IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

FFDL: Feature Fusion-Based Deep Learning Method Utilizing Federated Learning for Forged Face Detection

Vinay Gautam[1], Gaganpreet Kaur[1] , Meena Malik[2] , Ankush Pawar[3], Akansha Singh[4,*], Krishna Kant Singh[5], S.S. Askar[6], Mohamed Abouhawwash[7]

[1]Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India,
vinay.gautam@chitkara.edu.in, drgaganpreestcse@gmail.com
2Department of CSE, Chandigarh University, Mohali. meenamlk@gmail.com.
3Computer Science & Engineering (AI&ML) Department, Vishwaniketan's Institute of Management Entrepreneurship & Engineering Technology, Khalapur, ankushpawar1981@gmail.com
[4]School of CSET, Bennett University, Greater Noida, India
[5]Delhi Technical Campus, Greater Noida, India
[6]Department of Statistics and Operations Research, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia
[7]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt

***Corresponding Author: akanshasing@gmail.com**

ABSTRACTThe widespread adoption of advanced technologies may be responsible for the extensive dissemination of forged photographs and videos on the Internet. This could potentially result in the proliferation of fraudulent identities online, raising safety concerns in society. The traditional method for detecting forgery, commonly referred to as the classical forgery method, lacks the capability to accurately identify such fraudulent activities. This limitation arises because these algorithms are trained on publicly available centralized datasets and do not prioritize privacy and security considerations. Consequently, they adversely affect the ability to detect counterfeit content. As a potential solution to this problem, we employed a highly effective deep learning methodology rooted in federated learning. We introduced a novel deep learning approach that combines features to assess the authenticity of photographs and videos shared on social media platforms. The proposed model was trained using three widely recognized forensic datasets: FaceForensics++, Deepforensic-1.0, and WildDeepfake. Visual features were extracted using two widely recognized deep learning approaches, namelyInception and Xception. These features were then combined into a feature vector using Canonical Correlation Analysis, and Convolutional Neural Networks were trained on these features to identify manipulated images and videos. The experiments were carried out with publicly available datasets and involved changing several parameters. Finally, the proposed model's performance was compared with other deep learning models within federated learning environments to identify forgeries. Our proposed approach demonstrated exceptional performance, achieving an accuracy rate of 98.99% when evaluated on the merged dataset.

INDEX TERMS Fake Detection, Deep Learning, Feature fusion, Federated Learning, Privacy-Preserving.

I. INTRODUCTION

Deep generative models have made great progress, and as a result, the technology for making synthetic faces is now quickly and readily available. Because of this, it has become more difficult to spot indicators of artifact fabrication, sometimes to the point where they are invisible to the unaided eye. Moreover, thieves can utilize counterfeit technologies to manipulate the look of well-known people in recordings, including politicians and public personalities. This can result in the public learning harmful information. They may also aim for facial recognition systems in transit hubs, which would enable them to adopt the identities of certain people and avoid being apprehended. There is no question that taking part in these dangerous activities will probably have unexpected repercussions for social security. Even though a large number of academics have focused on

the identification of face forgeries, the accuracy of forgery detection tasks can be negatively impacted by the existence of artifact videos that contain a lot of redundant data, complex backdrops, and different kinds of objects. Consequently, in real-world scenarios, the identification of forged faces continues to be a challenging and important problem.

Their cognitive process may be summed up as a binary categorization problem. Detection techniques are divided into many categories, including those that use faked photos and videos. As mentioned in [1-4], the main goal of forgery picture detection systems is to differentiate real from fake images using low-level information. Unlike forgery image detection, forgery video detection techniques mainly concentrate on determining the authenticity of films by examining the visually odd picture cross-frame transition and temporal irregularities observed in counterfeit videos. In order to identify deep fakes, for example, [5] used a technique to get the sequential inconsistencies of faces. In order to extract the progressive information from a video frame and assess its validity, [6] used a recurrent model in their investigation. Most detection techniques already in use rely on centralized training data to create model parameters, which raises the possibility of privacy violations. In recent years, there has been a growing emphasis on efficient training models with dispersed training data across several devices while maintaining the privacy of individuals. Additionally, different distributions of forgeries might result from different types of artifacts, which could have much more detrimental impacts.

Here, in the research, the real-world situation was replicated with two innovative tasks such as generation of hybrid dataset and fusion based forgery detection method.

Federated learning has been rapidly developing and widely applied in real-world contexts in recent times [7]. Individual clients only use their own private data to train their local models in the federated learning architecture. Clients then replicate their model on a worldwide server in order to receive additional training. Each data center will then receive the aggregated parameters so they can update the server model. Until the training loss reaches a point of convergence, the process is repeated. The notion of federated learning encourages us to create a suitable training strategy that protects local data privacy and obtains robust discriminative features with strong generalization ability for forgery detection.

This paper introduces a concise deep-learning model that can accurately identify altered faces by employing the principle of federated learning. We introduced a novel deep learning approach that combines features to assess the authenticity of photographs and videos shared on social media platforms. The proposed model was trained using three widely recognized forensic datasets: FaceForensics++, Deepforensic-1.0, and WildDeepfake. Visual features were extracted using two widely recognized deep learning approaches, namely Inception and Xception. These features were then combined into a feature vector using Canonical Correlation Analysis, and Convolutional Neural Networks were trained on these features to identify manipulated images and videos.

The remaining portion of the paper is divided into multiple sections. Section 2 delves deeper into various models for detecting facial forgery. Section 3 and Section 4 provide an overview of the data collection and outlines the methodology that will be employed. Section 5 presents the findings and discusses them in a debate. Finally, Section 6 presents conclusions and future work.

II. RELATED WORK

Here the paper is described in several sub-sections, respectively explores a distinct cutting-edge method to resolve forgery issues. Initially, the research starts with various image-based forgery detection techniques followed by video-based forgery detection techniques. Afterward, the role of federated learning was explored.

A. Image based forgery detection.

Contemporary, the growing complexity of these technologies has sparked the public's interest in the technology of manipulating facial features. This serves as the main objective of the study: enhancing techniques for identifying counterfeit faces. Currently, there are multiple techniques available for identifying counterfeit facial images. Face forging is a binary classification problem that involves using markings to train the classifier. This can be categorized into two classes such picture forgery detection and video face forgery detection. Detection of forged images using visual analysis.

In a previous study [1], a method was suggested that was utilized to extract RGB and frequency domain data from photos for the purpose of detecting manipulated faces. Researchers created an X-ray system in [3] to detect deep false images by combining and creating hint artifacts from both photos. In [8] uses a recognition network and a backdrop recognition network for the purpose of identifying deep fake images.

The presence of minor abnormalities in photos was identified using a network of interconnected streams, and this method was summarized in reference [9] for the purpose of detecting fraudulent photographs. Deep learning algorithms were utilized in [10] to detect deep fake photos. In this study, a convolutional neural network was employed to detect and extract artifacts from counterfeit photographs in order to determine their genuineness. A unique U-Net model was employed in [11] to identify counterfeit photographs following the extraction of image information. The study in [12] utilized a Machine learning-

based Differential MAD method to identify counterfeit photos by recognizing alterations made using morphing techniques.

In [13], a unique convolution process was proposed for the purpose of identifying counterfeit photos. The convolution technique was incorporated into MTD-Netto to improve the ability to distinguish between genuine and counterfeit photos. The authors of [14] suggested a modified Convolutional Neural Network (mCNN) that lacks sufficient annotated data to accurately identify counterfeit photos. In this context, the facial expressions were examined using the annotation suggested in the model. In a study by [15], a technique based on hierarchy was suggested to extract picture frequency and RGM attributes for the purpose of identifying deep fake images.

In [16], a method was introduced that utilizes a confined invariant for many objectives, including enhancing localization consistency, achieving localization invariance, and detecting fraudulent images. In a study referenced as [17], a technique utilizing an attention mechanism was explained. This technique took specific characteristics from the face to improve the precision of recognition method.

