IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 10, No. 6, December, 2023, pp. 2265-2273
Journal homepage: http://iieta.org/journals/mmep

Enhancing Privacy Protection in Online Federated Learning: A Method for Secure Face Image De-Identification Using a Modified Diffie-Hellman Algorithm

Venkata Nagaraju Thatha[1], Srihari Varma Mantena[2], Chandra Sekhar Reddy LingaReddy[3], Phanikanth Chintamaneni[4], Revathy Pulugu[5], Venkata Subbaiah Desanamukula[6*]

[1] Department of Information Technology, MLR Institute of Technology, Hyderabad 500043, India
[2] Department of Computer Science and Engineering, Sagi Rama Krishnam Raju Engineering College, Bhimavaram 534204, India
[3] Department of Computer Science and Engineering (Data Science), CMR College of Engineering & Technology, Hyderabad 501401, India
[4] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur 520002, India
[5] Department of Computer Science and Engineering, Narsimha Reddy Engineering College, Hyderabad 500100, India
[6] Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram 521230, India

Corresponding Author Email: subbaiah@lbrce.ac.in

https://doi.org/10.18280/mmep.100642

Received: 21 July 2023
Revised: 18 October 2023
Accepted: 31 October 2023
Available online: 21 December 2023

Keywords:
face images, federated learning, genetic algorithm, extended version of Diffie-Hellman procedure, deep learning, data leakage, privacy

ABSTRACT

The proliferation of face images, alongside their widespread dissemination and easy accessibility through social media, underscores a pressing challenge to personal identification information protection. Conversely, advancements in identity-agnostic computer vision technologies offer valuable benefits, necessitating cautious utilization of face images to safeguard individual privacy. 'Face de-identification', or 'face anonymization', refers to the process of altering an original face image to a near-identical one that obscures the subject's actual identity. Existing de-identification strategies, despite considerable efforts, often fall short in photo-realism or fail to strike an optimal balance between privacy and utility. This study proposes an approach for generating de-identified facial images using instances, addressing the potential privacy breaches and identity exposure associated with facial features. The proposed system involves a two-stage training process. Initially, a federated learning framework is suggested, enabling knowledge amalgamation through the mutual exchange of model parameters among clients during federated training, devoid of data sharing. Subsequently, sensitive information is secured using an enhanced version of the Diffie-Hellman algorithm coupled with a genetic algorithm. In the event of data loss or corruption, an optimized genetic algorithm (OGA) is employed to successfully restore the data, thereby offering protection against potential insider threats in federated learning. The decryption process is then executed as if the user had initiated the request. Experimental results demonstrate that the proposed federated learning approach delivers performance equivalent to centralized learning, thereby validating the practicality and effectiveness of the suggested architecture. Specifically, a model of the federated learning-deep convolutional neural network (FL-DCNN) achieved an accuracy of 95.2%, precision and F1-score of 95%, recall of 96%, and a final specificity of 96.80%.

1. INTRODUCTION

The ubiquitous presence of mobile phones in contemporary society facilitates effortless capture of spontaneous self-portraits. Particularly, the swift evolution of media and network technologies has amplified the accessibility of a vast array of photographs [1]. Nevertheless, burgeoning image retrieval and face verification models have enabled indexing and analysis of data potentially sensitive to individual privacy with an unprecedented degree of precision [2]. Consequently, the scale of private information inadvertently divulged among image sources publicly accessible, knowingly or unknowingly, is often grossly underestimated [3]. The unguarded facial images, combined with state-of-the-art computer vision technology, present myriad, and potentially catastrophic, opportunities for misuse [4].

The increasing application of facial recognition in sectors such as banking and other financial transactions amplifies the significance of this technology, alongside the use of biometrics. Progress in microelectronics and vision systems have mainstreamed biometrics as a lucrative industry [5]. Within the biometrics sphere, facial recognition holds paramount importance. Modern information is juxtaposed with human characteristics using biometrics. An efficient method is

employed to extract and apply facial features, with minor modifications to the original algorithm model to further enhance its accuracy [6]. Computerized facial recognition harbors substantial potential in areas such as criminal identification, surveillance, and identity verification. The face in the input image is initially isolated using face detection processes, followed by the image processing phase which cleans the face for easy recognition [7].

As the avenues for individual identification worldwide continue to multiply daily, facial recognition technology has emerged as an indispensable necessity in the present era [8]. Over the past two decades, research in face recognition has thrived owing to its extensive applicability in domains such as image analysis and comprehension. Face recognition finds utility in a diverse array of fields, from computer science to medicine [9, 10]. Facial recognition is user-friendly, compact, and can swiftly gain ubiquity. Security, entertainment, attendance tracking, and even financial transactions represent potential applications for facial recognition technology [11]. Despite the robust performance of current facial recognition systems in laboratory conditions, their real-world application in surveillance systems is significantly hampered by challenges related to image quality, background clutter, variations in illumination, and changes in facial and expression posture.

