International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Deep Learning Based Web Data Classification Techniques for Forensic Analysis: An Overview

Ms. Shital B. Pawar[1], **Prof. Dr. Kamini A. Shirsath**[2]

Submitted: 07/09/2023 **Revised:** 21/10/2023 **Accepted:** 06/11/2023

Abstract: The rapid advancement of artificial intelligence (AI), machine learning (ML), and deep learning (DL) over the course of the previous several decades has led to the development of a variety of novel methodologies and tools for the manipulation of audiovisual. Even though technological advancement has been utilized for the most part in acceptable uses, like being used for entertaining and educational purposes, etc., fraudulent people have nonetheless found ways to abuse it for illegal or evil objectives. For instance, high-quality and convincingly authentic fake videos, photos, or audio recordings have been produced with the goals of disseminating false data and disinformation, sowing the seeds of political dissension and hatred, and even intimidating and blackmailing individuals. Deepfake is a relatively new term that refers to videos that have been modified but nevertheless maintain a high level of quality and realism. This application's intuitive qualities have contributed to a widespread rise in its appeal among the general public, and it is currently being utilized in a variety of fields, including fraudulent transactions, online criminal activity, politics, and possibly military operations. Therefore, it is of the utmost need to establish a variety of methods for detection that are capable of doing away with this kind of forgery and putting up an entirely novel approach in audio as well as video forensics. In this research work, the numerous detection strategies are presented that have been currently under investigation in the field of Deepfake research. So as to serve as the backbone for the creation of a new technique that would be more compressible and effective in identifying the presence of Deepfakes, this will be necessary. Also, a research investigation was conducted to compare different methods that are used in conventional methods with those that are used in state-of-the-art approaches. The investigation came to the conclusion that the majority of the methodologies that are used in conventional approaches are processes that take a lot of time, require skill and understanding of the technology for the individual attempting to use them, and so on. An introduction is given to the technological issues posed by DeepFake detection, as well as the methods researchers use to devise potential solutions to this issue. The benefits and disadvantages for every sort of solution, in addition to any possible hazards and disadvantages, are dissected and analyzed here. Despite this advancement, there are still a variety of significant issues that need to be fixed before present DeepFake detection approaches can be considered fully viable. Several of these issues are brought to light, and a discussion of the investigation prospects available in this field follows.

Keywords: *DeepFake Detection, Deep Learning, Forensic, Web Data*

1. Introduction

DeepFakes are a recent development that adds a new dimension to the troubling issue of the web misinformation. DeepFakes are deceptive pictures and movies that are generated by artificial intelligence systems. The fabrication and modification of digital images and videos is not a new concept; however, the rapid growth of deep neural networks (DNNs) over the past decade has made the technique of making believable false photographs and videos much simpler and quicker. This is due to the fact that DNNs have allowed for more accurate facial recognition. When a Reddit user with the identical name started releasing fake pornographic movies produced with a deep neural network based face-swapping technique in late 2017, DeepFake videos were first brought to the notice of the general public for the first time. As a consequence of this, the methods that allow for the creation of DeepFakes are being integrated via the use of programming code that is easily accessible and freely accessible on GitHub.1 These are also new web services being developed as well as start-up businesses that have industrialized software that can make DeepFake films whenever they are requested.

There are primarily three categories of DeepFake videos available right now.

• Head puppeteer comprises synthesizing footage of an intended person's full head and above shoulder employing a film of an original person's forehead, so the composite target appears to act in the exact same manner as the real person. This is accomplished through the use of a video of the original the individual's head.

[1] *Research Scholar: Dept. of Computer Engineering, K.K.Wagh Institute of Engineering Education and Research Nashik, Savitribai Phule Pune University, Pune MH India*
[1] *ssbhandare@kkwagh.edu.on*
[2] *Research Guide: Dept. of Computer Engineering, K.K.Wagh Institute of Engineering Education and Research Nashik, Savitribai Phule Pune University, Pune MH India*
Professor and Head Sandip Institute of Engineering and Management Nashik SPPU, Pune MH India
[2] *Kamini.nalavade@siem.org.in*

- Producing a video of the person being targeted with its visages substituted with the generated faces of the original source while maintaining the same facial emotions is required for face switching.
- Lip syncing is the process of creating a fabricated video by just altering the subject's lip area to give the impression that they are speaking a language that they do not actually communicate in actual life.

DeepFake films are capable of being armed despite the fact that they can be put to use in a variety of innovative and intriguing ways. This is because of the close relationship that people have with their looks and their identities. DeepFake movies that have been carefully created have the ability to generate impressions of an individual's existence and behaviors that are not present in fact. This has the potential to have major repercussions for politics, society, the economy, and the law [1]. The possible hazards include things like retaliatory pornographic clips of victims with their faces digitally manipulated and spliced in, films that appear to show state leaders making incendiary statements that they haven't actually said, a senior executive talking about her business's achievement in order to affect the worldwide stock market, and video conversations in which a digital sexual predator poses as an immediate family member or a close companion.

Due to the first identified case of DeepFake videos surfaced in the month of December 2017, growing worries throughout the adverse effects of DeepFakes have resulted in a growing curiosity in DeepFake detection in the Multimedia Forensics investigation community. The very first devoted DeepFake detection technique was invented by group in June 2018, [2] and it was published in the journal Digital media Forensics. As a consequence of this, there has been a flurry of activity regarding the creation of numerous DeepFake detection systems over the course of the past couple of years. In a similar vein, there are additionally various large-scale baseline data sets created in order to assess the efficacy of DeepFake's fake detection. DeepFake identification has also received assistance from public funding bodies as well as business entities.

The culmination of all of these initiatives will be the first DeepFake Detection Test, which will take place between the end of 2019 and the beginning of 2020. In general, the results of the DeepFake Identification Challenge reflect to the current state of the art, revealing the best methods representing a tour de force of cutting-edge DNNs (the top performance achieved a mean precision of 82%). These offer with excellent methods for uncovering DeepFakes, which are digital forgeries that are automatically generated in large quantities by AI algorithms. On the other hand, one must exercise extreme caution when interpreting these data. Even though the team behind the event have made a concerted effort to recreate the situations in which DeepFake videos are used in everyday life, there currently is still a substantial gap among the results on the assessment dataset and the results on the true dataset. When examined on undiscovered videos, the highest performer's accuracy dropped to 65.18%, indicating that the the highest performer's accuracy could be improved. Furthermore, each of the proposed solutions is predicated on ingenious layouts of DNNs as well as information augmentations; nonetheless, they offer very little knowledge that goes above the "black box" categorization methods. Additionally, it is possible that these outcomes for detection do not perfectly represent the real identification effectiveness of the technique on an individual DeepFake film. This is particularly true for videos that have undergone extensively manipulated and refined after being produced by AI methods. DeepFake movies that have been "crafted" in this manner are more probable to produce genuine harm, and thorough hand post processing has the potential to decrease or remove abnormalities that the identification techniques rely on.