In [18], a DFT transformation was utilized to obtainattributes of images and subsequently be utilized for the detection of forged faces. In [19], a transformer was utilized to identify anomalies in the image's identification. The article described a novel approach, presented in [4], for detecting counterfeit movies by utilizing 3D head position features applied to support vector machines. Researchers employ a 3D decomposition methodology in [20] to obtain many graphic elements from images. The extracted elements were subsequently utilized to uncover signs of falsification within the images. The authors propose employing many visual sensors to identify misleading visual cues, as stated in reference [21]. A technique was employed in [22] to exploit the similarities between authentic and false pictures by acquiring shared compact representations through learning. The process of generalization was improved by utilizing identical representations. As a result, many strategies were put forth to deal with the problem of forged data utilizing photos, but some users also had problems with video forging. The following subsection provided specifics on several techniques for detecting faked videos.

B. Detection of video-based forgeries

The section covers detailed study of various methods to detect forged video. The techniques employ visual characteristics, inter-frame shift, and temporal randomness to recognize forgery in the video. Here are various techniques that videos might utilize to ascertain the genuineness of a face.

In [5], a paradigm for multi-instance learning was proposed, where video content is treated as instances and bags. The strategies employ facial images extracted from the movie as training examples in a bag and subsequently utilize them for predicting instances. In [6], a recurrent network was used to extract information from videos and then detect fraudulent data. In [23] biological signals were extracted from video using a novel classifier to identify manipulated frames.

A combination of transfer learning network was utilized in [24] to uncover counterfeit data. Abnormalities were detected by analyzing video frames using deep learning models. An integrated dual-network system was employed to provide accurate information and control the visibility of material [25]. Afterwards, the DL model was employed to extract information from videos.

A multidimensional DL model was employed in [26] to extract spatial-temporal data to recognize irregularities in forge video. Videofraudster detection is more resource-intensive than forgery detection in images. The sequential irregularity present in the motion picture is more complicated than the irregularity found in individual pictures. The face forgery detection approaches employed a centralized methodology and circumvented concerns around data privacy. Both datasets have been consolidated into a federal spot and utilized similar federal data to optimize the model. The investigation examines the devolved strategy and assesses the influence on forgery detection.

Several approaches were described here to address the issue with machine learning, the approaches' efficacy was questioned. Therefore, deep learning was used to examine the effect on the detection of fabricated images and videos.

C. Federated Learning

Federated learning, a technique that enables training machine learning models without sharing raw data, has gained significant attention due to its potential to safeguard data privacy. A basic federated learning system consists of two essential components: a data center and a global server. The data center utilized the application interface to update the server with exclusive data and later the parameters were aggregated at server level. Initially, the aggregation was achieved in [7] with a biased average of model parameters.

An algorithm was proposed in [32] to address the issue of data heterogeneity of data spread across the network. It effectively enhances the conjunctive performance of FL in real-life scenarios with heterogeneous networks. The confidentiality conserving the efficacy of FL has garnered increasing interest. In order to safeguard confidential personal data in activities involving the identification of individuals, a dispersed approach utilizing unlabeled data is implemented in [33-34] for the purpose of optimizing federated operations on cloud and edge platforms. Shao et al.

[35] investigated the detection of shared face representation by implementing a federated domain decoupling technique. [36] developed a method to implement FL in edge computing. Through the implementation of a versatile participation training method, it successfully minimized operating costs and safeguarded privacy, hence enhancing the effectiveness of edge computing.

[37] proposed a framework that utilizes homomorphic encoding as base technology and utilized the same to accurately access the contaminating actions through complete process of FL. In this research, the issue was resolved with private distributed data [38] and introduced a regularization method based on SoftMax. The objective is to improve the discriminative ability of class embeddings across different clients.

Zhuang et al. [39] conducted research on a cluster-based domain-adaptive federated learning technique aimed at enhancing the recognition accuracy of the target domain. Their study specifically focused on the challenge of face recognition while considering privacy limitations. Nevertheless, just a few studies have utilized federated learning for face forgery detection tasks. The quantity of training data has experienced a rapid increase, hence amplifying the need of safeguarding data privacy.

In addition, the implementation of a distributed data collaborative training technique can effectively enhance the model's performance by mitigating the risk of overfitting. Given these concerns, the research suggests a new approach called generalized residual federated learning for detecting face forgeries. This method aims to address the challenges faced.

However, significant efforts have been made to detect face forgery using centralized data, and in specific situations, federated learning has been employed to tackle privacy concerns. In the research, the task of face forgery detection is accomplished in federated environment and evaluates the impact of FL on forgery detection. Hence, the investigation utilizes a transfer learning model to accurately identify forgery in static images and videos in federated learning environment.

The primary significance of this study is:

1. Investigation is accomplished with FL for the purpose of detecting facial manipulation in both photos and videos.

2. The research retrieved quality features from a hybrid dataset consisting of three well-known datasets: FaceForensics++, Deepforensic-1.0, and WildDeepfake.

3. Investigate the influence of different client variations, communication rounds, and other optimal aspects on the detection of face forgery.

4. Investigate different transfer learning networks for the purpose of detecting deep fake images.

III. FEATURE FUSION DEEP LEARNING FACE FORGERY DETECTION

The methods for detecting deep face forgeries begin by preprocessing face photos using Dlib[38]. This tool is employed to minimize the dispersion of intricate backgrounds in photographs and adjust their dimensions to 256*256 pixels. The data is extracted sequentially from the video collection. In this case, the Python library is utilized to build a feature fusion network to detect forged images.
Feature extraction was accomplished with two well-known deep learning architecture Xception and Inception. The deep learning models used distinct convolution filters to extract image or video features. The details of the models were illustrated below:

A. Preprocessing and Augmentation

As seen in Figure 2, we apply four tiers of image preparation procedures to our datasets in order to improve the effectiveness of our model in our FL system of forgery detection. These techniques fall into the following categories: high pass filtering and Gaussian noise.

1) **Data Augmentation:** First, we use data augmentation methods, such as horizontal flipping and small width and height adjustments, but not vertical flips. These additions improve the model's capacity to identify patterns in the input data independent of their alignment or orientation by simulating changes in the subjects' placement and orientation inside the pictures.

2) **Gaussian filter:** Often called Gaussian blur, a Gaussian filter is a smoothing filter that is essential to image processing in order to soften images and reduce unwanted noise and tiny details [34]. To decide how each pixel in the image should be altered, this filter uses a Gaussian function, which is closely related to the normal distribution in statistics. We apply the Gaussian blur approach to the edge map in order to add noise and fine-scale variations. A Gaussian kernel of size (5,5) is used for this smoothing operation, which aims to remove high-frequency elements that could obstruct further processing stages.

3) **High-Pass Filtering:** A high-pass filter reduces or suppresses sounds below a predetermined cutoff frequency while permitting high frequencies to pass through [36]. Sharpening, which is just a frequency-domain high-pass operation in the context of image processing, is applied to our dataset. In this case, sharper images result from increasing the contrast between nearby regions with minimal brightness variation.

B. Feature Extraction

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3523257

In research, the image features were extracted with two feature extraction models: Xception and Inception. Both models were elaborated below in sub-sections.

a. Xception Feature Extractor

The Xception neural network utilizes depth-wise separable convolution to perform the convolution function followed by a pointwise convolution. Depth-wise convolution refers to a type of convolution operation where the convolution is performed independently on each input channel, using a spatial filter of size n×n. Figure 1 illustrates the convolution operation with 5 n×n spatial convolutions. The pointwise convolution refers to a 1×1 convolution operation that is used to alter the dimensionality of the data. Unlike conventional convolution, we can avoid the necessity to conduct convolution across all channels. This implies that there are a reduced number of links, and the model has a lower weight. The final output after convolution operation is depicted in Figure 2.

