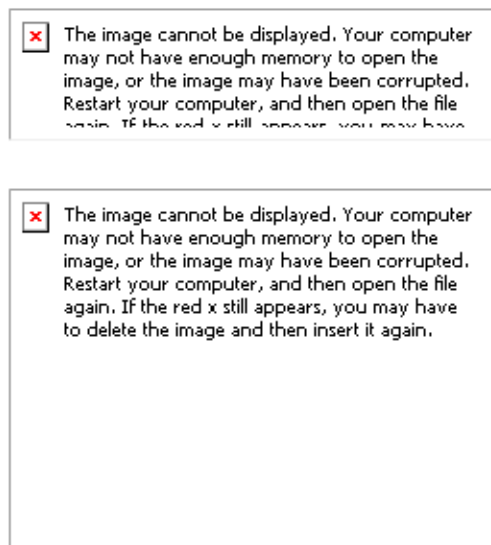



Fig 5 Recall comparison graph

 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.


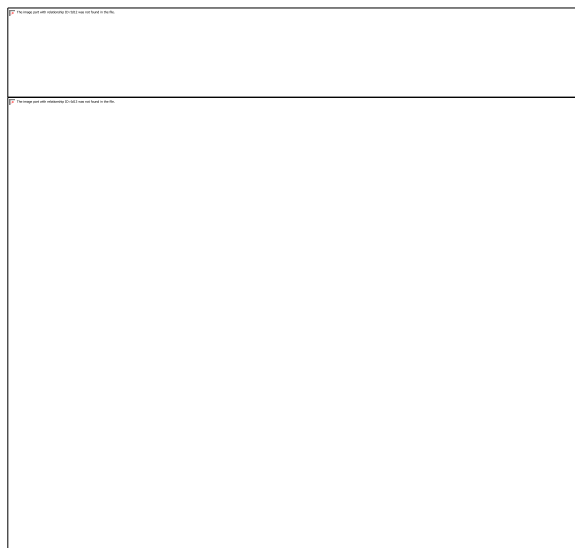
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 6 F1Score comparison graph

F1-Score:

Sensitivity:



Specificity:

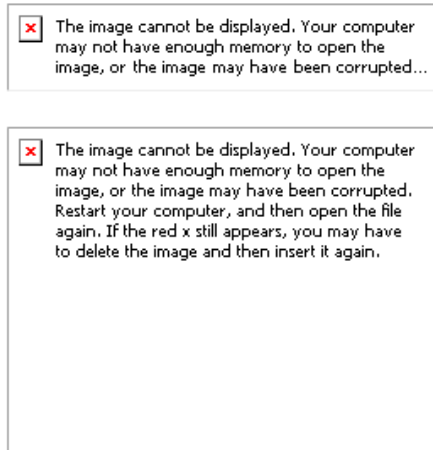



Fig 8 Specificity comparison graph

MAE: To get the MAE, take all of the mistakes in the calculations and divide them by the number of samples. In this case, the absolute errors between the forecast and the actual value are averaged out. It is possible to use relative frequencies as weight factors in alternative formulations.



MSE: A statistical study's mean squared error (MSE) is the average squared deviation between the study's actual value and the model's predicted value. Since certain data values will be larger than the prediction (and therefore their differences will be positive), and other data values will be less (and hence their differences will be negative), it is required to square the differences when comparing anticipated values with observed values. Since the likelihood of the observed values being higher or lower than the projected values is equal, the discrepancies would add up to zero. This problem disappears when the disparities are squared. To get the mean squared error, one uses =

 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 9 Performance evaluation table


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 10 Performance evaluation comparison graph