Typically, face recognition systems encompass three stages: image preprocessing, feature extraction, and recognition classification [12]. Geometric features include facial characteristics that can be extracted such as lips, nose, eyebrows, etc. The detected and processed face is matched with a database of known faces to ascertain the individual's identity. The surveillance system necessitates human supervision. However, human monitoring presents limitations in terms of reliability, scalability, and individual identification [13]. Facial occlusions, including beards and accessories (glasses, hats, and masks), complicate the evaluation of face recognition systems in a realistic environment. Another critical factor to consider is the abundance of terminologies used to denote a similar concept: Macro and micro terminologies find their place on an individual's face, and effective recognition becomes challenging due to the diversity of such expressions [14, 15]. An ideal face recognition system would cater to a large number of users with minimal photographs, while remaining resilient to changes in lighting, emotions, postures, and occlusions.

The primary contributions of this paper can be summarized as follows:

i. This study offers a practical and effective federated learning system for face recognition and image security.
ii. The proposed architecture facilitates the optimal utilization of resources.
iii. As a case study, facial photographs are incorporated within the suggested framework. The CelebA-HQ dataset is used as the basis for several experimental comparisons.
iv. The experimental results from this work affirm that federated learning is an effective strategy to address data privacy concerns within the context of the knowledge fusion procedure involved in intelligent prediction.

The remainder of this paper is organized as follows: Section 2 provides an overview of the relevant literature. The methodology is delineated in Section 3, while Section 4 discusses the results. Section 5 constitutes the conclusion of the paper.

2. LITERATURE REVIEW

The rapid development in biometric technology has stimulated significant advancements in various fields, including attendance automation. A notable contribution to this domain was made by Kulkarni et al. [16], who developed a system capable of leveraging face recognition technology for automated student attendance. Their system, which uses CCTV to capture student images and store them in a database, not only relieves educators from manually taking attendance but also generates comprehensive attendance records on a weekly and monthly basis.

Progress in recognizing obscured facial features was recently reported by Dosi et al. [17]. They proposed Seg-DGDNet, an innovative approach that applies segmentation models for identifying unobscured pixels on the subject's face. Their guided dropout approach then concentrates the recognition model on these features. Seg-DGDNet was evaluated using three datasets, including images of faces obscured by masks or glasses. The model demonstrated significant superiority over existing face recognition techniques across a variety of disguised and high-resolution face datasets.

Zennayi et al. [18] proposed a unique approach to enhance the certainty of face recognition by utilizing the overall settings of the image. Their method not only improved recognition rates but also minimized the increase in false alarms. Furthermore, the developed algorithms were optimized for real-time implementation while maintaining high efficiency. Evaluation results on both public and private datasets showed an increase in accuracy when using the system as a whole, with no recorded false alarms.

Contardo et al. [19] introduced the Face Recognition from the Mugshots Database (FRMDB), containing 28 mugshots and five surveillance footage of 39 individuals. The primary objective of the FRMDB is to explore the impact of different mugshot angles on the accuracy of facial recognition from surveillance video frames. Accuracy tests were conducted on two CNNs and the VGGFace2 dataset to validate the FRMDB and provide an initial benchmark. Their findings highlighted the characteristics of the proposed database, showing that the subset of mugshots consisting of the frontal image and the right profile achieved the lowest accuracy result.

In the field of crime-solving, Lakshmi and Arakeri [20] developed an automated sketch-based face recognition method. The histogram of oriented gradients (HOG) method was implemented due to its consistent results for both sketch and photo, regardless of lighting conditions. Once a face was detected, it was encoded in 128 different ways via a deep neural network. The network was fine-tuned such that similar-looking faces had closely related encodings, while strangers had distinct encodings. A minimum distance criterion was used to find the closest match among these encodings. The method was evaluated on the CUHK database and demonstrated accurate results.

Lv et al. [21] proposed a face detection and recognition scheme for criminal documentation using a multi-task network. This system had the capability to automatically recognize criminal faces in real-time. A distinctive feature of the algorithm was its one-shot learning capability, requiring only a single example of the criminal's face for recognition. The aim was to recognize the criminal's face, retrieve their profile from a database, and alert the authorities to their presence.

Vijayalakshmi et al. [22] developed a system that could

identify human faces detected in an input image. The Viola-Jones Algorithm was used to detect faces in the input image after the system was trained with a database of faces and non-faces. Feature extraction from the training dataset was accomplished using principal component analysis (PCA), and the system was trained for face recognition using support vector machine (SVM) classification. PCA was used for feature extraction from the input image, and SVM was utilized for multiclass classification in face recognition.