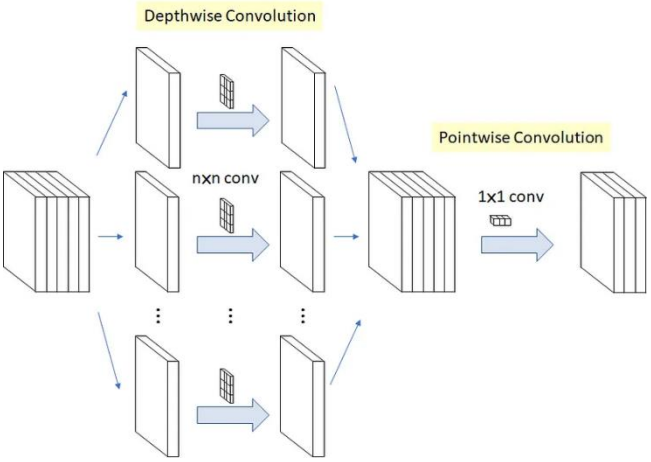

Figure 1. XceptionCconvolution Operation [14]

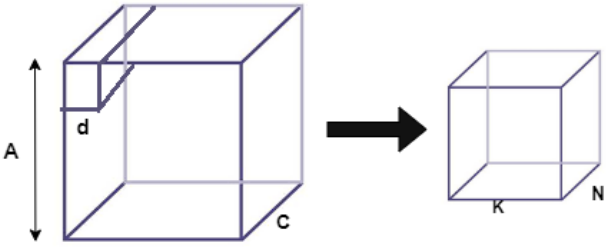

Figure 2. Convolution Operation [14]

The input color image is composed of three channel RGB denoted as C. It possesses a specific dimension, denoted as A, which is 100 * 100 and applies a convolution filter of dimensions d*d, specifically 3*3.

The formula for calculating the value of one kernel is presented in Eq. (i):

$$K^2 \times d^2 \times C \qquad \text{Equation (i)}$$

The outcome after convolution is depicted as K and based on padding values. Thus, for N Kernels (the number of layers in the convolution) presented in Eq. (ii) :

$$K^2 \times d^2 \times C * N \qquad \text{Equation (ii)}$$

A technique to reduce the costs of these processes was introduced: depth-wise separable convolutions. They are divided into two main stages by nature: Depth-wise convolution is a type of convolution where each channel of an input is processed independently.

Convolution that is carried out point by point. The Depth-wise Convolution refers to a specific type of convolutional operation in deep learning models. Depth-wise Convolution is an initial stage where we replace the convolution of size d×d×C with a convolution of size d×d×1. Put simply, we do the convolution computation on each channel individually, rather than on all channels simultaneously.

This results in an initial volume with dimensions of K×K×C, rather than K×K×N as previously. Currently, we have only performed the convolution process for a single kernel/filter, not for many kernels. This brings us to the second phase.

The pointwise convolution performs a conventional convolution operation, using a size of 1×1×N over the K×K×C volume. This enables thecreation of a volume of dimensions K×K×N, as mentioned before.

b. Inception Feature Extractor

Filters of different sizes can be used with the Inception network architecture without requiring the network's depth to be increased. Instead of applying the several filters one after the other, they are applied in parallel. The Inception pre-trained network's layered structure is seen in Figure 3. Figure 4 elaborates on the Inception network's convolution procedure.

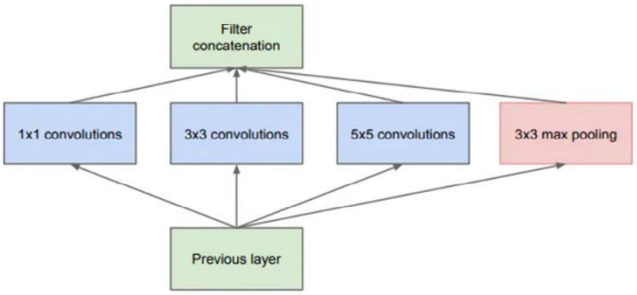

Figure 3. Inception Network

This is referred to as the rudimentary iteration of the inception model. The issue with this model stemmed from the excessive quantity of parameters. In order to alleviate this issue, they devised the following architecture.

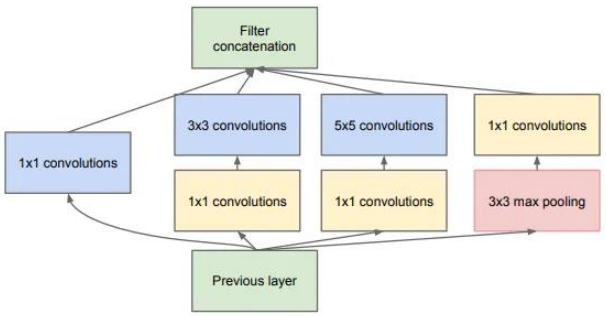

Figure 4. Convolution Filter

The Inception module with dimension reduction operates in a comparable fashion to the naïve module, except for one distinction. In this process, features are obtained by applying 1 * 1 convolutions at the pixel level, followed by 3 * 3 convolutions and 5 * 5 convolutions. The dimension of the image remains unchanged when the 1 * 1 convolution process is applied. Nevertheless, the achieved outcome provides superior precision.

C. Feature Fusion

In the proposed study, extracted features were combined into a fusion matrix using a canonical correlation analysis (CCA). Canonical association analysis (CCA) was applied in this instance to generate fused features by considering the associations between the retrieved parameters. The correlation value between various features is computed by the CCA algorithm. The most significant features are chosen and included in the fusion matrix based on this correlation value. From eq. (iii) to (v), the CCA [39] feature fusion procedure is illustrated.

$$u = A_{x_1}x_1 + A_{x_2}x_2 \ldots + A_{x_n}x_n = A_x^T X \quad \text{(iii)}$$

$$v = B_{y_1}y_1 + By_2y_2 \ldots + B_{y_k}y_k = B_y^T Y \quad \text{(iv)}$$

u and v represent the measurement of linear relationships of features represented with $(x_1 .. x_n and\ y_1 \ldots y_2)$

$CCA\ finds\ weight\ vectors\ that\ expressed\ with\ Ax\ and\ By$:

$$Ax = [A1, \ldots, Aq] \in R\ d \times P\ and\ By = [B1, \ldots, Bq] \in R\ d \times Q \quad \text{(v)}$$

that maximize the correlation ρ between the variate u and v by solving following optimization problem as presented in (vi):

$$\max_{A_x \to A_y} \rho(u, v) = \frac{E(u,v)}{E[u^2]E[v^2]} \to \frac{A_x^T \Sigma_{xy} B_y}{\sqrt{(A_x^T \Sigma_{xx} A_x)(B_y^T \Sigma_{yy} B_y)}} \text{(vi)}$$

$where\ \Sigma xx\ and\ \Sigma yy\ are\ autocovariance\ matrices.$Σxy and E[.]are cross covariance matrix of X and Y and mean respectively (Note The overall covariance matrix C that includes Σxx, Σxy, Σyx and Σyy, cover all feature information on their associations. Optimization problem is solved by using Lagrange multipliers subjecting to eq (vii)

$$\Sigma xxA = BT\ \Sigma yyB = \Sigma xx = \Sigma T\ yy) \quad \text{(vii)}$$

D. Classification

The fusion matrix features were employed to classify images and identify forgery in the images that were flattened and linked to fully connected layers (FC). The layers in question operate as conventional neural network layers and are responsible for categorizing the extracted features. The fully connected layers acquire intricate connections between features and generate class probabilities or predictions. The classification function softmax can be describes with equation (viii):

$$S_{m_i} = \frac{e^{m_i}}{\sum_j e^{m_j}} A = \pi r^2 \quad \text{(viii)}$$

$S_{m_i}\ represnts\ the\ softmax\ function\ to\ classify\ features$

IV. FEDERATED ARCHITECTURE

Numerous convolution layers were employed to extract image features and employed to train the network. The model performance is evaluated on several factors such as communication values, learning rate (LR) and epoch values. The investigation involves testing different LR, such as 0.1 and 0.01, on each client within the FL environment.