In this research work, a look at the most recent developments in the field of DeepFake detection algorithms is taken. The procedural obstacles that must be overcome in order to identify DeepFakes are presented, as is the method investigators use to devise possible remedies to this issue. The positive and negative aspects of every sort of an approach in addition to any potential dangers and disadvantages, are dissected in this article as well. A summary of the research attempts for DeepFake identification as well as an in-depth assessment of the currently available datasets, algorithms, and results are illustrated below. Despite all of this development, however are still plenty of significant issues that need to be fixed before present DeepFake detection systems can be considered fully viable. A couple of these difficulties as well as the opportunity for study in this path are discussed about.

2. Background Study

2.1 DeepFake Video Generation

Even if over the past few years there have emerged a lot of advanced techniques for producing realistic artificial face films [3, 4, 5, 6, 7], the majority of these programs have yet to appear in the public as open-source programs that anybody can use. It is a much easier technique that is built on the concept of neural image transfer of style [8], and it gets the tool that is utilized to make DeepFake films at scale. There are multiple separate open-source applications of this technology. This technique is commonly known as the fundamental DeepFake creator, and it is the foundation of many DeepFake movies that have been circulating on the internet or in the databases that are currently available.

Faces of the intended subject are identified from the video footage that is being input, and then facial characteristics are retrieved from those identified faces. [9] The points of reference are what are utilized to position the faces so that they are in the usual layout. After the faces have been aligned, they are trimmed and sent into an auto-encoder. This allows the auto-encoder to generate donor faces that have identical emotions as the features of the target that was originally selected.

The auto-encoder is typically created by combining the encoder and the decoder, which are both examples of CNNs. Encoder E is responsible for transforming the face of the input subject into a vector that is referred to as the code. There is only one encoder used, and it does not matter who the participants are; this is done so that the encoder can accurately record identity-independent characteristics like facial expressions. On the opposite side, each person's identity is paired with a specific decoder known as Di, that interprets in a code and produces a face for the individual that corresponds to that code. Both the encoding algorithm and the decoder are trained simultaneously in an unsupervised way utilizing uncorresponded face sets of many different people as training data. To be a bit more precise, an encoder pair is produced by alternatingly employing E as well as Di for the input face for every participant, and its variables are optimized in order to reduce the amount of mistakes that occur during reconstruction. Back-propagation is used throughout the process of updating the parameters until convergence is reached.

After that, the synthetic faces are distorted so that they match the configuration of the faces of the initially created target, and then they are pruned using a mask comprised of the facial features. In the final stage, the edges of the synthesized sections and the initial footage frames will be blended together to create a smoother transition. The majority of the steps in this procedure are carried out automatically, and only a few require human interaction.

2.2 Categorization Existing DeepFake Detection Methods

2.2.1 Categorization based on Methodology

The currently available approaches for detecting DeepFake can be divided down into 3 separate categories. The first two methods accomplish their goals by searching DeepFake videos for particular artifacts that set them apart from actual footage.

2.2.1.1 Signal Feature-Based Methods

The signal feature-based approaches (such as [10, 11, 12, 13]) check for irregularities at the level of the signal by considering the videos as a series of frames f (x, y, t) and a coordinated audio stream a(t) if a soundtrack is present in the footage. If the acoustic track is present, these techniques additionally search for the presence of a soundtrack. These kinds of anomalies are frequently brought on by one or more of the computation phases involved in the development of DeepFake.

For example, new research [13] takes advantage of the signal artifacts that are produced as a result of the scaling and scaling processes that take place throughout the additional processing of DeepFake creation. In the same way, the research presented in [14] emphasizes the boundary region that results from the blending of the synthetic face regions with the initial frame. Due of the upsampling technique, the researchers found of note in [15] that synthetic faces frequently exhibit irregularities in high frequencies. This is owing to the fact that the procedure. On the basis of this fact, a straightforward identification technique for the frequency realm is suggested as a potential solution. In the paper [16], the method for detection begins with a standard frequency-domain evaluation and then moves on to an SVM classification model. The research described in [17] applies the EM technique to the task of extracting a collection of local characteristics in the frequency domain. These characteristics are then put to work in order to differentiate between each frame of DeepFakes from the ones of real movies.

The fact that anomalies are typically essential to the production procedure is the primary benefit of using signal feature-based approaches. Fixing these outliers may involve considerable adjustments to the fundamental DNN structure or additional processing procedures. On the contrary, as signal characteristics are relied on, DeepFake identification techniques which depend feature-based on signals are vulnerable to disturbances to the signals, which involve interpolation (up-sizing, down-sizing), addition noise, distortion, and compression.

2.2.1.2 Physical/Physiological-Based Methods

The physical and physiologically based techniques, such as [2, 18, 19, 20, 21], uncover DeepFake films due to the fact that they violate the fundamental principles of physiology or the laws of physics The deep neural network algorithm that is used to synthesize human appearances does not have a firsthand understanding of the biological features that characterize human face or the laws of physics of the setting in which they are situated. However, this knowledge may be included into the framework implicitly (and inefficiently) via data used for training. The absence of information might lead to characteristics that can be recognized, which are also obvious to people. In this regard, an initial approach that was specifically designed to identify DeepFake [2] operates by identifying the irregularity or lack of natural eye movements in DeepFake films. This is since the data used for training for the DeepFake generation system are frequently collected from the web in the form of portrait photographs of a topic. This is how the algorithm learns to generate fake content. Since the majority of portrait photographs include the person with their eyes wide, the DNN generation algorithms that undergo training using these pictures can not replicate the person's eyes shut in order to simulate genuine eye blinking. The work of [18] capitalizes on of the physical deviations that occur in the head postures of the DeepFake films as a result of the merging of a computer-generated face area into portions of the initial footage. The research presented in [19] provides a concise summary of the numerous visual errors that may be seen in DeepFake movies. Some of these artifacts include uneven eye hues, absent reflections, and fuzzy features in the eye and dental regions. The researchers then present a set of straightforward characteristics that can be used to identify DeepFake. The research presented in [20] presents a DeepFake identification technique that relies on the extraction biological information from parts of the face that are undetectable to the human gaze in profile movies. For example, the minor color shifts that occur as a result of the circulation induced by cardiac activity are one example. The coherence of space and temporal coherence can be deduced from these signals in biology.

The superior ease and capacity for clarification of both physical and physiologically oriented procedures is the primary benefit of these types of approaches. This is of utmost significance in the event that the outcomes of the identification are utilized by specialists including journalists. On the opposite end of the spectrum, identification approaches that relies on mechanical or biological mechanisms are constrained by the efficiency and resiliency of the machine vision methods, and their excessive reliance on lexical signals also restricts the range of situations in which they can be used.

