2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) | 978-1-6654-7436-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAC3N56670.2022.10074593

A Comparative Study on Deepfake Detection Algorithms

Anukriti Kaushal
Department of Computer Engineering
Delhi Technological University
Delhi, India
anukritikaushal@dtu.ac.in

Sanchit Singh
Department of Computer Engineering
Delhi Technological University
Delhi, India
sanchitsingh513@gmail.com

Shashank Negi
Department of Computer Engineering
Delhi Technological University
Delhi, India
shashank.negi2000@gmail.com

Shikhar Chhaukar
Department of Computer Engineering
Delhi Technological University
Delhi, India
shikharchhaukar@gmail.com

Abstract— **In recent years, the number of images and videos shared online increased and people have easy ways to access such content. "DeepFake" refers to any multimedia content created using deep learning technology in order to make it appear realistic. The creation of deepfake videos and images using deep learning techniques leads to very realistic "DeepFake" videos and images by changing the digital content of images and videos. Deepfake is widely recognized as one of artificial intelligence's most dangerous uses. Deepfake makes it possible to place a person in a totally imaginary situation since it is used to imitate an activity that the person did not perform. Deepfakes have been becoming increasingly dangerous to democracy, society's security and people's privacy. The distribution of such deepfake content on various platforms urged the international community to revaluate the threat to social security posed by such content. It encouraged the researchers around the world to develop effective deepfake detection methods. In this paper we have discussed such approaches of deepfake detection in videos and images that are available in recent studies and have provided comparative review of research on deepfake detection algorithms. It also compares the different detection techniques and examines their limitations and advantages.**

Keywords— Deepfake, Deep Learning, Deepfake Detection, Detection Accuracy, Artificial Intelligence, Generative Adversarial Networks.

I. INTRODUCTION

In 1997, an original, totally unique program called Video Rewrite Program was developed which automated what some movie companies could achieve during that time. From just audio output, that Program could create new animations. Video Rewrite Program used previous work that produce audio from text, modelled lips in 3D and interpreted faces and it was the first program that put all these features together and animate it smoothly. In the early 2000s computer vision went further into the facial recognition world. Advances in this field have led to considerable improvements in areas like motion tracking, making today's deepfakes more convincing. Researchers from Erlangen-Nuremberg, Max Planck and Stanford presented an IEEE paper for Face2Face, that edits video in real time and easily converts the target person's facial gestures with the source facial gestures. Face2Face seeks to create a real time animation by using actors to replace the mouth area of the target video. Although this method does not include audio, there are already developed methods for synthesizing human speech. Nowadays, it's very common to encounter fake videos and photoshopped pictures on the internet. It's uncommon these days that you visit social media and do not discover any kind of fake content whether it's a selfie captured using a filter, a video with edited soundtrack or a meme. Deepfake, it was coined in 2017 to describe photos and videos that use deep learning algorithms to create realistic looking fake videos and photographs.

The term Deepfake is plainly a mixture of two common words: "deep" and "fake" [33]. The term "deep" refers to the AI technology used in this case, that is deep learning [19]. Deepfake techniques are used to create material that is not real in AI-generated media, for example generating faces, altering emotions and speech [9]. Machine learning (ML) and deep learning (DL) techniques found numerous applications in real-life problems like medical imaging [26], social network [34], computer vision [35] and
Deepfake is one of the most sought after application of ML and DL techniques where main component of deepfakes, can be used to build deepfakes more quickly and at a lower cost [10]. GAN are a class of deep learning algorithms used to be the driving force behind the creation and development of deepfake.
Deepfake is widely recognized as one of artificial intelligence's most harmful uses. Malicious uses of deepfake include political disinformation, fraud and extortion [11, 12]. A deepfake could easily be mistaken for the real thing. It has the ability to harm a person's reputation or cause them to say or do something unsuitable. It's a perfect weapon for the con artists to use against their target. To create a deepfake detection program sufficient amount of time is needed. The

deepfake detection system requires training before it can distinguish between a real and fake media.

Deepfakes have been becoming increasingly dangerous to democracy, society's security and people's privacy. Methods for detecting deepfakes have been proposed as the threat of deepfakes was acknowledged [13]. Some approaches rely on features acquired from flaws of the fake video synthesis process [14, 15]. Deep learning was used in some methods to automatically extract important characteristics in order to detect deepfakes [16, 17].