The investigation involves establishing a FL with different numbers of clients and interaction iterations. The outcome is documented with a total of 10 clients, and the outcome is presented below. Figure 5 illustrates the whole architecture of the federated learning system designed for detecting deep face forgeries.

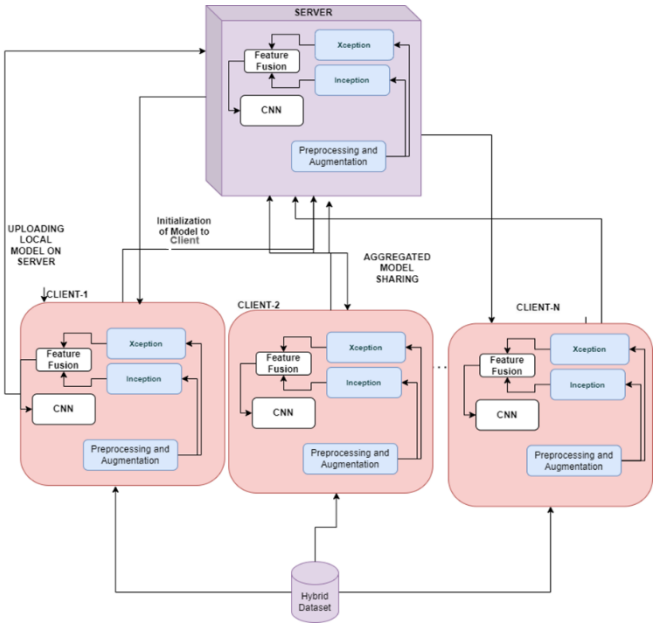

Figure 5. Face Forgery Detection with FL

It is a complex procedure that necessitates multiple rounds of communication. Each operation within the federated environment is spontaneously administered.

a) Client Process

b) Server Process

a) Client Process

This describes how the various clients behave in the environment and how they use their local data to update the initial and later global models. Several parameters are fixed

at the beginning of this process, including the number of clients overall, the number of communication rounds, the number of epochs, the local learning rate (LR), and the size of local batches (Bc). Therefore, during our experiments, we change these various factors to see how each affects the performance of the various models. In order to accomplish this, we simulate a group of clients who work together and share a dataset (which consists of both healthy and infected leaves) for model testing and training. Equal and random distribution of the dataset is used for data splitting among the various clients.
Put differently, D = k=1 Pk, where Pk(k = 1, 2,..., n) is the partition of each client, P1 = P2 =... = Pn, and D is the dataset size.

b) Server Process

This is the central server where the federated learning process occurs. This procedure is basically in charge of gathering the many local models and combining them to create a global aggregated model, which will be distributed to the clients at the conclusion of the communication cycle. An aggregation algorithm is used in order to accomplish the aggregation. This method acts as the rationale for combining the updates from the local models used in the training cycle at the server level. The most popular aggregation method is federated averaging. A partial list of some of the more popular aggregation algorithms is shown below: Within the methodology, the client and server procedures execute iteratively until a flawless and enhanced global model is achieved.

- FedAvg, or Federated Averaging: One of the most widely used federated learning algorithms that aggregates local models by calculating a weighted average of each model's weights to produce a global model. With this method, the raw data is not provided; only the model parameters are shared

- FedProx is an enhanced FedAvg that tackles data heterogeneity and non-IID (non-identical and independently distributed) issues. This method employs disparate or imbalanced data distribution.

- Federated Stochastic Gradient Descent (Federated SGD): A variation of stochastic gradient descent is called Federated Stochastic Gradient Descent (Federated SGD). Based on the corresponding performance, the federated SGD assigns distinct weights to each local model. A weighted average is then used for aggregation. Federated SGD, in contrast to FedAvg, does not require devices to share their model updates after completing several local training epochs.

- Secure Multi-Party Computation Averaging (SMC-Avg): SMC is the foundation of this aggregation approach. The purpose of SMC is to maintain the confidentiality of the inputs while enabling multiple parties to compute a function on them. SMC-Avg is used to safely aggregate model updates in federated learning without disclosing specific device updates.

All federated learning topologies depend on these various techniques, which are designed to increase the privacy of local model updates. Hence, here Federated averaging (FedAvg) algorithm was employed in this instance.

V. EXPERIMENT SETUP AND DISCUSSION

A. Datasets

The study employed a composite dataset of three distinct datasets to detect forge data. The datasets comprise the FaceForensics++ dataset. The abbreviation FF++ refers to the WildDeepfake dataset and the Deepforensic-1.0 dataset. Figure 1 illustrates the samples images from composite dataset. The datasets employed to accomplish the task is explained here:
The FaceForensics++ benchmark dataset is the main one [35]. One thousand videos from YouTube make up the compilation. 707 deepfake films yielded 7314 facial pictures for the WildDeepfake dataset [36]. The dataset's accompanying video was downloaded from the internet. A further dataset, Deeperforensics-1.0, was acquired from a highly reputable public repository. The collection is made up of one thousand movies along with the corresponding face photos, all from the same source. The three datasets were combined to form a hybrid dataset. Figure 6 shows a selection of the information.

Figure 6. Sample Images[35-36].

B. RESULT AND DISCUSSION

The result and discussion section offers a thorough examination of the experimental results, encompassing the choice of parameters from multiple datasets. The performance of the proposed model was assessed using different hyper-parameters, as outlined below:

a) Variable Number of Client
b) Variable Number of Communication Rounds
c) Impact of local iterations

a) Variable Client Impact

The federated environment is created by integrating different quantities of clients. The value of the clients directly affects

the global model, which will be updated by employing local models trained with local datasets. The research entailed doing experiments with different quantities of clients, notably 3, 5, 7, and 9. The research results were displayed at this site, in conjunction with client values 3 and 5. However, the investigations were carried out using pre-established parameters for communication rounds and epochs. The results were presented in Table 1 and Figure 7.

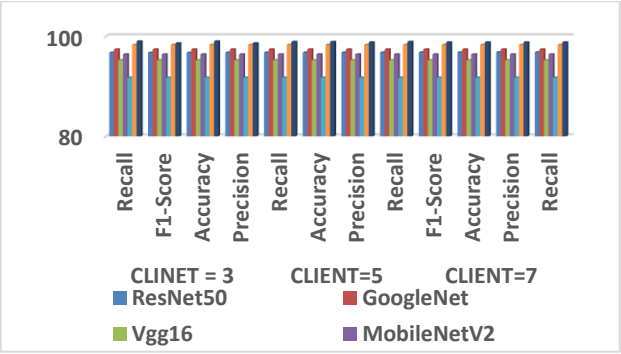

Figure 7. Evaluation of State-of-the-art Model

Table 1 and Figure 7 demonstrate that the FFDL attained a superior level of performance, as indicated by an accuracy rating of 98.9%. During the test, it was demonstrated that this phenomenon was consistent across multiple client configurations and various hyperparameter values. The accuracy and precision levels consistently neared 99.5. Although the other pre-trained models mentioned in Table 1 demonstrated acceptable performance, their results were marginally inferior to those of FFDL. The effectiveness of the Inception network varied significantly across different client setups, indicating a relatively low level of efficacy. Table 4 and Figure 7 provide evidence that the FFDL model outperformed other models in all evaluation parameters. Although architecture is a challenging field, the FFDL has shown exceptional outcomes. The results indicate that using FFDL leads to decreased training costs and amplifies the benefits of the network.

Table 1. DEPICTS THE PERFORMANCE ANALYSIS WITH VARYING NUMBERS OF CLIENTS.