3. BACKGROUND OF FEDERATED LEARNING

As was previously said, combining large amounts of data helps improve machine learning models. In the medical industry, however, access to data is severely limited due to concerns over patient confidentiality and individual privacy. Intelligent medical diagnosis systems are best developed using decentralized, collaborative machine-learning methods that protect users' privacy. Since Google's 2016 proposal of federated learning, the notion has grown to include specialized frameworks [23]. Federated learning offers a secure and effective solution for addressing data and label shortages, given that it allows for the localized realization of training models to synthesize and fuse information as long as by several parties' data.

The safe implementation of machine learning algorithms has been the subject of extensive study. Using homomorphic circuits [24], researchers are hoping that linear regression, a key machine-learning technique, can fit the optimal curve without revealing the input data. Using the assumption of privacy protection, the gradient boosting decision trees (GBDT) secure computing system allows for the training of models by several private parties, which can subsequently be safely aggregated. Both the secure boost framework for vertical federation and the loose privacy constraint technique for horizontal federation [25] offer effective solutions for GBDT safe computing following WeBank's proposal of an industrial-level federated learning framework. Mobile federated learning, federated communication efficiency optimization, and scalable federated production systems are all areas of focus at Google. In addition, cross-silo federated learning [26] handles no more than a few hundred trustworthy data silos outfitted with robust computing resources and high-speed connections, while cross-device federated learning [26] handles a rudimentary processing power and sluggish communication channels.

3.1 Problem definition

If the face data assume $X = \{(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)\}$, If x_i is a face picture in the range (X, R), then y_i is the identification tag for that image. If Q is used to produce x_i', a de-identity face picture, then *f*, a random generator, satisfies Eq. (1).

$$Pr[f(x_i) \in y_i] \leq \delta \times \Pr\left[f(x_i') \in y_i\right] \tag{1}$$

The constant d indicates the level of privacy protection and the likelihood that the random method *f* will correctly identify the de-identification face picture x_i' as the original identity tag y_i denotes the privacy risk leaking. The de-identity face picture must ensure the privacy image x_i' is made available without being misclassified by chance algorithm *f*. In other words, acquaintances will recognize it as expected. Therefore, as demonstrated in Eq. (2), the size of the newly introduced adversarial cases should be sufficiently modest.

$$\begin{aligned} &min\|\xi\|_e \\ &s.t \;\; Pr[f(x_i) = y_i] \leq \delta \times Pr[f(x_i') = y_i] \end{aligned} \tag{2}$$

In order to guarantee the obtainability of a de-identity face picture while the algorithm Q generates adversarial instances without compromising the privacy of the face image, the adversarial examples should be kept as short as feasible x_i'.

4. PROPOSED SYSTEM

4.1 Dataset description

The CelebA-HQ datasets [27] are used to train our network in stage-I of the project, and they feature 30K high-resolution photos of celebrities together with different demographic information including age, gender, and ethnicity. It uses a random selection process to choose 27K training photos and 3K test images. We also run tests on the Celebi [28] datasets to show how well our model generalizes and to make it easy to make conditional comparisons. Aligning and cropping each image to a 256×256 resolution ensures that the whole face and portions of the backdrop are visible.

4.2 Preprocessing

Preprocessing a picture occurs after its initial capture and before it is used in any further processing. The two primary phases of preprocessing are grayscale conversion and edge detection.

4.2.1 Grayscale conversion

The picture is obtained from the camera in RGB format (R, G, B). One red pixel is joined with two blue ones and one green one to make an RGB pixel. With 1 pixel requiring 8 bits, the computation for an RGB picture would require 24 bits. A grayscale picture is always 8 bits since each pixel is a scalar. Therefore, the equation for converting RGB to grayscale is:

$$Grayscale = 0.3 * R + 0.59 * G + 0.11 * B \tag{3}$$

Here *R*, *G*, and *B* signify red, green, and blue pixels, correspondingly.