2.2.1.3 Data-Driven Methods

The third type of identification approaches consists of data-driven methods (for example, [22, 23, 24, 25]), which aren't aimed at particular characteristics but instead use movies that have been annotated as legitimate or DeepFake to train machine learning algorithms (particularly in DNNs) which are able to distinguish genuine footage from DeepFake videos. It should be noted that feature-based approaches can also use DNN classification methods; hence, what differentiates data-driven techniques from techniques based on features is that the signals for categorizing the two distinct kinds of movies are implied and are discovered by machine learning models. As a result, the effectiveness of data-driven approaches is heavily dependent, not only on the quantity and variety of training data, but also on the structure of the machine learning algorithms themselves.

The initial data-driven DeepFake detection approaches made use of conventional DNN methods, which were originally created for other machine learning tasks including identifying objects and categorization. In addition, there are approaches that make advantage of more specialized or original network structures. MesoNet [10] is a rapid identification technique that analyzes its identification findings by associating these with certain mesoscopic layer visual properties. It does this by using an adapted DNN models to identify DeepFakes, which were previously undetectable. The DeepFake identification approach proposed by Liu et al. (2020) utilizes the capabilities of the Gram-Net to identify changes in the image's overall structure. The Gram-Net differs from the traditional CNN framework because it includes supplementary "Gram blocks" that are able to construct Gram matrices at various stages of the network's complexity. The identification techniques described in [24] make utilization of capsular systems, and they demonstrate that this technique can produce comparable results to those obtained by CNN-based models while using a reduced number of variables.

It is important to note that the current state-of-the-art efficacy for DeepFake identification is accomplished with data-driven techniques that rely on massive amounts DeepFake datasets as well as novel model development as well as training techniques. For example, the highest participant of the DeepFake Identification Challenge relied on the implementation of an ensemble DNN framework that included seven different EfficientNet models [27]. This was accomplished by using an ensemble DNN framework. The technique that came in second place, similarly makes application to ensemble algorithms, such as EfficientNet and XceptionNet models. However, it also introduces a novel data augmentation technique called WSDAN, which is designed to predict the different combinations of appearances.

2.2.2 Categorization Based on Input Types

The nature of the inputs can also be used as a criterion for classifying the various DeepFake detection algorithms that are currently in use. The vast majority of currently available methods for detecting DeepFake rely on binary categorization at the video frame level. This means that they determine the chance of a particular frame being genuine or DeepFake. Additionally, there are two problems that are associated with using frame-based identification approaches, despite the fact that they are straightforward and straightforward to apply. To begin, the consistency of time between frames is not specifically examined, despite the reality that (i) a great number of DeepFake films have temporal distortions and (ii) authentic DeepFake frames generally appear at consistent intervals. Furthermore, while a video-level integrity rating is required, it requires a further procedure to be taken, which is that one must collect the scores throughout each frame in order to arrive at an appropriate score. Whenever doing so, onecan choose from several different types of aggregation criteria, the most frequent of which are the average, the highest possible score, and the mean of top range. On the contrary, some temporal approaches, such as [22, 28, 29], utilize the entire frame series as its input and employ the temporal relationship among the photos as an inherent characteristic. These techniques may be found in [22, 28, 29]. Temporal approaches frequently make utilization of sequential algorithms like RNNs as the fundamental model framework, and immediately output the degree of forecast for the footage. The aural track is also used as a source of information for the audio-visual recognition algorithms, and DeepFakes are identified depending on the inconsistency that exists among the audio files and the picture frames.

2.2.3 Categorization Based on Output Types

A great deal of currently available approaches for detecting DeepFakes formulate the issue as a binary categorization. This means that they produce an identification for every input clip that indicates whether the footage is actual or a DeepFake. This is true irrespective of the fundamental approach or kinds of input. The projected labeling frequently come accompanied by a score of confidence that corresponds to a real value that falls within the range [0, 1]. This confidence score can be read as the chance that the input belongs to a particular of the classes (that is, real or DeepFake). A few distinct approaches take this concept and expand it to the realm of multi-class classification issues, in which the labels additionally take into account the various DeepFake generation algorithms. Furthermore are also ways that handle the location issue (for example, [30]), which additionally determines the spatial area (in a series of box boundaries or a masked out area) and time period of DeepFake operations.

2.2.4 The DeepFake-o-Meter Platform

Regrettably, the abundance of DeepFake detection techniques was not utilized to their maximum potential. On the one hand, the fact that numerous investigations use distinct training datasets, equipment, and training structures makes it difficult to conduct comprehensive evaluations between the various methods utilized for detection. On the other side, the majority of users are unable to utilize the most sophisticated DeepFake identification techniques since it is such a tedious process to acquire, configure, and run different detecting algorithms. In order to achieve this goal, DeepFake-o-meter is developed, which is a free platform for DeepFake identifications. An Application Programming Interface (API) design is provided for programmers of DeepFake identification methods, allowing them to encapsulate specific algorithms and execute them on an external server hosted by another company. It serves as a review and benchmarking framework for academics, allowing them to contrast various methods based on an identical input. Users get access to a user-friendly interface via which they can make use of several cutting-edge detecting methods. At this time, the 11 innovative techniques were integrated for detecting fake images and videos using the DeepFake platform.

2.3 Datasets

One of the prerequisites for the advancement of DeepFake detection techniques is the accessibility of huge data sets of DeepFake movies. As it first became available in the month of June, the initially released DeepFake dataset known as UADFV [18] contained just 49 DeepFake films that had noticeable artifacts. Following this, other DeepFake datasets are put forward, each with an increase in the quantity and quality of information.

- **UADFV** [18]: This dataset comprises 49 genuine films that were obtained from YouTube and utilized to build 49 DeepFake films. The dataset additionally contains 49 phony videos.
- **DeepfakeTIMIT** [31]: The original movies that are included in this dataset originate out of the VidTIMIT dataset. From those clips, an aggregate of 640 DeepFake movies have been created.
- **FaceForensics++** [23]: A forensics dataset known as FaceForensics++ is comprised of one thousand different original video clips that were artificially altered using one of four different automatic face alteration techniques. These techniques are known as DeepFakes, Face2Face, FaceSwap, as well as NeuralTextures.
- **DFD**: In the databases of Google as well as Jigsaw DeepFake identification dataset, there are a total of 3,068 DeepFake films. These were made from the initial recordings of 363, which were provided by 28 persons of varying ages, sexes, and ethnicities.
- **DFDC** [32]: The Facebook DeepFake Detection Challenge (DFDC) Dataset is a component of the

DeepFake detection test, which consists of 4,113 DeepFake films that were made according to 1,131 actual footage of 66 persons who gave consent to it and whose sexes, age groups, and ethnic backgrounds varied.