	CLIENT = 3				CLIENT=5				CLIENT=7			
	Recall	F1-Score	Accuracy	Precision	Recall	Accuracy	Precision	Recall	F1-Score	Accuracy	Precision	Recall
ResNet50	96.72	96.73	96.74	96.75	96.76	96.77	96.78	96.79	96.80	96.81	96.82	96.83
GoogleNet	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38
Vgg16	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23
MobileNetV2	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39
InceptionV3	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75
Xception	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29
FFDL	**98.99**	**98.59**	**98.99**	**98.59**	**98.89**	**98.89**	**98.8**	**98.89**	**98.79**	**98.79**	**98.79**	**98.79**

Figure 8 and Figure 9 depict the experimental setup involving three distinct client environments. The experiment tested state-of-the-art approaches using different communication rounds and assessed their performance based on multiple criteria, including accuracy, precision, recall, and F1-score.

Figure 8 depicts the assessment of models with 3 clients and 30 rounds of discussion. From Figure 8, it is evident that all assessment metrics, such as accuracy, precision, recall, and F1-score, increase when the values of communication rounds increase. It can be inferred that the FFDL yields superior results and decreases both training time and energy consumption. While the MobileNetV2 network was intended to reduce energy usage and computational costs for training, its performance falls short of expectations when compared to comparable networks.

The findings indicate that MobileNetV2 exhibits marginally inferior performance compared to ResNet50 across various client setups. However, it is evident that opting for a network with lighter configurations is a more advantageous decision. Based on the findings, it is evident that networks such as FFDL are preferable over other networks.

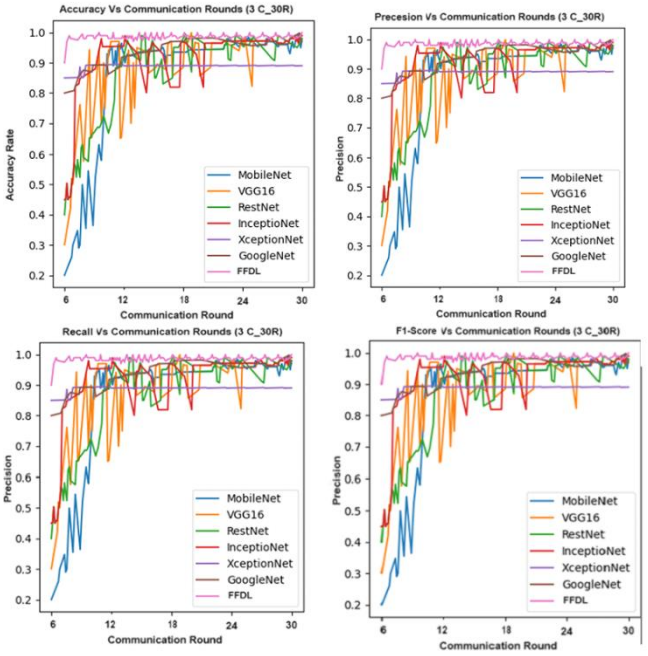

Figure 8. Comparison of State-of-the -art model with FFDL using 3-Client-30 Round Communication

Figure 9 depicts the assessment of models with 3 clients and 50 rounds of discussion. From Figure 9, it is evident that all assessment metrics, such as accuracy, precision, recall, and F1-score, increase when the values of communication rounds increase. It can be inferred that the FFDL yields superior results and decreases both training time and energy consumption. While the MobileNetV2 network was intended to reduce energy usage and computational costs for training, its performance falls short of expectations when compared to comparable networks. The findings indicate that MobileNetV2 exhibits marginally inferior performance compared to ResNet50 across various client setups. However, it is evident that opting for a network with lighter configurations is a more advantageous decision. Based on the findings, it is evident that networks such as FFDL are preferable over other networks.

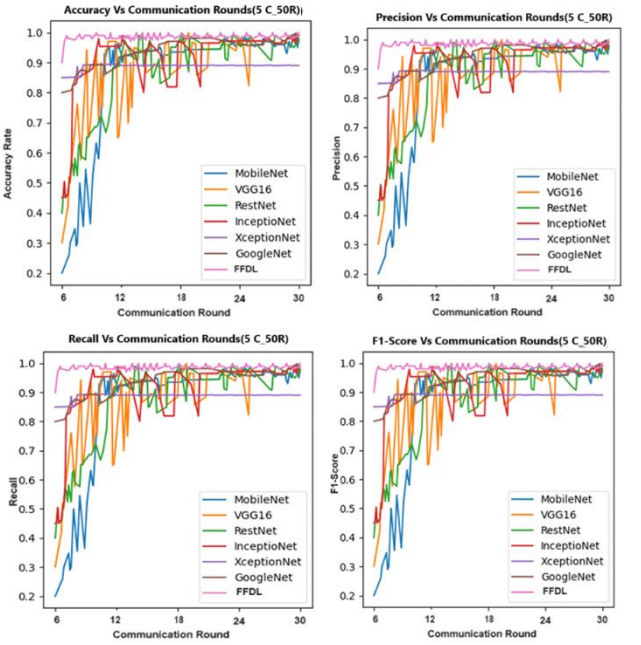

Figure 9. Outcome with 3 clients and 50 Communication Channels

Figure 10 and Figure 11 depict the experimental setup involving three distinct client environments. The experiment tested state-of-the-art approaches using different communication rounds and assessed their performance based on multiple criteria, including accuracy, precision, recall, and F1-score.

Figure 10 depicts the assessment of models with 5 clients and 30 rounds of discussion. From Figure 10, it is evident that all assessment metrics, such as accuracy, precision, recall, and F1-score, increase when the values of communication rounds increase. It can be inferred that the FFDL yields superior results and decreases both training time and energy consumption. While the MobileNetV2 network was intended to reduce energy usage and computational costs for training, its performance falls short of expectations when compared to comparable networks. The findings indicate that MobileNetV2 exhibits marginally inferior performance compared to ResNet50 across various client setups. However, it is evident that opting for a network with lighter configurations is a more advantageous decision. Based on the findings, it is evident that networks such as FFDL are preferable over other networks. Model achieves superior performance with a 98.9% accuracy rate.