Detecting deepfakes visually with the naked eye can be done using a few easy ways like checking resolution differences between the suspected areas and rest of the video. One can even look for inconsistent skin tones around suspected areas or looking at how the facial features like eyes, hairline, jaws etc align in different shots in the video. However, these techniques are limited to older GAN generated deepfakes as some newer deepfake creation techniques make it harder to distinguish between reality and deepfake created content with the naked eye.

II. Related Work

Deep Learning technology, that is derived from ANN which is Artificial Neural Network, has become very popular in the context of computing and it is broadly used in fields such as visual identification, cybersecurity, text analytics, healthcare and cybersecurity. In the past, neural networks were successfully used in a number of applications, ANN a deep learning based concept has gained popularity, leading in a resurgence in neural network research.

This is because deep networks have demonstrated great effectiveness in various regression and classification challenges when properly trained. Although deep learning takes a lengthy time to train a model because of the number of parameters, it takes less time to execute during testing as compared to other machine learning algorithms.

Generative Adversarial Networks are an approach to generative modelling.

The first researches under deepfake dedicated an entire section to GAN for their impressive ability to make deepfakes that are near impossible to tell from real faces and thus make it possible for anyone to create hard to differentiate deepfakes. GAN models work great for synthesising images; however, they are not for making videos. GAN models have many flaws such as requiring a huge amount of training data and take a long time to generate images when compared to other techniques. The prime defects for not using GAN models for videos is that they have problems preserving temporal consistency. Some of the best early examples of audio deepfakes such as when a company used Joe Rogan’s voice from a talk show to utter sentences that he never said but even in these GAN’s were not involved. The truth is that in these modern times, GAN models have lost their touch and most of the deepfakes are made using a constellation of AI and non - AI algorithms.

Convolution Neural Network (CNN) has a deep feed forward architecture with a remarkable ability to generalize when compared with networks having fully layers. It is capable of learning highly abstract traits and accurately identifying objects. CNN doesn't suffer from overfitting and it is possible to train it smoothly because of the fewer parameters. Large networks are far more difficult to create using general models of ANN than they are in Convolutional neural network. Due to their exceptional performance, CNNs are broadly employed in a variety of fields, including facial expression recognition, face detection, image classification, voice recognition and many more.

To construct a deepfake video, a person must first need to train a neural network on the original video clip of the person to give it a knowledge of how the person appears from various different angles. Computer graphics techniques would then be combined with the trained network. While the use of AI speeds up the process, it still takes time to create a realistic composite that places a person in a totally imaginary situation since it is used to imitate an activity that the person did not perform. In the 20^{th} century, Academic institutions started working towards this technology to see its various applications. Despite the fact that the creation of deepfake is not that easy, the concept has dug its way into making fake news for the media. In the United Kingdom, one of the earliest deepfake related scam incidents occurred. Imitating his German employer, scammers called the Director of a UK company and asked him to send €220,000 to a bank account.

III. Comparative Analysis

Rana and Sung [1] proposed a technique called DeepFakeStack which gives us an improved composite classifier by combining multiple deep learning based avant-garde classification models. In DeepfakeStack a meta-learner on top of pre-trained base-learners is trained. It creates an interface which shows us how the ensemble technique performs the classification task. It also fits the meta-learner on the predictions of the base-learners. They used the FaceForensics++ (FF++) dataset and then manipulated the videos in them using 3 popular avant-garde manipulation techniques. After generation of a balanced dataset, they tracked the face in each of the videos taking 101 frames as images and fed them into the classifier [27]. They considered 7 deep learning models as base-learners and applied the transfer learning. [20].

$$\sigma(\vec{z})_i = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \tag{1}$$

Where σ is softmax function, $\vec{z}$ is input vector, e^{z_i} is standard exponential function for input vector, K = number of classes in the multi-class classifier and e^{z_j} is standard exponential function for output vector. The SoftMax activation function is used in last output layer to normalize neural network output to fit between 0 and 1. For training the models, Greedy Layer-wise Pretraining (GLP) technique was used because of its ability to add a new hidden layer which lets it refit the model [21]. Pretraining is beneficial for dealing with problems involving huge volumes of unlabelled data and little amount of labelled data. DeepfakeStackClassifier (DFC) is employed as a meta-learner. The proposed DeepFakeStack model outperforms the deep learning based models and thus is an effective Deepfake detector.