- **Celeb-DF** [33]: The Celeb-DF dataset includes both genuine and DeepFake-generated videos, all of which have a visual appeal comparable to that of films that are widely distributed web. It features 590 authentic videos taken from YouTube and containing people of various ages, ethnicities, and races, as well as 5,639 films through DeepFake that correlate to those authentic films.
- **DeeperForensics-1.0** [34]: DeeperForensics-1.0 is made up of ten thousand different DeepFake films that were produced by an entirely novel swapping of faces architecture that is built on DNN.
- **DFFD** [35]: The DFFD collection includes three thousand movies demonstrating many sorts of computerized manipulation, including identification swapping, emotion swapping, attribute deceit, and completely generated faces.

3. Literature Survey

In this section, the many different kinds of published research has been discussed that have been done in the field of Deepfake production and identification. Raahat Devender Singh et al. [36] present an in-depth analysis of the different methods for authenticating video information. These methods are typically split up into active and passive designs, and the purpose of this study is to provide a comprehensive assessment of the many passively blind footage authentication methods, with the primary emphasis being placed on detecting forgeries, recapturing videos, and identifying phylogenies. Further on, with the advent of DL, Deepfake became prominent across an extensive range of individuals owing to the excellent quality of the manipulated movies that were made and the simplicity and ease to utilize offered by the internet-based Deepfake creation and face-swapping programs that were built using DL methods. This popularity was owing to the fact that Deepfake was able to produce tampering films of high quality. DL is well-known for its capacity to handle data with a high number of dimensions and complex structures. In earlier times, algorithms including encoder-decoder or auto encoders were employed to handle a variety of issues in the field of machine vision. These models are still commonly used today. In contrast to the more modern CNN, however, early auto encoders possessed a number of drawbacks that can be summarized as follows [37]. The absence of temporal awareness is the primary cause of a number of anomalies that can be found in auto encoders. This is the first of several potential drawbacks. Since the auto encoder does its evaluation of the Deepfake films using a frame-by-frame generation and proved completely oblivious of any already produced face which it could have produced immediately, it was unable to make a fake face mechanically. The subsequent problem is the discrepancies that are present with the face encoder. For example, the encoder does not take into account the individual's skin tone or additional background data. When integrating the freshly added picture with the remaining components of the frame, border effects are extremely frequent and should be expected. It is difficult for the auto encoder to produce films that are particularly realistic and precise when used in a variety of settings because of the visual discrepancy that occurs as a result of the utilization of various recording devices, variable lighting circumstances, or merely the usage of various video codecs. This is the one-third of the system's drawbacks. In the end, the problem is that there is no uniformity in the selection of the lighting across the many backgrounds and frames. This typically results in flickering in the facial area throughout the vast majority of the Deepfake films. CNN, Recurrent Neural Networks (RNN), and GAN, amongst other DL strategies, were created as a means of compensating for the shortcomings of auto encoders.

With the development of this CNN, several more methods have been created for the development and identification of Deepfake. These methods include RNN, Long Short-Term Memory (LSTM), as well as mixed methods of all the most recent algorithms in DL, amongst others. In the first stage of the method, which is described by David Guera et al. [37], the frame-level characteristics are obtained out after all analyzing in a CNN. These characteristics are subsequently introduced into the RNN as training data, and what is obtained from this RNN is the outcome of the classification. In addition to the amalgamation of CNN and RNN, an assortment of encoder-decoder networks with shared weighting for the network that encodes is also utilized for decreasing dimensionality and picture reduction throughout the training and production stage. Finally, a network using LSTM is employed for the evaluation of temporal order in sequence. The human face manipulation identification utilizing RNN methods has been put up by Ekraam Sabir in [38]. In this method, they employ an assortment of deviations in RNN models in addition to domain-dependent face pre-processing methods to achieve outstanding results on freely accessible facial manipulation footage produced via FakeApp, Face2Face, and FaceSwap. The test results indicates that this method has an accuracy of 4.55%. Identification of swapped faces was discussed using a method quite similar to the one presented in [39], which combined DL with Subjective Evaluation. Whenever contrasted with the various systems that are already available, the approach that they designed and described in this study has a positive detection rate of 96% and less false alarms than the rest of the systems. In addition to identifying instances of face-swapping, this algorithm assesses the degree of ambiguity associated with every forecast. This is an extremely important factor to consider when determining the effectiveness of an approach. They have established an internet presence in order to examine how people react throughout the dataset by gathering paired to pair comparisons of depicts over films on human beings. The goal of this is to increase the dependability of the results. Pictures are determined to be either authentic or false according to the assessments made here. This categorization output is contrasted with the results that result from their autonomous approach, which produces a very excellent, but somewhat incomplete, correlation with a linear correlation that exceed 0.75. The results can be determined by some form of likelihood, and this categorization output is contrasted with those outputs. The findings of this experiment indicate that the model being suggested is a significant improvement over the procedures that are currently in place.

An implementation of a hybrid strategy was used for the most recent and most powerful iteration of this DNN. They train a GoogLeNet to identify manipulation artifacts such as powerful edges close to lips, distorted regions on the face, etc. in the classification of the image flow, and in the subsequent stream, they ought to train a patch-based three-layer structure for gathering native noise parts and camera traits. The two-stream NN was suggested in [40]. The purpose of developing the aforementioned network was to assess the possibility that both of the patches that were obtained were taken from an identical image. It was discovered that the patchwork taken from the true samples surrounding the area of the face appear to be very straightforward and has an extremely tiny distance between them. On the other hand, in the instance of the tampering video, the patched form the face area will be distinct and are going to have wider space among them. This was discovered by comparing the two sets of patchwork. Also, if the footage has been interfered with, the attributes of the frames that are close to the facial will appear distinct from those of the original or genuine film, and the categorization according to these features is carried out with the assistance of an SVM classifier in this scenario. They created a second dataset that was produced through 2 web face-swapping applications. This dataset is made up of 2010 photos that have been modified, and all of these images includes a fabricated profile so that its performance can be evaluated. The findings of the experiments indicate that this method may identify both controlled artifacts and concealed noisecomponents.

A further concept that was included in the hybrid framework was something called pairwise training [41]. This is a technique that uses a method based on DL to determine whether or not a picture has been modified through the use of the contrastive loss. To begin, a GANs network that is up to date will be utilized in order to produce a pair of false and real photos. The next step is to use an algorithm called the common fake feature network (CFFN) to discover the key difference that separates the false picture and the genuine picture using the paired data gathered from both of these image instances. After that, in the next and last the platform, a tiny network will be employed to amalgamate all of these characteristics in order to reach a judgement regarding whether or not it is authentic. The findings of the experiments reveal that the suggested approach has excellent results in comparison to other image detection methods that are currently considered state of the art. A focused on tasks GAN utilizing PoISAR image clustering and classification methods was utilized in the study that was referred to in the literature [42]. This GAN consisted of a Triplet network. They are a third network that is referred to as the task networking or T-net. This network is comprised of the producer and the discriminator, respectively. The network of neurons that is used in the suggested system generally consists of two different task networks; the first of these is known as the classifier the network, and the second is known as the clustering network. The initial phase is the period of learning, and it consists of two different generating and discriminator networks that compete with one another while functioning together, just like GANs do. In the subsequent phase, the generator network's structure is modified and orientated as a Task networks. This means that during this phase, certain samples from the original training sets are assigned with specific tasks, one of which is the generation of the manipulated data. This not only makes use of the benefits of a GAN system but also helps mitigate the issues that are associated with using a GAN network. Following the conclusion of the learning stage, the altered data are utilized to focus on the role of improving the sets used for training and preventing excessive fitting among instances. As a result, role-Oriented GAN is able to function effectively regardless of the amount of manually tagged information is limited. A graphical comparison is presented in order to check the reliability of the Task Network. The contrast shows some modified digits created from Project-Oriented GAN in tandem with those produced by GAN, as shown in the example. The primary point to keep in mind is that there is more of a distinction among the PolSAR image data and the PolSAR image dataset that is employed in this method as the photograph.