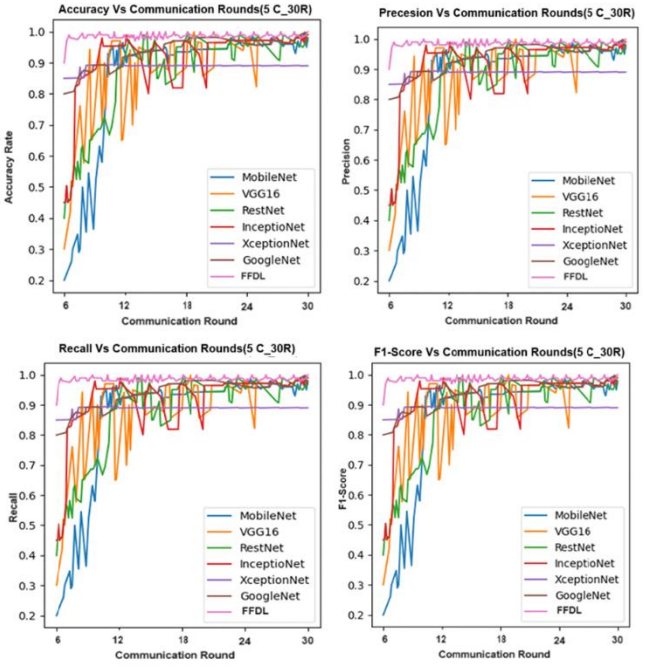

Figure 10. Outcome with 5 clients

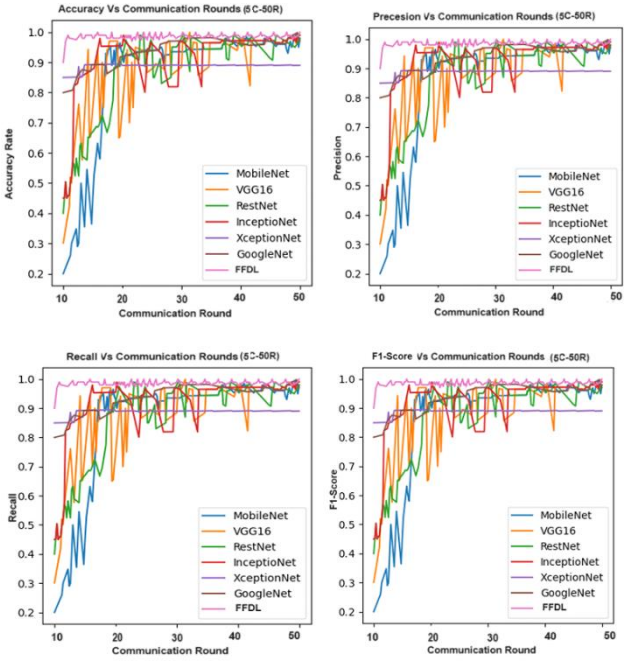

Figure 11. Outcome with 5 clients

Figure 11 depicts the assessment of models with 5 clients and 50 rounds of discussion. From Figure 11, it is evident that all assessment metrics, such as accuracy, precision, recall, and F1-score, increase when the values of communication rounds increase. It can be inferred that the FFDL yields superior results and decreases both training time and energy consumption. While the MobileNetV2 network was intended to reduce energy usage and computational costs for training, its performance falls short of expectations when compared to comparable networks. The findings indicate that MobileNetV2 exhibits marginally inferior performance compared to ResNet50 across various client setups. However, it is evident that opting for a network with lighter configurations is a more advantageous decision. Based on the findings, it is evident that networks such as FFDL are preferable over other networks. Model achieves superior performance with a 98.9% accuracy rate.

b) COMMUNICATION ROUNDS IMPACT ON PERFORMANCE

The objective of this study was to examine the influence of iteration or communication rounds on performance. The rounded values were distributed among clients and servers. The experiment included the consideration of other round types, such as 10, 30, and 50. For client configuration, we explored implementing both the 3-client and 5-client configurations. Under this arrangement, the models demonstrate enhanced performance. Table 2 and Figure 12 display the outcome of the conducted experiment.

The findings illustrated in Table 2 and Figure 12 demonstrate a direct correlation between the communication round and the performance of the majority of models. Table 5 clearly demonstrates that FFDL achieves superior performance compared to other methods after each communication round. FFDL models outperform other models in all communication rounds. Following each iteration, it is evident that the model's performance metrics, including F1 Score, Accuracy, accuracy, and recall, consistently reach a value of 98.9% for the FFDL model, while other models exhibit somewhat lower performance. The performance of the FFDL model surpasses those of other models, with FFDL demonstrating marginally superior performance.

The findings illustrated in Table 2 and Figure 12 demonstrate a direct correlation between the communication round and the performance of the majority of models. Table 5 clearly demonstrates that FFDL achieves superior performance compared to other methods after each communication round. FFDL models outperform other models in all communication

rounds. Following each iteration, it is evident that the model's performance metrics, including F1 Score, Accuracy, accuracy, and recall, consistently reach a value of 98.9% for the FFDL model, while other models exhibit somewhat lower performance. The performance of the FFDL model surpasses those of other models, with FFDL demonstrating marginally superior performance.

Table 2. COMMUNICATION ROUND IMPACT ON PERFORMANCE

	CR-30				CR-50			
	Recall	F1-Score	Accuracy	Precision	Recall	Accuracy	Precision	F1-Score
ResNet50	96.72	96.73	96.74	96.75	96.76	96.77	96.78	96.79
GoogleNet	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38
Vgg16	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23
MobileNetV2	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39
InceptionV3	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75
Xception	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29
FFDL	**98.99**	**98.59**	**98.99**	**98.59**	**98.89**	**98.89**	**98.8**	**98.89**

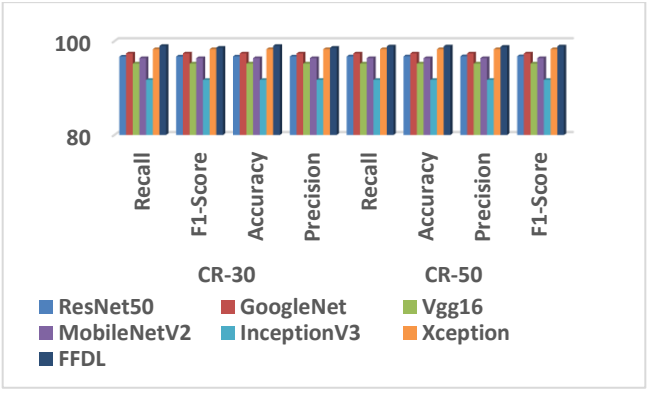

Figure 12. Comparison with different CR

c) IMPACT OF THE LOCAL ITERATIONS

This section of the paper discusses the analysis of the experiment conducted with different iterations or epochs on the client machine. Table 3 displayed two epoch values, and in both configurations, the FFDL models had the highest performance. Table 3 reveals that the performance of the other model is marginally worse than that of the FFDL models. The performance analysis is presented in Table 3 and Figure 13.

Table 3. MODEL PERFORMANCE VERSUS NUMBER OF EPOCHS.

	Epochs=100				Epochs-200			
	Recall	F1-Score	Accuracy	Precision	Recall	Accuracy	Precision	F1-Score
ResNet 50	96.72	96.73	96.74	96.75	96.76	96.77	96.78	96.79
Google Net	97.38	97.38	97.38	97.38	97.38	97.38	97.38	97.38
Vgg16	95.23	95.23	95.23	95.23	95.23	95.23	95.23	95.23
Mobile NetV2	96.39	96.39	96.39	96.39	96.39	96.39	96.39	96.39
InceptionV3	91.75	91.75	91.75	91.75	91.75	91.75	91.75	91.75
Xception	98.29	98.29	98.29	98.29	98.29	98.29	98.29	98.29
FFDL	**98.99**	**98.59**	**98.99**	**98.59**	**98.89**	**98.89**	**98.8**	**98.89**

The decentralized approach using Federated Learning (FL) demonstrates superior performance and yields improved results while ensuring data privacy and confidentiality.

In summary, the experiment's results indicate that tweaking the hyperparameters of the chosen deep architecture can enhance the performance of the deep learning architecture in the Federated learning technique. Dataset quality is another factor that significantly influences the outcomes of architecture. Quality data refers to the presence of a sufficient quantity of data that is used to train the model. The disparity in the size of client data and the number of classes can lead to variation in the outcome of the aggregated model. Consequently, it was necessary to fine-tune the hyperparameters before conducting the tests.

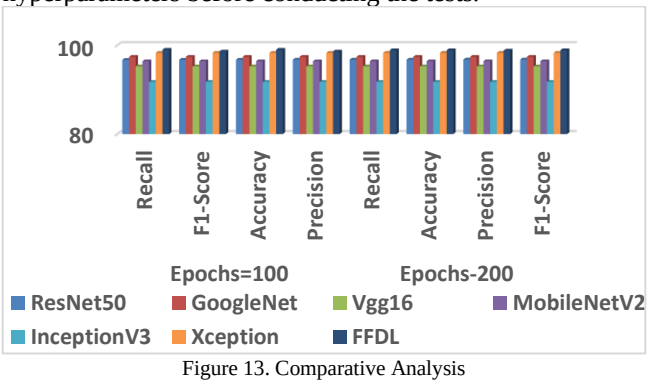

Figure 13. Comparative Analysis

Figure 14, Figure 15, and Table 4 depict the performance comparison of the proposed model with various state-of-the-art pretrained CNN models. Evidence indicates that the proposed model surpasses previous cutting-edge models.