Younus and Hassan [2] proposed DeepFake detection method takes into account the fact that current algorithms for creating DeepFakes can't make images with different resolution in the image, i.e., can only produce new faces of a certain size and resolution; blurring and further distortion are required to perfect and blend the false face with the surrounding environment and the backdrop in the source footage [22, 23, 24, 25, 26]. In the resulting DeepFake films, this transformation generates unique blur inconsistencies between the created face and its backdrop. These alterations may be efficiently detected by comparing the edge pixels in the wavelet zone of the faces in each frame to the remainder of the frame. Blur inconsistencies are discovered by studying the type of edge and its sharpness. By sampling Harr functions at 2^k places, the Harr wave transform function is used, and a matrix was created to express the function in simple terms. The following function can be used to gain any dimension of this Harr matrix.

Any dimension of this Harr matrix is gained by using the function :

$$H(k) = \begin{pmatrix} H(k-1) & \otimes & [1 \quad 1] \\ 2^{\frac{k-1}{2}} l(k-1) & \otimes & [1 \quad 1] \end{pmatrix}, H(0) = 1 \qquad (2)$$

Where H(k) represents the distinct Haar functions of degree at 2^k matrix, and I(k) represents the degree at 2^k identity matrix. It can determine whether a face image has been blurred by marks left behind by matching a fake face generated by GAN. By comparing the blur extent of the rest of the image to the ROI to the blur extent, it can be identified if the images are tampered with or not. On the UADFV dataset, this technique was put to the test, and the findings indicated that it was quite good at spotting DeepFake videos.

Zhu et al. [3] developed a new technique for detection of deepfakes which uses clustering based embedding regularization. They combined clustering based embedding regularization term into the classification objective for improving the local smoothness of the representation space and for training, Xception networks were used. For the datasets, UADFV which is a dataset with low quality videos, DeepFakeDetection and Celeb-DF both of which are dataset with high quality were selected [28]. They used open source algorithms to perform experiments on the selected datasets and then under identical conditions compared them with the proposed model. Parameters like margin value, batch size value and different conditions were adjusted to the improve the results. Deepfake detection algorithms(Meso4 algorithm ,FWA algorithm, EVA algorithm, Multi-task algorithm ,Xception-c23) were compared with his model. The model achieved an accuracy of 98.4%,99.99% and 99.9% for DeepFakeDetection, UADFV and Celeb-DF datasets, respectively.

Kumar et al. [4] developed a strategy employing a triplet network to identify between false and real video embedding vectors. In this, Facenet was used to create 512 dimension embeddings for each face in the feature space after MTCNN extracted faces from the frames. They began using the XceptionNet architecture for video classification after seeing its effectiveness in detecting fraudulent and authentic films in the FF++ paper [3]. Recurrence networks were introduced to help the network learn the sequences. In contrast to 2D convolution, which collapses the temporal domain, the 3D convolution model incorporates 3D filters that take up knowledge of spatiotemporal properties from the movies. After that they created semi-hard triplets. Through triplet loss, the embeddings of false frames and positive frames are distinguished using these triplets.

Triplet loss function equation is:

$$L(A, P, N) = \max(||f(A) - f(P)||^2 - ||f(A) - f(N)||^2 + \alpha, 0) \qquad (3)$$

In this α is a hyperparameter. S is an anchor input sample. T is a sample with the same label. N is another different label sample. They looked at numerous strategies to battle low-resolution video categorization. They surpass the prior results by a significant margin using the Triplet network on the Celeb-DF and FF++ datasets, while only using 25 frames each video.

Chen et al. [5] proposed a deepfake detection technique based on successive subspace learning (SSL) . In this technique, Firstly image processing was utilized to crop off face pictures to produce patches of size 32 × 32 that are input to PixelHop++. It then extracts rich and distinguishing characteristics from local blocks with a block size of 3 × 3 and a stride of one without padding. After that, two approaches for further distilling the feature to acquire a concise description of whether a face is false or genuine, namely Channel-wise Soft Classification and spatial dimension reduction. In computer vision, Channel-wise Soft Attention is a technique which assigns "soft" attention weights for each channel c. The alignment weights that are learned through soft channel-wise attention and placed "softly" over each channel. This is different than hard attention as hard channel attention selects only one channel to attend to at a time. To check if a video clip is authentic or not, they merged soft judgments from all facial locations and selected frames by combining the probability of several face areas into a Multi-Frame Ensemble because against different Deepfake manipulations, each facial region can have distinct weaknesses and strengths [36]. Thus, by taking the average of the probabilities of all frames, they calculated its likelihood of being phony. FaceForensics++ (FF++), UADFV, Celeb-DF v2 and Celeb-DF v1 datasets were used to assess this. With a lower model size, a faster training approach, a high detection AUC, and fewer training data, it proved to be quite successful.