This is the PolSAR image dataset that is utilized in this method as the photograph. The efficacy of the approach is examined by numerous tests using this PolSAR picture dataset, and the results suggest that the suggested technique demonstrates good accuracy when dealing with PolSAR image grouping and classification on three different PolSAR images.

Following through, an LSTM as well as Encoder-Decoder mixed architecture [43] was created for the purpose of detecting image counterfeiting. In this particular system, a high-confidence design is implemented. This framework makes use of resampling characteristics, which are then used to the task of capturing artifacts. These imperfections consist of a loss of JPEG quality, as well as up collection, down collection, movement, and other similar operations; LSTM cells; and an encoder-decoder system to determine the existence of a particular section of the image has been altered. In this case, they combine the efforts of LSTM and Encoder networks to discover the different features of the modified and non-manipulated areas by using the spatial map and the amount of frequency domain association. Ultimately, in order to identify tampering, the decoder network must understand how it converts from low-resolution map features to pixel-wise forecasts. They also give a dataset which can be utilized in subsequent study work pertaining to multimedia forensic as a result of this group of research. They came to the notion that their approach divided multiple kinds of operations such as copy-move, object elimination, and merging in an effective manner after conducting a number of tests with a variety of datasets. In the realm of DL, the active training strategy was also mentioned [44] as a larger progression to obtain annotating for information gathered from responses from humans by grabbing useful data with an elevated likelihood to boost efficiency. This was done in order to improve the accuracy of the model. The above framework is put into action in order to produce an identifier for the data in the most cost-effective way possible. In this case, a reward will be awarded to every instance by the classification algorithm that was trained based on these pre-existing tags, and these incentives may be employed to lead a constrained GAN to produce data that are useful and instructive while also having an increased likelihood for an identified label. In conclusion, the assessment of this model allows for a projection of the efficacy of the approach, indicating that the samples produced have the potential of increasing categorization efficiency for common picture tasks such as classification. This projection is made possible by the fact that the algorithm is being evaluated. After that, particular pre-processed genuine and counterfeit images [45] are able to be utilized for training the CNN algorithm for use in the generation. This eliminates the unreliable low-level noise indications on the controlled pictures, and the discriminative share is compelled to acquire additional distinct characteristics in order to differentiate between the controlled and genuine facial pictures. The employment of an image pre-processing phase during the training phase is the primary distinction between this approach as well as other GAN-related approaches. This step destroys low-level unstable artefacts in GAN pictures, which compels the machine learning system to concentrate on more distinguishable cues and, as a result, results in improved generalisation abilities. However, putting this strategy into action was a challenge, and it has produced only a few tentative outcomes. Because of this, a strategy for detecting face wrap artifacts was devised [46] in order to increase the discriminative abilities. The existing Deepfake techniques can produce pictures with a poor image quality, therefore this approach was built based on the finding that more wrapping is required to align the modified one with the same resolution as the initial one. This technique was created as a result of the finding. Therefore, this transformation yields an artifact following the line of false one termed resolution discrepancy, and such anomalies can be efficiently collected utilizing a network like CNN for the purpose of determining whether or not movies are legitimate.

Although many alternative methods, including indirect implementations of DL, were also put into practice in conjunction with the initial approaches, the results of these methods show a lower level of accuracy in comparison to those of other current methods. A particular approach was suggested by Pavel Korshunov et al. [44], in which it was described how a computerized system could be constructed for identifying the forgeries in videos that were captured in the camera's memory as well as in the audio stream of the lens. In this case, they applied a technique where they discover audio-visual discrepancies with specific artifacts such as lip syncing, Dubbing errors, and other such issues. During the experiment's assessment, the suggested approach is tested with a number of different classifiers, including the LSTM, GMM, and PCA, among others; nonetheless, the LSTM yields the best results, which can be seen as a limitation of the system. Huy H. Nguyen et al. [47] describe a kind of capsule forensic conduct in which they utilize a network of capsules for identifying the discrepancy in the relive attack employing created videos and images in addition to the computer-generated footage employing DCNN. This method was used in identifying the presence of the counterfeiting in the pictures and films. Another method of this kind was a capsule forensic strategy. The purpose of the test was to determine whether or not it would be possible to develop a standardized method of detection that would be capable of identifying instances of photo and video forgery. In this case, the network of capsules can be utilized in the field in addition to machine vision, during its training period of which it utilizes data of unknown noise. The protection of random data from both machine and hybrid assaults was the primary objective of this body of research. Another method is the Eye blinking detection [48], in which the temporal aspects of the eye and the inconsistencies in the eye blinking are recognized to determine whether or not the file containing the sample has been manipulated.

Finally, a detail on an uncommon strategy that is completely distinct from the realm of DL and that can be utilized for the forgery detection in described in [49]. In that article, the authors apply a Photo Response Non-Uniformity (PRNU) assessment in order to identify the deep fake video alteration. In this method, the films are separated into their component frames, and the portions of the frames that represent the face are trimmed. After then, the mean correlation among the genuine and Deepfake one is determined in order to figure out which one is phony and which one is not. This approach was also utilized in order to ascertain the level of manipulation included in every Deepfake clip. Analysis conducted by PRNU reveals a significant disparity among the mean normalized cross-correlation ratings of actual and Deepfake media. In the beginning stages of the deployment of identifying methods, there was not a great deal of academic paper discovered on the subject of the identification of Deepfake. Despite the fact that attempts have been made to identify and delete movies of this nature from websites, certain sites continue to host them. Gyft makes an effort to identify discrepancies in the area of the face of a transmitted video by employing machine learning and technology that recognizes facial features.

Comparison Chart on Various Deepfake Detection Technologies

The table below shows the summary chart on the various Deepfake Detection Technologies mentioned in the related works.