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 11 Home & about page


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 12 Registration page


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 13 Login page


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 14 Main page


 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Fig 15 Upload input

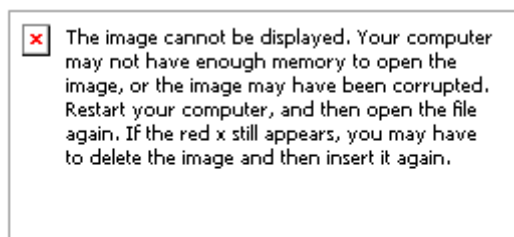


Fig 16 Predict result as fake

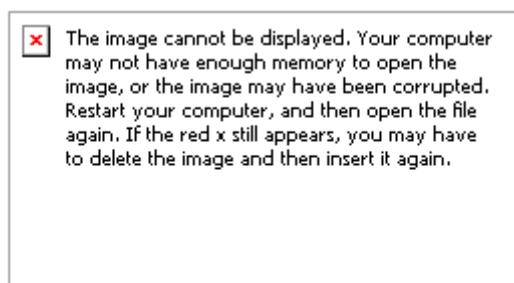


Fig 17 Upload another input

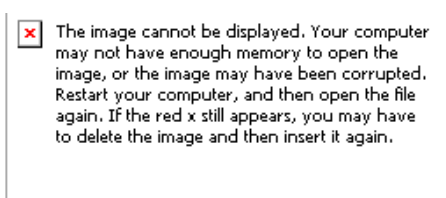


Fig 18 Final outcome as real for given input

V. CONCLUSION

As the level of manipulation by technology continues to rise, this research concludes that deep fake detection systems must adapt. While the current system does investigate both traditional and modern approaches, it shows its limits when it comes to responding to new dangers and deciphering complex patterns. The suggested solution is proactive in addressing these issues by using state-of-the-art algorithms like Xception and InceptionResnetV2. A broad training ground is ensured by using a Kaggle deep fake dataset, which enhances the system's adaptability to real-world settings. The suggested method takes a comprehensive view of the problem, with the dual goals of increasing detection accuracy and providing more understanding of the dynamics of deep fake generation and spread. The possible social consequences of altered material, such as false news, privacy breaches, and impersonations, must be well understood in order to implement effective responses. A more secure and resilient digital environment for consumers globally may be achieved by the suggested system, which is a crucial step in protecting our digital landscape from the malicious use of deep fake technologies.

8. IN THE LONG TERM

Constant improvements to tackle new deep fake threats are where this research's future rests. Improved detection capabilities may be possible with more research into novel algorithms and the incorporation of developing technologies like reinforcement learning. The development of established methods for deep fake detection requires the combined efforts of academics, businesses, and politicians. Further investigation into real-time detection systems and the incorporation of explainability characteristics might enhance the trustworthiness and openness of deep fake detection technologies for users.

REFERENCES

- [1]. M. Mirza and S. Osindero, "Conditional generative adversarial nets," arXiv preprint arXiv:1411.1784, 2014.
- [2]. Y. Bengio, P. Simard, and P. Frasconi, "Long short-term memory," *IEEE Trans. Neural Netw.*, vol. 5, pp. 157–166, 1994.
- [3]. I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.
- [4]. S. Hochreiter, "Ja1 4 rgenschmidhuber (1997). "long short-term memory"," *Neural Computation*, vol. 9, no. 8.
- [5]. M. Schuster and K. Paliwal, "Networks bidirectional recurrent neural," *IEEE Trans Signal Proces*, vol. 45, pp. 2673–2681, 1997.
- [6]. J. Hopfield et al., "Rigorous bounds on the storage capacity of the dilute hopfield model," *Proceedings of the National Academy of Sciences*, vol. 79, pp. 2554–2558, 1982.
- [7]. Y. Wu, M. Schuster, Z. Chen, Q. V. Le, M. Norouzi, W. Macherey, M. Krikun, Y. Cao, Q. Gao, K. Macherey, et al., "Google's neural machine translation system: Bridging the gap between human and machine translation," arXiv preprint arXiv:1609.08144, 2016.
- [8]. L. Nataraj, T. M. Mohammed, B. Manjunath, S. Chandrasekaran, A. Flenner, J. H. Bappy, and A. K. Roy-Chowdhury, "Detecting gan generated fake images using co-occurrence matrices," *Electronic Imaging*, vol. 2019, no. 5, pp. 532–1, 2019.
- [9]. B. Zi, M. Chang, J. Chen, X. Ma, and Y.-G. Jiang, "Wilddeepfake: A challenging real-world dataset for deepfake detection," in *Proceedings of the 28th ACM international conference on multimedia*, 2020, pp. 2382–2390.
- [10]. H. A. Khalil and S. A. Maged, "Deepfakes creation and detection using deep learning," in *2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*. IEEE, 2021, pp. 1–4.
- [11]. J. Luttrell, Z. Zhou, Y. Zhang, C. Zhang, P. Gong, B. Yang, and R. Li, "A deep transfer learning approach to fine-tuning facial recognition models," in *2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)*. IEEE, 2018, pp. 2671–2676.
- [12]. S. Tariq, S. Lee, H. Kim, Y. Shin, and S. S. Woo, "Detecting both machine and human created fake face images in the wild," in *Proceedings of the 2nd international workshop on multimedia privacy and security*, 2018, pp. 81–87.
- [13]. N.-T. Do, I.-S. Na, and S.-H. Kim, "Forensics face detection from gans using convolutional neural network," *ISITC*, vol. 2018, pp. 376–379, 2018.
- [14]. X. Xuan, B. Peng, W. Wang, and J. Dong, "On the generalization of gan image forensics," in *Chinese conference on biometric recognition*. Springer, 2019, pp. 134–141.
- [15]. P. Yang, R. Ni, and Y. Zhao, "Recapture image forensics based on laplacian convolutional neural networks," in *International Workshop on Digital Watermarking*. Springer, 2016, pp. 119–128.
- [16]. B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *Proceedings of the 4th ACM workshop on information hiding and multimedia security*, 2016, pp. 5–10.
- [17]. T. Zhao, X. Xu, M. Xu, H. Ding, Y. Xiong, and W. Xia, "Learning selfconsistency for deepfake detection," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2021, pp. 15 023–15 033.
- [18]. D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "Mesonet: a compact facial video forgery detection network," in *2018 IEEE international workshop on information forensics and security (WIFS)*. IEEE, 2018, pp. 1–7.
- [19]. E. Sabir, J. Cheng, A. Jaiswal, W. AbdAlmageed, I. Masi, and P. Natarajan, "Recurrent convolutional strategies for face manipulation detection in videos," *Interfaces (GUI)*, vol. 3, no. 1, pp. 80–87, 2019.
- [20]. Y. Li, M.-C. Chang, and S. Lyu, "In ictuoculi: Exposing ai created fake videos by detecting eye blinking," in *2018 IEEE International workshop on information forensics and security (WIFS)*. IEEE, 2018, pp. 1–7.
- [21]. J. Donahue, L. Anne Hendricks, S. Guadarrama, M. Rohrbach, S. Venugopalan, K. Saenko, and T. Darrell, "Long-term recurrent convolutional networks for visual recognition and description," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 2625–2634.
- [22]. Y. Li and S. Lyu, "Exposing deepfake videos by detecting face warping artifacts," arXiv preprint arXiv:1811.00656, 2018.
- [23]. X. Yang, Y. Li, and S. Lyu, "Exposing deep fakes using inconsistent head poses," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2019, pp. 8261–8265.