Guarnera et al. [6] proposed a technique based on GAN that analyses the deepfakes of the faces and can expose the forensic traces hidden in the image, which is a kind of fingerprint found on a tempered image. The technique proposed by the authors extracts local features that are precisely targeted to describe the basic convolutional generative process by using the algorithm Expectation Maximization [29]. They used Ad-hoc validation by performing experiments with naive classifiers on ATTGAN, STARGAN, STYLEGAN2, GDWCT and STYLEGAN architectures against the CELEBA dataset. They used CELEBA, which contains solely legitimate celebrity face images and deepfakes created by GANs (STYLEGAN2, STYLEGAN, GDWCT, STARGAN, ATTGAN). In order to build their image datasets ATTGAN, GDWCT and STARGAN were used in inference mode. They were able to create a new detection technique which uses features extracted from the Expectation-Maximisation (EM) algorithm to detect deepfakes. In EM Algorithm a set of incomplete data is taken and a set of starting parameters is considered. It consists of two steps which are repeated until convergence is achieved. The first step is called the Expectation step (E – step). In E - step we guess the values of the missing data using the observed available data of the dataset. The second step is called the Maximization step (M – step). In M - step we update the parameters using the complete data generated after E - step.

Jung et al. [7] developed the DeepVision algorithm, which took advantage of the fact that blinking is a natural and voluntary movement that does not require conscious effort. Deepfakes which are created by the generative adversarial network model can be detected by the algorithm DeepVision that look for a notable change in the blinking pattern. The pattern of human eye blinking can change greatly depending on the person's physical state, biological parameters and cognitive activities. The blinking pattern can be influenced by a person's age, gender, or the level of awareness. As a result, the authors used blinking eye patterns to identify Deepfakes by using a heuristic method. DeepVision repeats the eye blinks relentlessly within a very small period of time and studies the elapsed eye blink time, the period and the repeated numbers.

In the architecture of the algorithm proposed by the authors, Age, Time, Gender and Activity are taken as important parameters as data input for the pre-process [30]. Changes in Human eye blinks can be checked because of the pre-process [32]. DeepVision is utilized for taking measurements through detecting objects in the video by the use of the Target Detector, and blinking is recorded using Eye Tracker. The idea behind the Eye Tracker is the Eye Aspect Ratio(EAR) which determines the absolute area of the vertical and horizontal axes using six points (ti) around the eyes. It was created by Jan Cech and Tereza Soukupova. The formula EAR, which is used to recognize eye blinks, is shown below.

$$EAR = \frac{\|t2-t6\|+\|t3-t5\|}{2\|t1-t4\|} \tag{4}$$

In the equation the points other than t4 and t1 represents the vertical axis whereas points t4 and t1 represent the horizontal axis in the eye area. EAR is an absolute size which is calculated with the help of vertical and horizontal.
Since eye blinks usually happen at the same time in both eyes, They made use of Eq. (2), which calculates the eye's ratio (EARi) with the help of the right eye (EARr) value and the left eye (EARl) value.

$$EAR_i = \frac{(EAR_l+EAR_r)}{2} \tag{5}$$

The EARi value can detect a blink of the eye that is smaller than a threshold.
To calculate the standard deviation following equation is used.

$$\sqrt{\frac{\sum (x-\bar{x})^2}{(n-1)}} \tag{6}$$

Where x denotes the sample's average and n denotes the sample size. These procedures are worked out in frame units. Deepfake is then detected by comparing the measured data with the DeepVision's database that includes the natural movements of a human eyeblink. The accuracy of the proposed algorithm was 87.5% showing that it can overcome the constraints of integrity verification algorithms which are based on just pixels [31]. The drawback of the authors' algorithm is that Deepfake with a forged nose and mouth nose excluding eyes cannot be detected by DeepVision.

Afchar et al. [8] proposed a method that can detect if a video is authentic or not and the method especially focuses on Face2Face and Deepfake. Due to the compression that severely reduce quality of the data, conventional image forensics methods are normally not used to detect deepfake. As a result, the authors used a deep neural network with a limited number of layers. The proposed architectures Meso-4 and MesoInception-4 outperformed all the tests performed by the authors in terms of the classification scores, with a modest level of representation and remarkably minimal parameters. They collected 175 rushes of fake videos from the various sources and compressed them with different compression levels using H.264 codec. They were able to achieve detection rate of 95% and 98% for Face2Face and Deepfake videos, respectively.