Author	Framework	Features	Pros	Cons	Dataset Used
David et al. [37]	CNN, RNN	A pipeline that is aware of time and is able to instinctively identify Deepfake videos.	Obtain competitive outcomes for this endeavor while utilizing a straightforward framework.	Efficient with videos as short as a matter of seconds in length.	300 films sourced from a variety of film hosting web pages, and another 300 videos collected from the HOHA dataset
Ekraam Sabir et al. [38]	CNN, RNN	Suggest the most effective way to combine the varying CNN algorithms and face pre-processing methods that are appropriate to the domain.	More effective than the most recent state-of-the-art methods currently in use	With the substantial rise in the settings put up in the various layers, it demonstrates a very poor effectiveness in multi-layer RNN	FaceForensics ++ dataset
Xinyi Ding et al. [39]	DL, Face swapping	In order to identify swap of face, deep transfer learning is used.	Include a measure of uncertainty with the results for every forecast.	Offer a lower accuracy rate relative to individuals when compared	It is now possible for everyone to access one of the most extensive face swapping datasets consisting of still photos.
Peng Zhou et al. [40]	Two-Stream NN, RNN	Analyze the camera's properties as well as the surrounding noise elements as when search	This method can learn both controlled artifacts and concealed noise elements at the same time.	-	2010 digitally altered photographs make up the dataset that was produced by two different web face-swapping applications.

		for manipulation artifacts such as razor-sharp edges around the lips and fuzzy patches on the face.			
Chih-Chung Hsu et al. [41]	CFFN, RNN, GAN	Integrating the contrastive loss with a technique that utilizes DL can be utilized to determine whether or not a photograph has been edited.	In regards to accuracy as well as recall rate, it achieved superior results compared to other cutting-edge approaches.	-	CelebA Dataset
Fang Liu et al. [42]	GAN, Image Clustering, PoISAR	Gain an understanding of the challenges associated with PoISAR interpretation of images and experience finding solutions to sample-sized difficulties.	It has provided excellent results, and it may be used to a large number of additional databases.		PoISAR datasets
Jawadul H. Bappy et al. [43]	Hybrid LSTM, Encoder Decoder	For classification purposes, broader receptive fields including a frequency-domain association are utilized.	Efficient across a wide variety of forms of manipulation, including copy-move forgeries, item elimination etc.	-	A substantial image splicing dataset has been presented.
Xinsheng Xuan et al. [45]	CNN	Uncertain low-level noise elements are eliminated, and a greater emphasis is placed on inherent characteristics in the classification process.	More efficient than the one that is currently in use	However, some preliminary findings were reached.	CelebA-HQ
Yuezun Li et al. [46]	CNN	Find the unique artifacts that are only present in the fraudulent videos and report them.	Does not need images produced through Deepfake to be used as	Essentially, less robust when used to a variety of video methods of compression	DEEPFAKE TIMIT

			unfavorable samples for training.		
Pavel Korshunov et al. [44]	Lip syncing, dubbing detection, GAN, LSTM, GMM, SVM, MLP	A computerized system that can identify irregularities in the audio and video	Only LSTM showed improved performance in the test across each of the three datasets.	There was not a single technique that produced an outcome that was superior to LSTM.	VidTIMIT, AMI, and GRID
Huy H. Nguyen et al. [47]	Capsule Network, Deep CNN	A method to identify forgeries in images as well as videos had been suggested.	Capsule Network's applications have been widened so that they now encompass DNN	There is a necessity to be more resistant against mixed attacks.	Visuals and moving pictures created by a computer
Li Y. et al. [48]	Eye Blinking, LSTM [48]	Analyse the temporal characteristics of Eye by using LRCN.	Technique that is effective under images of the face	Only operates with photographs of faces in which the pupil of the eye is clearly visible.	49 videos of the demonstration together with its altered versions
Steven Fernandes et al. [50]	Attribution based confidence network (ABC)	The ABC measurement approach is considered to be state of the art, as well as the value for realistic footage is 0.94.	A new method of identifying has been devised.	-	Deepfake TIMIT, a set of data that was built by the user from a commercial website, COHFACE, and movies from YouTube
PRNU[49]	PRNU	Take the average of the normalized cross correlation ratings for real footage and Deepfake films.	Method for efficient detection that may be used to enormous datasets	The dataset is insufficient for developing suggestions for ratios of likelihood	The video was recorded with a real camera, a Canon Pixma SX210 IS, however it has been manipulated.

4. Challenges

Although significant strides have been achieved in the efficiency of detecting DeepFake films, there are a number of problems with the approaches that are currently being used, which recommend that caution should be exercised.

- **Performance Analysis:** The challenge of detecting DeepFake films is often posed, resolved, and assessed as an issue of binary classification, currently. This means that every film is labeled as either legitimate or a DeepFake, depending on its authenticity. In controlled experiments, in which test DeepFake detection methods are developed utilizing videos which have been either unaltered or altered with DeepFake generation techniques, such a contradiction is straightforward to set up using movies which are alternatively authentic or fabricated using those methods. When the identification approach is put into usage in the actual world, nevertheless, the image becomes more complicated. For example, movies can be produced or modified in ways that go beyond DeepFakes; hence, the fact that a film cannot be identified as a

DeepFake does not automatically mean that it is a true one. Additionally, a DeepFake film may have been subjected to numerous kinds of alterations, and one label might not accurately convey this fact in its whole. In addition, when DeepFake is applied to a movie featuring the visages of numerous people, it only produces one or several of those faces for a portion of the intervals. Therefore, in order to adequately address the intricacies of real-world media counterfeits, the binary categorization method requires to be expanded to include multi-class, multi-label, as well as localized detection and classification.