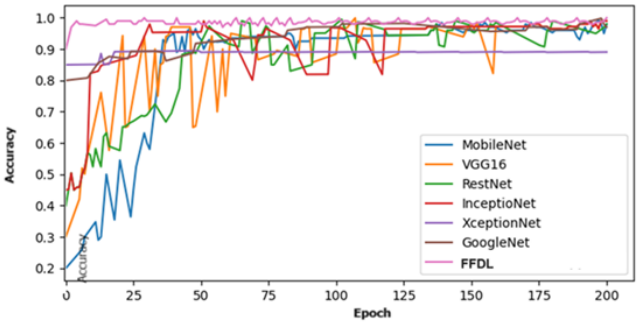

Figure 14. Accuracy Comparition of distinct Deep Learning Model with FFA

TABLE 4. COMPARATIVE STUDY OF DEEP LEARNING MODELS

DL model	Training accuracy	Validation accuracy	Testing accuracy	Precision (Average)	Recall (Average)	F1 score (Average)
VGG16	0.9721	0.8556	0.83	0.8546	0.8456	0.8546
ResNet-50	0.98212	0.8755	0.86	0.8655	0.8555	0.8655
Inception-V3	0.99	0.8956	0.88	0.8856	0.8756	0.8856
Xception	0.99	0.9201	0.9125	0.9101	0.9001	0.9101
MobileNetV2	0.99	0.8955	0.88562	0.8855	0.8755	0.8855
FFDL	**0.99**	**1**	**0.98995**	**0.9863**	**0.98083**	**0.98963**

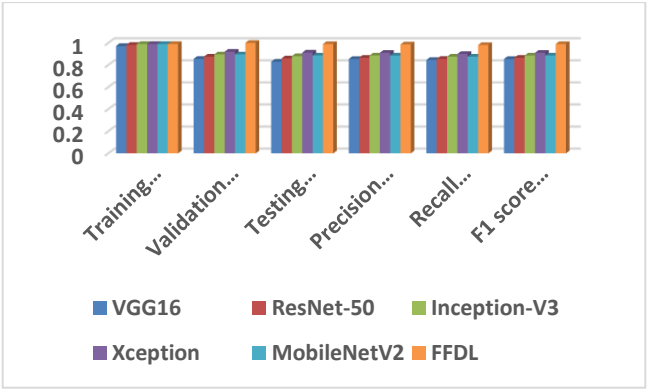

Figure 15. Model Evaluation Based on Various Parameters.

VI. CONCLUSION

The study investigated the effectiveness of different deep learning models in detecting facial forgery inside federated learning environments. The study employed a range of face forgery datasets, such as FaceForensic++, WildDeepfake, and Deepforensic datasets. In this scenario, the deep learning model was trained using all available datasets, and the performance of the models was evaluated by assessing accuracy and precision. After careful analysis, it was shown that the Feature Fusion Method demonstrated exceptional performance in a federated setting while utilizing the merged face forgery dataset. The objective of the study was to improve the identification of manipulated facial images while maintaining the confidentiality of the data. The results indicate that the model not only exceeds but also much improves the ability to protect data privacy.

The research centers on the escalating problem of forged pictures, but its reliance on publicly available data may limit its applicability in real-life situations. The proposed methodology, which employs federated learning in the field of deep learning, is novel. Nevertheless, it neglects to acknowledge the possible privacy issues that could emerge from utilizing decentralized methods.

Acknowledgments: Researchers Supporting Project number (RSP2025R167), King Saud University, Riyadh, Saudi Arabia.

Funding: This project is funded by King Saud University, Riyadh, Saudi Arabia. Researchers Supporting Project number (RSP2025R167), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] S. Chen, T. Yao, Y. Chen, S. Ding, J. Li, and R. Ji, "Local relation learning for face forgery detection," in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 35, no. 2, 2021, pp. 1081–1088.

[2] Shukla, P.K., Sandhu, J.K., Ahirwar, A., Ghai, D., Maheshwary, P. and Shukla, P.K., 2021. Multiobjective genetic algorithm and convolutional neural network based COVID-19 identification in chest X-ray images. Mathematical Problems in Engineering, 2021, pp.1-9.

[3] Sharif MI, Mehmood M, Sharif MI, Uddin MP. Human gait recognition using deep learning: A comprehensive review. arXiv preprint arXiv:2309.10144. 2023 Sep 18.

[4] Khalil M, Sharif MI, Naeem A, Chaudhry MU, Rauf HT, Ragab AE. Deep Learning-Enhanced Brain Tumor Prediction via Entropy-Coded BPSO in CIELAB Color Space. Computers, Materials & Continua. 2023 Dec 1;77(2).

[5] Trivedi, N.K., Tiwari, R.G., Anand, A., Gautam, V., Witarsyah, D. and Misra, A., 2022, November. Application of Machine Learning for Diagnosis of Liver Cancer. In 2022 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS) (pp. 1-5). IEEE.

[6] Balyan, A.K., Ahuja, S., Lilhore, U.K., Sharma, S.K., Manoharan, P., Algarni, A.D., Elmannai, H. and Raahemifar, K., 2022. A hybrid intrusion detection model using ega-pso and improved random forest method. Sensors, 22(16), p.5986.

[7] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Artificial intelligence and statistics. PMLR, 2017, pp. 1273– 1282.

[8] Y. Nirkin, L. Wolf, Y. Keller, and T. Hassner, "Deepfake detection based on discrepancies between faces and their context," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021.

[9] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Two-stream neural networks for tampered face detection," in 2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW). IEEE, 2017, pp. 1831–1839.

[10] Y. Li and S. Lyu, "Exposing deepfake videos by detecting face warping artifacts," arXiv preprint arXiv:1811.00656, 2018.

[11] P. Yu, J. Fei, Z. Xia, Z. Zhou, and J. Weng, "Improving generalization by commonality learning in face forgery detection," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 547–558, 2022.

[12] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch, "Deep face representations for differential morphing attack detection," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3625–3639, 2020.

[13] J. Yang, A. Li, S. Xiao, W. Lu, and X. Gao, "Mtd-net: Learning to detect deepfakes images by multi-scale texture difference," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4234–4245, 2021.

[14] Z. Jian, J. Li, Z. Fang, S. Yan, and J. Feng, "Marginalized cnn: Learning deep invariant representations," in 28th British Machine Vision Conference, 2017, 2017.

[15] C. Miao, Z. Tan, Q. Chu, N. Yu, and G. Guo, "Hierarchical frequencyassisted interactive networks for face manipulation detection," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 3008– 3021, 2022.

[16] J. Wang, Y. Sun, and J. Tang, "Lisiam: Localization invariance siamese network for deepfake detection," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2425–2436, 2022.

[17] J. Wang, Y. Qi, J. Hu, and J. Hu, "Face forgery detection with a fused attention mechanism," in 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), 2022, pp. 722–725.

[18] Trivedi, N.K., Tiwari, R.G., Witarsyah, D., Gautam, V., Misra, A. and Nugraha, R.A., 2022, November. Machine Learning Based Evaluations of Stress, Depression, and Anxiety. In 2022 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS) (pp. 1-5). IEEE.

[19] X. Dong, J. Bao, D. Chen, T. Zhang, W. Zhang, N. Yu, D. Chen,F. Wen, and B. Guo, "Protecting celebrities from deepfake with identity consistency transformer," in proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2022, pp. 9458–9468.

[20] X. Zhu, H. Fei, B. Zhang, T. Zhang, X. Zhang, S. Z. Li, and Z. Lei, "Face forgery detection by 3d decomposition and composition search," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 7, pp. 8342–8357, 2023.

[21] H. Zhao, W. Zhou, D. Chen, T. Wei, W. Zhang, and N. Yu, "Multiattentional deepfake detection," in proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2021, pp. 2185–2194.

[22] J. Cao, C. Ma, T. Yao, S. Chen, S. Ding, and X. Yang, "End-toend reconstruction-classification learning for face forgery detection," in proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2022, pp. 4113–4122.