TABLE 1. COMPARISON TABLE

Paper Number	Classifiers/Techniques	Dataset	Deepfake Detection Accuracy (%)
Rana and Sung [1]	DeepfakeStackClassfier	FaceForensics++	99.65
Younus and Hassan [2]	Blur Detection using Harr walvet transform	UADFV	90.5
Zhu et al. [3]	Clustering-based Embedding Regularization	UADFV	99.99
		Celeb-DF	99.95
		Deep Fake Detection	98.43
Kumar et al. [4]	Metric Learning	Celeb-DF	99.2
		FaceForensics++	90.71
Chen et al. [5]	DefakeHop	UDAFV	100
		FaceForensics++	97.45
		Celeb-DF v1	94.95
		Celeb-DF v2	90.56
Guarnera et al. [6]	Analyzing convolutional traces	CELEBA vs Deepfake datasets generated from multiple GAN	Max - 90.22
Jung et al. [7]	DeepVision	Self-created Deepfake dataset	87.5
Afchar et al. [8]	MesoNet	Deepfake one composed of online videos	98
		FaceForensics++	95
Joseph and Nyirenda [17]	Two-Stream Capsule Network	DFDC	73.39
		Celeb-DF	57.45
Stanciu and Ionescu [18]	CNN-LTSM	Celeb-DF	97.06
		FaceForensics++	99.95

IV. Conclusion and Future Work

In this paper, we did a comparative analysis of the most noteworthy research works on deepfake detection techniques. The benefits and drawbacks of adopting certain techniques for detection tasks were also explored. Each year more techniques to improve deepfakes as well as techniques to detect deepfakes are emerging therefore, we believe that this paper will provide a thorough understanding of the work, give the readers a grasp of the fundamental concepts of this discipline and offer light on future research.

References

[1] M. S. Rana and A. H. Sung, "DeepfakeStack: A Deep Ensemble-based Learning Technique for Deepfake Detection," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2020, pp. 70-75

[2] M. A. Younus and T. M. Hasan, "Effective and Fast DeepFake Detection Method Based on Haar Wavelet Transform," 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 186-190,

[3] K. Zhu, B. Wu and B. Wang, "Deepfake Detection with Clustering-based Embedding Regularization," 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), 2020, pp. 257-264,

[4] A. Kumar, A. Bhavsar and R. Verma, "Detecting Deepfakes with Metric Learning," 2020 8th International Workshop on Biometrics and Forensics (IWBF), 2020, pp. 1-6,

[5] Chen, Hong-Shuo & Rouhsedaghat, Mozhdeh & Ghani, Hamza & Hu, Shuowen & You, Suya & Kuo, C.. (2021). DefakeHop: A Light-Weight High-Performance Deepfake Detector.

[6] L. Guarnera, O. Giudice and S. Battiato, "DeepFake Detection by Analyzing Convolutional Traces," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2020, pp. 2841-2850, doi: 10.1109/CVPRW50498.2020.00341.

[7] T. Jung, S. Kim and K. Kim, "DeepVision: Deepfakes Detection Using Human Eye Blinking Pattern," in IEEE Access, vol. 8, pp. 83144-83154, 2020, doi: 10.1109/ACCESS.2020.2988660.

[8] D. Afchar, V. Nozick, J. Yamagishi and I. Echizen, "MesoNet: a Compact Facial Video Forgery Detection Network," 2018 IEEE International Workshop on Information Forensics and Security (WIFS), 2018, pp. 1-7, doi: 10.1109/WIFS.2018.8630761.

[9] Tewari, A., Zollhoefer, M., Bernard, F., Garrido, P., Kim, H., Perez, P., and Theobalt, C. (2020). High-fidelity monocular face reconstruction based on an unsupervised model-based face autoencoder. IEEE Transactions on Pattern Analysis and Machine Intelligence, 42(2), 357-370.

[10] Liu, M. Y., Huang, X., Yu, J., Wang, T. C., & Mallya, A. (2021). Generative adversarial networks for image and video synthesis: Algorithms and applications. Proceedings of the IEEE, DOI: 10.1109/JPROC.2021.3049196.

[11] Zhou, X., and Zafarani, R. (2020). A survey of fake news: fundamental theories, detection methods, and opportunities. ACM Computing Surveys (CSUR), DOI: https://doi.org/10.1145/3395046.

[12] Guo, B., Ding, Y., Yao, L., Liang, Y., and Yu, Z. (2020). The future of false information detection on social media: new perspectives and trends. ACM Computing Surveys (CSUR), 53(4), 1-36.