- **Outcomes of Detection:** The majority of current techniques for detecting DeepFake are primarily intended to carry out batch assessment across an enormous number of movies. On the other hand, when the techniques of identification are utilized in situations such as by journalists or prosecutors, there is only a need to examine a restricted amount of movies. The numeric score that corresponds to the probability of a film being made utilizing a method for synthesizing is not nearly as valuable to those who use it if it is not validated with correct rationale of the result. In these kinds of circumstances, it is quite common practice to ask for justification of the numerical rating before considering whether or not the evaluation can be published or brought up in court. Yet, considering the "black box" aspect of the DNN designs, several data-driven Deepfake identification techniques, particularly those that relies on the utilization of DNN, typically lack comprehensibility
- **Generalization across Different Datasets**: A dearth of generalization had been reported for DeepFake films that were made using models that weren't included in the training dataset. This is because a DNN-based DeepFake detection approach requires to be trained on an individual training dataset. This does not constitute the exact same thing as excessive fitting because the learnt model may have performed satisfactorily in test films that were made with the exact same framework but weren't utilized in training. Whenever a trained identification approach is utilized to DeepFake movies that were made with different generating designs, a phenomenon known as "domain shifting" occurs, which is the underlying cause of the issue at hand. Expanding the set of training data to include more variants of generation concepts is a straightforward approach; however, a more adaptable strategy is required in order to scale to the extent of models that have not been considered before.
- **Fraud on social media platforms:** Social networking sites like Twitter, Instagram, and Facebook are now responsible for the distribution of a significant portion of the videos that can be seen on the internet. While being posted to social networks, these movies typically have their metadata removed, their file sizes reduced, and finally, they are subjected to high compression. This is done to both conserve network traffic and safeguard the confidentiality of the users. These actions, which are more commonly referred to as social media laundering, are harmful because they uncover traces of underneath deceit, and at the precise same time, they raise the likelihood of false positive identifications, which is the act of labeling a genuine film as a DeepFake. The vast majority of data-driven techniques for detecting DeepFake that rely on signal-level properties are heavily impacted by internet-based money laundering at this point. Enhancing assessment datasets by including effectiveness on social networking laundered videos, including real and synthetic, is an achievable measure that may be taken to enhance the resistance of DeepFake detection technologies to social media laundering. This can be done by deliberately incorporating simulations of these impacts into the data used for training, as well as by enhancing assessment datasets to include effectiveness on social media laundered movies.
- **Anti forensic:** With the growing efficacy of DeepFake identification techniques, the emergence of equivalent anti-forensic measures van also be forecasted. These countermeasures will take use of the flaws in the existing DeepFake detection methods in order to prevent revealing evidence of DeepFake films. Owing to the recognized fragility of standard DNN algorithms for classification, the data-driven DNN-based DeepFake identification techniques are especially vulnerable to anti-forensic assaults. This is the case because of the nature of the approaches. In point of fact, the past few years have seen an explosive growth of antiforensic techniques that rely on hostile assaults on DNN algorithms aimed at DeepFake detection [30, 51, 52, 53]. Anti-forensic methods may additionally be produced in the third component, which is to masquerade actual footage as a DeepFake video through the incorporation of generated signal level attributes required by existing detection techniques. This circumstance is what we refer to as fake DeepFake. Anti-forensic countermeasures are additionally possible in this aspect. In addition, DeepFake detection algorithms need to be improved so that

they can defend against attacks that are maliciously intended.

5. Conclusion and Future Scope

Deepfakes are videos that have been digitally altered to look extremely realistic, and they feature individuals performing or expressing things that they do not actually do or say. Simply relying on visual evidence to form an opinion on the reality of something is insufficient, and the tools that are now available to determine whether or not the recording has been tampered with are unreliable. Because the visual appeal of Deepfakes is currently so perfect, it will be difficult to make a decision on truthfulness based solely on visual confirmation. The solution that Digger has come up with for this problem is to make advantage of the most advanced technology available in order to design a toolset that is able to identify forged Deepfakes. As a result, the development of a system that is able to identify forged content within Deepfake films is of the utmost importance. Therefore, further research can offer an algorithm that will automatically identify the Deepfake films by employing an audio-visual technique that recognizes the discrepancy that occurs with lip motions and words in audio.

References

[1] Chesney R, Citron DK (2019) Deep Fakes: a looming challenge for privacy, democracy, and national security. In: 107 California Law Review (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper No. 2018-21

[2] Li Y, Chang M-C, Lyu S (2018) In Ictu Oculi: exposing AI generated fake face videos by detecting eye blinking. In: IEEE international workshop on information forensics and security (WIFS)

[3] Bitouk D, Kumar N, Dhillon S, Belhumeur P, Nayar SK (2008) Face swapping: automatically replacing faces in photographs. ACM Trans Graph (TOG)

[4] Dale K, Sunkavalli K, Johnson MK, Vlasic D, Matusik W, Pfister H (2011) Video face replacement. ACM Trans Graph (TOG)

[5] Suwajanakorn S, Seitz SM, Kemelmacher-Shlizerman I (2015) What makes tom hanks look like tom hanks. In: ICCV

[6] Suwajanakorn S, Seitz SM, Kemelmachershlizerman I (2017) Synthesizing obama: learning lip sync from audio. ACM Trans Graph 36(4):95

[7] Thies J, Zollhofer M, Stamminger M, Theobalt C, Niessner M (2016) Face2Face: real-time face capture and reenactment of rgb videos. In: IEEE conference on computer vision and pattern recognition (CVPR)

[8] Liu M-Y, Breuel T, Kautz J (2017) Unsupervised image-to-image translation networks. In: NeurIPS

[9] Kazemi V, Sullivan J (2014) One millisecond face alignment with an ensemble of regression trees. In: CVPR

[10] Afchar D, Nozick V, Yamagishi J, Echizen I (2018) Mesonet: a compact facial video forgery detection network. In: WIFS

[11] Güera D, Delp EJ (2018b) Deepfake video detection using recurrent neural networks. In: AVSS

[12] McCloskey S, Albright M (2018) Detecting gan-generated imagery using color cues. arXiv:1812.08247

[13] Li Y, Lyu S (2019) Exposing deepfake videos by detecting face warping artifacts. In: IEEE conference on computer vision and pattern recognition workshops (CVPRW)

[14] Li L, Bao J, Zhang T, Yang H, Chen D, Wen F, Guo B (2019a) Face x-ray for more general face forgery detection. arXiv:1912.13458

[15] Frank J, Eisenhofer T, Schönherr L, Fischer A, Kolossa D, Holz T (2020) Leveraging frequency analysis for deep fake image recognition. arXiv:2003.08685

[16] Durall R, Keuper M, Keuper J (2020) Watch your up-convolution: Cnn based generative deep neural networks are failing to reproduce spectral distributions. arXiv:2003.01826

[17] Guarnera L, Battiato S, Giudice O (2020) Deepfake detection by analyzing convolutional traces. In: Proceedings of the IEEE conference on computer vision and pattern recognition workshops

[18] Yang X, Li Y, Lyu S (2019) Exposing deep fakes using inconsistent head poses. In: ICASSP

[19] Matern F, Riess C, Stamminger M (2019) Exploiting visual artifacts to expose deepfakes and face manipulations. In: IEEE winter applications of computer vision workshops (WACVW)

[20] Ciftci UA, Demir I, Yin L (2020) How do the hearts of deep fakes beat? Deep fake source detection via interpreting residuals with biological signals. In: IEEE/IAPR international joint conference on biometrics (IJCB)

[21] Hu S, Li Y, Lyu S (2009) Exposing GAN-generated faces using inconsistent corneal specular highlights. arXiv:11924:2020

[22] Sabir E, Cheng J, Jaiswal A, AbdAlmageed W, Masi I, Natarajan P (2019) Recurrent convolutional strategies for face manipulation detection in videos. Interfaces (GUI) 3:1

[23] Rössler A, Cozzolino D, Verdoliva L, Riess C, Thies J, Nießner M (2019) FaceForensics++: learning to detect manipulated facial images. In: ICCV

[24] Nguyen HH, Yamagishi J, Echizen I (2019b) Capsule-forensics: using capsule networks to detect forged images and videos. In: ICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, pp 2307–2311