[23] D. CIFTCIUA and Y. Fakecatcher, "Detection of synthetic portrait videos using biological signals," IEEE TransactionsonPatternAnalysis and Machine Intelligence, 2020.

[24] P. Saikia, D. Dholaria, P. Yadav, V. Patel, and M. Roy, "A hybrid cnnlstm model for video deepfake detection by leveraging optical flow features," in 2022 International Joint Conference on Neural Networks (IJCNN). IEEE, 2022, pp. 1–7.

[25] I. Masi, A. Killekar, R. M. Mascarenhas, S. P. Gurudatt, and W. AbdAlmageed, "Two-branch recurrent network for isolating deepfakes in videos," in Proceedings of the European conference on computer vision (ECCV), 2020, pp. 667–684.

[26] I. Ganiyusufoglu, L. M. Ngo, N. Savov, S. Karaoglu, and T. Gevers,ˆ "Spatio-temporal features for generalized detection of deepfake videos," arXiv preprint arXiv:2010.11844, 2020.

[27] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," Proceedings of Machine Learning and Systems, vol. 2, pp. 429–450, 2020.

[28] W. Zhuang, Y. Wen, and S. Zhang, "Joint optimization in edgecloud continuum for federated unsupervised person re-identification," in Proceedings of the 29th ACM International Conference on Multimedia, 2021, pp. 433–441.

[29] C.-H. Yao, B. Gong, H. Qi, Y. Cui, Y. Zhu, and M.-H. Yang, "Federated multi-target domain adaptation," in proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2022, pp. 1424–1433.

[30] R. Shao, P. Perera, P. C. Yuen, and V. M. Patel, "Federated generalized face presentation attack detection," IEEE Transactions on Neural Networks and Learning Systems, 2022.

[31] H. Zhou, G. Yang, H. Dai, and G. Liu, "Pflf: Privacy-preserving federated learning framework for edge computing," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1905–1918, 2022.

[32] X. Liu, H. Li, G. Xu, Z. Chen, X. Huang, and R. Lu, "Privacy-enhanced federated learning against poisoning adversaries," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4574–4588, 2021.

[33] Zahra R, Shehzadi A, Sharif MI, Karim A, Azam S, De Boer F, Jonkman M, Mehmood M. Camera-based interactive wall display using hand gesture recognition. Intelligent Systems with Applications. 2023 Sep 1;19:200262.

[34] W. Zhuang, X. Gan, Y. Wen, X. Zhang, S. Zhang, and S. Yi, "Federated unsupervised domain adaptation for face recognition," arXiv preprint arXiv:2204.04382, 2022.

[35] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "Faceforensics++: Learning to detect manipulated facial images," in proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 1–11.

[36] B. Zi, M. Chang, J. Chen, X. Ma, and Y.-G. Jiang, "Wilddeepfake: A challenging real-world dataset for deepfake detection," in Proceedings of the 28th ACM international conference on multimedia, 2020, pp. 2382– 2390.

[37] L. Jiang, R. Li, W. Wu, C. Qian, and C. C. Loy, "Deeperforensics-1.0: A large-scale dataset for real-world face forgery detection," in proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2020, pp. 2889–2898.

[38] C. JEONG and T. KIM, "Eye blink detection using algorithm based on dlib and opencv library for game players in competitive environments," Journal of International Research in Medical and Pharmaceutical Sciences, pp. 33–45, 2021.
[39] Ramya, R., A. Anandh, K. Muthulakshmi, and S. Venkatesh. "Gender recognition from facial images using multichannel deep learning framework." In Machine Learning for Biometrics, pp. 1

Dr. Vinay Gautam was born in India in 1981. He received the B.E. and M.E. degrees in Computer engineering from the Kurukshetra University in 2006 and the Ph.D. degree in CSE from Jawaharlal Nehru University, India in 2014. From 2007 to 2012, he was a Research Assistant with JNU lab. Since 2018, he has been Professor with the CSED, Chitkara University. He is the author of books, more than 100 articles, and more than 4 inventions. His research interests include Deep leaning and machine learning

Dr. Gaganpreet Kaur is currently working as an Professor at Department of Computer Science & Engineering, Chitkara University, Punjab, India. She has obtained Ph.D (CSE),from I.K. Gujral Punjab Technical University, Jalandhar, M.Tech (CSE), from I.K. Gujral Punjab Technical University, Jalandhar and B.Tech (CSE), from Kurukshetra University. She has rich teaching experience of 19 years. She has published more than 100+ research articles in various peer reviewed, SCI, Scopus Journals, International and National Conferences in the field of computer science. She has published more than 17 Indian patents. She has authored a book on biometrics. She has guided a Ph.D scholar and 38 students have completed M. Tech thesis under her guidance. She has acted as a guest editor in multiple journals. She has been reviewer and session chair for various conferences. She has delivered expert talk in various colleges and universities. Her research interest includes biometrics, image processing, forensic science, cloud computing, healthcare sector.

Meena Malik is currently working as an Associate Professor at Department of Computer Science & Engineering, Chandigarh University, Punjab, India. She has received Ph.D. from Maharishi Dayanand University, Rohtak, Haryana, India in 2019. She has teaching experience of more than 10 years and efficiently published more than 35 papers in various peer reviewed, SCI, Scopus Journals, International and National Conferences. Her research interests include blockchain, cybersecurity, IoT security, and network and cloud security.

Dr. Ankush Pawar is a Professor and Head Of Department in Computer Science and Engineering at Vishwaniketan Institute of Management Entrepreneurship and Engineering Technology, Khalapur, Maharasshtra India. He received his PhD degree in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi in 2022 and B.Tech and M.Tech from Dr. Babasaheb Ambedkar Technological University, Lonere. He has 21 years of teaching experience. He has published 27 papers in international journals and conferences. His main research areas of interests are Cloud Computing, IoT, Storage and Network Security.

Akansha Singh is B.Tech, M.Tech and PhD in Computer Science. She received her PhD from IIT Roorkee in image processing and machine learning. Currently, she is working as Professor in School of Computer Science and Engineering, Bennett University, Greater Noida, India. She has served as Associate Editor and guest editor of several journals. Dr. Singh has also undertaken government funded project as Principal Investigator. Her research areas include image processing, remote sensing, IoT and machine learning.

Krishna Kant Singh is working as Director, Delhi Technical Campus,Greater Noida, India. He has wide teaching and research experience. Dr. Singh has acquired B.Tech, M.Tech, MS, and Ph.D. (IIT Roorkee) in the area of image processing and Machine Learning. He has authored more than 140 research papers in Scopus and SCIE indexed journals of repute. He has also authored 25 technical books. He is an associate editor of Journal of Intelligent and Fuzzy Systems (SCIE Indexed), IEEE ACCESS (SCIE Indexed) and Guest Editor of Open Computer Science, Wireless Personal Communications. He is serving as the member of Editorial board of Applied Computing and Geoscience (Elsevier).

S.S. Askar received his BSc. Degree in mathematics and the MSc. degree in applied mathematics from Mansoura University, Egypt, in 1998 and 2004, respectively. He got his PhD in Operation research from Cranfield University from UK in 2011. He works as an associate Professor at Mansoura University Egypt since 2016. He has joined King Saud University in 2012 and till present he works at the Department of Statistics and Operation Research at King Saud University as a professor. His main interests lie in game theory and its applications that include mathematical economy, dynamical systems and Network analysis.

MOHAMED ABOUHAWWASH} received the BSc and MSc degrees in statistics and computer science from Mansoura University, Mansoura, Egypt, in 2005 and 2011, respectively. He finished his Ph.D. in Statistics and Computer Science, 2015, in a channel program between Michigan State University, USA, and Mansoura University, Egypt. He is an Associate Professor with the Department of Mathematics, Faculty of Science, Mansoura University, Egypt. Dr. Abouhawwash was a recipient of the best master's and Ph.D. thesis awards from Mansoura University in 2012 and 2018, respectively.