[13] Lyu, S. (2020, July). Deepfake detection: current challenges and next steps. In IEEE International Conference on Multimedia and Expo Workshops (ICMEW) (pp. 1-6).

[14] Guarnera, L., Giudice, O., Nastasi, C., and Battiato, S. (2020). Preliminary forensics analysis of deepfake images. arXiv preprint arXiv:2004.12626.

[15] Jafar, M. T., Ababneh, M., Al-Zoube, M., and Elhassan, A. (2020, April). Forensics and analysis of deepfake videos. In The 11th International Conference on Information.

[16] Trinh, L., Tsang, M., Rambhatla, S., and Liu, Y. (2020). Interpretable deepfake detection via dynamic prototypes. arXiv preprint arXiv:2006.15473.

[17] Z. Joseph and C. Nyirenda, "Deepfake Detection using a Two-Stream Capsule Network," 2021 IST-Africa Conference (IST-Africa), 2021, pp. 1-8.

[18] D. -C. Stanciu and B. Ionescu, "Deepfake Video Detection with Facial Features and Long-Short Term Memory Deep Networks," 2021 International Symposium on Signals, Circuits and Systems (ISSCS), 2021, pp. 1-4, doi: 10.1109/ISSCS52333.2021.9497385.

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

[20] de Lima, O., Franklin, S., Basu, S., Karwoski, B., and George, A. (2020). Deepfake detection using spatiotemporal convolutional networks. arXiv preprint arXiv:2006.14749.

[21] Amerini, I., and Caldelli, R. (2020, June). Exploiting prediction error inconsistencies through LSTM-based classifiers to detect deepfake videos. In Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security.

[22] Gandhi, A., and Jain, S. (2020). Adversarial perturbations fool deepfake detectors. arXiv preprint arXiv:2003.10596.

[23] Neekhara, P., Hussain, S., Jere, M., Koushanfar, F., and McAuley, J. (2020). Adversarial deepfakes: evaluating vulnerability of deepfake detectors to adversarial examples. arXiv preprint arXiv:2002.12749.

[24] Carlini, N., and Farid, H. (2020). Evading deepfake-image detectors with white-and black-box attacks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 658-659).

[25] Yang, C., Ding, L., Chen, Y., and Li, H. (2020). Defending against GAN-based deepfake attacks via transformation-aware adversarial faces. arXiv preprint arXiv:2006.07421.

[26] Bhowmik, A., Kumar, S. and Bhat, N., 2019, May. Eye disease prediction from optical coherence tomography images with transfer learning. In International Conference on Engineering Applications of Neural Networks (pp. 104-114). Springer, Cham.

[27] Fernandes, S., Raj, S., Ewetz, R., Singh Pannu, J., Kumar Jha, S., Ortiz, E., ... and Salter, M. (2020). Detecting deepfake videos using attribution-based confidence metric. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

[28] Li, Y., Yang, X., Sun, P., Qi, H., and Lyu, S. (2020). Celeb-DF: A large-scale challenging dataset for deepfake forensics. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 3207-3216).

[29] Karras, T., Laine, S., Aittala, M., Hellsten, J., L ehtinen, J., and Aila, T. (2020). Analyzing and improving the image quality of StyleGAN. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 8110-8119).

[30] Li, L., Bao, J., Zhang, T., Yang, H., Chen, D., Wen, F., & Guo, B. (2020). Face X-ray for more general face forgery detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5001-5010).

[31] Wang, S. Y., Wang, O., Zhang, R., Owens, A., & Efros, A. A. (2020). CNN-generated images are surprisingly easy to spot... for now. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 8695-8704).

[32] Malolan, B., Parekh, A., and Kazi, F. (2020, March). Explainable deep-fake detection using visual interpretability methods. In The 3rd International Conference on Information and Computer Technologies (ICICT) (pp. 289-293). IEEE.

[33] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion, 64, 131-148.

[34] Kumar, S., Mallik, A. and Panda, B.S., 2022. Link prediction in complex networks using node centrality and light gradient boosting machine. World Wide Web, pp.1-27.

[35] Bhowmik, A., Kumar, S. and Bhat, N., 2021. Evolution of automatic visual description techniques-a methodological survey. Multimedia Tools and Applications, 80(18), pp.28015-28059.
[36] Kumar, S. and Kumar, M., 2018, July. A study on the image detection using convolution neural networks and TenserFlow. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 1080-1083). IEEE.