[25] Nataraj L, Mohammed TM, Manjunath BS, Chandrasekaran S, Flenner A, Bappy JH, RoyChowdhury AK (2019) Detecting gan generated fake images using co-occurrence matrices. Electron Imag (2019)5:532–1

[26] Do N-T, Na I-S, Kim S-H (2018) Forensics face detection from gans using convolutional neural network

[27] Tan M, Le Q (2019) EfficientNet: rethinking model scaling for convolutional neural networks. In: Chaudhuri K, Salakhutdinov R (eds) Proceedings of the 36th international conference on machine learning, vol 97 of Proceedings of machine learning research, Long Beach, California, USA, 09–15 Jun 2019. PMLR, pp 6105–6114

[28] Amerini I, Galteri L, Caldelli R, Del Bimbo A (2019) Deepfake video detection through optical flow based cnn. In: Proceedings of the IEEE international conference on computer vision workshops, pp 0-0

[29] Koopman M, Rodriguez AM, Geradts Z (2018) Detection of deepfake video manipulation. In: The 20th Irish machine vision and image processing conference (IMVIP), pp 133–136

[30] Huang Y, Juefeixu F, Wang R, Xie X, Ma L, Li J, Miao W, Liu Y, Pu G (2020) Fakelocator: robust localization of gan-based face manipulations via semantic segmentation networks with bells and whistles. Computer vision and pattern recognition. arXiv:2001.09598

[31] Korshunov P, Marcel S (2018) Deepfakes: a new threat to face recognition? Assessment and detection. arXiv:1812.08685

[32] Dolhansky B, Howes R, Pflaum B, Baram N, Ferrer CC (2019) The deepfake detection challenge (DFDC) preview dataset. arXiv:1910.08854

[33] Li Y, Sun P, Qi H, Lyu S (2020) Celeb-DF: a Large-scale challenging dataset for DeepFake forensics. In: IEEE conference on computer vision and patten recognition (CVPR), Seattle, WA, United States

[34] Jiang L, Wu W, Li R, Qian C, Loy CC (2020) Deeperforensics-1.0: a large-scale dataset for real-world face forgery detection. arXiv:2001.0302

[35] Stehouwer J, Dang H, Liu F, Liu X, Jain AK (2019) On the detection of digital face manipulation. Computer vision and pattern recognition. arXiv:1910.01717

[36] Raahat Devender Singh, Naveen Aggarwal," Video content authentication techniques: a comprehensive survey", Springer, Multimedia Systems, pp. 211-240, 2018.

[37] David G'uera Edward J. Delp," Deepfake Video Detection Using Recurrent Neural Networks", Video and Image Processing Laboratory (VIPER), Purdue University,2018.

[38] Ekraam Sabir, Jiaxin Cheng, Ayush Jaiswal, Wael AbdAlmageed, Iacopo Masi, Prem Natarajan," Recurrent Convolutional Strategies for Face Manipulation Detection in Videos", In proceeding of the IEEE Xplore Final Publication, pp. 80-87, 2018.

[39] Xinyi Ding, Zohreh Razieiy, Eric C, Larson, Eli V, Olinick, Paul Krueger, Michael Hahsler," Swapped Face Detection using Deep Learning and Subjective Assessment", Research Gate, pp. 1-9, 2019.

[40] Peng Zhou, Xintong Han, Vlad I. Morariu Larry S. Davis," Two-Stream Neural Networks for Tampered Face Detection", IEEE Conference on Computer Vision and Pattern Recognition, 2019

[41] Chih-Chung Hsu, Yi-Xiu Zhuang, and Chia-Yen Lee," Deep Fake Image Detection based on Pairwise Learning", MDPI, Applied Science,2020, doi:10.3390/app10010370.

[42] Fang Liu, Licheng Jiao, Fellow, IEEE, and Xu Tang, Member" Task-Oriented GAN for PolSAR Image Classification and Clustering", IEEE Transactions On Neural Networks and Learning Systems, Volume 30, Issue 9, 2019.

[43] Jawadul H. Bappy, Cody Simons, Lakshmanan Nataraj, B.S. Manjunath, and Amit K. Roy-Chowdhury," Hybrid LSTM and Encoder-Decoder Architecture for Detection of Image Forgeries", IEEE Transaction on Image Processing, Volume: 28 , Issue: 7 ,pp. 1-14, 2019.

[44] Pavel Korshunov, S´ebastien Marcel," Speaker Inconsistency Detection in Tampered Video", 26th European Signal Processing Conference (EUSIPCO), 2018, ISBN 978-90-827970-1-5.

[45] Xinsheng Xuan, Bo Peng, Wei Wang and Jing Dong," On the Generalization of GAN Image Forensics", Computer Vision and Pattern Recognition, Cornell University, Volume 1, pp. 1-8, 2019.

[46] Yuezun Li, Siwei Lyu," Exposing DeepFake Videos by Detecting Face Warping Artifacts", In Proceedings of the IEEE Xplore Final Publication, pp. 46- 52, 2019.

[47] Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen," Capsule-Forensics: Using Capsule Networks to detect Forged Images and Videos", ICASSP, pp. 2307 – 2311, 2019

[48] Li, Y., Chang, M. C., and Lyu, S, "Exposing AI created fake videos by detecting eye blinking", In

IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-7). 2018.

[49] A.M. Rodriguez, Z. Geradts," Detection of Deepfake Video Manipulation", In Proceedings of the 20th Irish Machine Vision and Image Processing conference, Belfast, Northern Ireland, pp. 133-136, 2018, ISBN 978-0-9934207-3-3.

[50] Steven Fernandes, Sunny Raj, Rickard Ewetz, Jodh Singh Pannu, Sumit Kumar Jha, Eddy Ortiz, Iustina Vintila, Margaret Salte," Detecting deepfake videos using attribution-based confidence metric", In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 308-309), 2020.

[51] Carlini N, Farid H (2020) Evading deepfake-image detectors with white- and black-box attacks. arXiv:2004.00622

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

[53] Neekhara P (2020) Adversarial deepfakes: evaluating vulnerability of deepfake detectors to adver-sarial examples. arXiv:2002.12749

[54] Ibrahim, S. S. ., & Ravi, G. . (2023). Deep learning based Brain Tumour Classification based on Recursive Sigmoid Neural Network based on Multi-Scale Neural Segmentation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 77–86. https://doi.org/10.17762/ijritcc.v11i2s.6031

[55] Mr. Kaustubh Patil, Promod Kakade. (2014). Self-Sustained Debacle Repression Using Zig-Bee Communication. International Journal of New Practices in Management and Engineering, 3(04), 05 - 10. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/32

[56] Anand, R., Khan, B., Nassa, V.K., Pandey, D., Dhabliya, D., Pandey, B.K., Dadheech, P. Hybrid convolutional neural network (CNN) for Kennedy Space Center hyperspectral image (2023) Aerospace Systems, 6 (1), pp. 71-78.