- [24]. S. Fernandes, S. Raj, R. Ewetz, J. S. Pannu, S. K. Jha, E. Ortiz, I. Vintila, and M. Salter, "Detecting deepfake videos using attributionbased confidence metric," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020, pp. 308–309.
- [25]. U. A. Ciftci, I. Demir, and L. Yin, "Fakecatcher: Detection of synthetic portrait videos using biological signals," *IEEE transactions on pattern analysis and machine intelligence*, 2020.
- [26]. D. Guera and E. J. Delp, "Deepfake video detection using recurrent " neural networks," in 2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS). IEEE, 2018, pp. 1–6.
- [27]. S.-Y. Wang, O. Wang, R. Zhang, A. Owens, and A. A. Efros, "Cnn-generated images are surprisingly easy to spot... for now," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2020, pp. 8695–8704.
- [28]. A. Gandhi and S. Jain, "Adversarial perturbations fool deepfake detectors," in 2020 International joint conference on neural networks (IJCNN). IEEE, 2020, pp. 1–8.
- [29]. L. Li, J. Bao, T. Zhang, H. Yang, D. Chen, F. Wen, and B. Guo, "Face x-ray for more general face forgery detection," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2020, pp. 5001–5010.
- [30]. H. Cui, A. Liu, X. Zhang, X. Chen, K. Wang, and X. Chen, "EEGbased emotion recognition using an end-to-end regional-asymmetric convolutional neural network," *Knowledge-Based Systems*, vol. 205, p. 106243, 2020.
- [31]. Z. Chen and H. Yang, "Attentive semantic exploring for manipulated face detection," in ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021, pp. 1985–1989.
- [32]. R. Durall, M. Keuper, F.-J. Pfreundt, and J. Keuper, "Unmasking deepfakes with simple features," arXiv preprint arXiv:1911.00686, 2019.
- [33]. X. Li, Y. Lang, Y. Chen, X. Mao, Y. He, S. Wang, H. Xue, and Q. Lu, "Sharp multiple instance learning for deepfake video detection," in Proceedings of the 28th ACM international conference on multimedia, 2020, pp. 1864–1872.
- [34]. M. S. Rana and A. H. Sung, "Deepfakestack: A deep ensemblebased learning technique for deepfake detection," in 2020 7th IEEE international conference on cyber security and cloud computing (CSCloud)/2020 6th IEEE international conference on edge computing and scalable cloud (EdgeCom). IEEE, 2020, pp. 70–75.
- [35]. H. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task learning for detecting and segmenting manipulated facial images and videos," in 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2019, pp. 1–8.
- [36]. Z. Guo, L. Hu, M. Xia, and G. Yang, "Blind detection of glow-based facial forgery," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7687–7710, 2021.