4.2.2 Canny edge detection

The Canny filter may identify picture edges by looking for dramatic tonal shifts. We're utilizing it to sharpen the photographs' borders. The more these benefits are honed, the more precise our expression recognition will become. Gaussian and Sobel filters make up the filter. To begin, grayscale pictures are given a Gaussian filter with a specified value to facilitate edge discovery.

$$G = \frac{1}{(2\pi\sigma^2)} e^{-(x^2+y^2)/2\sigma^2} \tag{4}$$

To locate edges in subsequent photos, the Sobel filter is used. The filter that is employed to locate the borderlines is:

$$G_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \tag{5}$$

For edges, the filter is:

$$G_y = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \quad (6)$$

In order to locate all of the edges in the filter, the horizontal and vertical edges are calculated.

$$A = x = \sqrt{G_x^2 + G_y^2} \quad (7)$$

Images with edges are subjected to the hysteresis threshold, the third and final phase of the savvy edge detector. The cutoff is denoted by the expression:

$$H = \frac{1}{1+e^{-x}} \quad (8)$$

Initial decisions are made on the range of allowed values. One is allocated to the pixel if its value is more than the threshold; zero is assigned if the pixel's value is less than the threshold. When the value is the same as the cutoff, the cutoff is maintained. The final improved image is created by adding the edges to the original. This makes face feature identification and extraction simple, which boosts the system's effectiveness.

4.3 Feature extraction and classification using DCNN

After the pre-processing stage of a facial expression recognition system, features are extracted. It is a method of dimensionality reduction that extracts the most important features of a picture. It's a simplified representation of the data extracted from the image. The primary purpose of feature extraction is to scale down a high-resolution image into a more manageable feature vector for processing without sacrificing accuracy or quality.

Deep convolutional neural networks (DCNNs), a type of deep learning-based technique, are used [29]. DCNNs have an input layer, an output as the initial step in feature extraction. It is made up of a series of filters or kernels, each of which is convolved with the input picture separately before sending the result onto the layer above it. The primary goal of the convolution procedure is to recover salient features, such as edges, from the input picture. The dimensions of the output convoluted features are lower than those of the original input picture. Each pixel added to the input picture matrix is represented by a stride.

Value of the convolutional matrix at each layer.

$$W_{out}(i) = \frac{(W_{in}(i)-F+2P)}{S} + 1 \quad (9)$$

The matrix value at apiece pooling layer is,

$$\frac{(W_{out}(i)-F)}{S} + 1 \quad (10)$$

The size of the input matrix Win, the size of the output matrix Wout, the padding factor *P*, the filter size *F*, and the stride *S*. The pooling layer, also sampling, shrinks the data representation in space. There are two common approaches to pooling: maximum pooling and average pooling. Max pooling takes the highest value across all filter sub-regions into account. Like average pooling, median pooling takes an average across all sub-regions. The space between the convolutional layers can be filled by a pooling layer. The overfitting issue is kept under control, and the number of parameters is decreased, all thanks to the pooling layer.

To get rid of the negative value, RELU uses an element-wise non-function, f(x)=max (0, x). The activation function softmax is also commonly used on CNN. In the completely connected layer, all of the layers are linked to all of the neurons in the next layer, much like in a multi-layer perceptron. At last, the convolutional neural network's output layer is shown. As can be seen in Figure 1, the suggested system makes use of a CNN with the following architecture: to cap things off. After each set of two convolution layers comes a pooling layer.

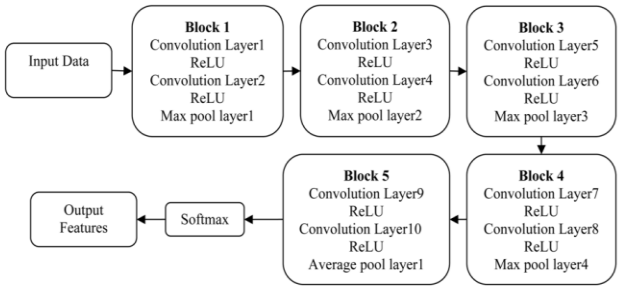

Figure 1. Architecture of the feature extraction technique

After each set of four layers is implemented, and finally, an average-pooling layer is implemented after the final set of convolution layers. Except for the last convolutional layer, the ReLU rectified linear unit follows every convolution layer. Therefore, the DCNN can extract the specific, accurate, and informative features from the facial picture during feature extraction. Once the characteristics have been extracted, the same model can be used to classify the input photos and determine which ones include human faces. The next section details how federated learning may be used to secure this data throughout its cloud transmission.

4.4 Data encryption based on federated learning

Data encryption based on federated learning is an approach to secure and protect sensitive data while allowing for collaborative model training. Federated learning is a decentralized machine learning technique where multiple parties (such as devices or organizations) collaborate to train a global machine learning model without sharing their raw data. Data encryption is used in federated learning to ensure the privacy and security of the participants' data.

4.4.1 Overview

The user platform, federated server are the three components that make up the proposed federated learning architecture.

Tools and data servers are two components of the user platform. The data server offers the labelled data necessary for model training, and the tools give customers access to a variety of facial prediction services. Platform-created datasets and external data from partner institutions are also viable options.

A job scheduler, model container, and federated module are all parts of the federated server. The HGA-IDHA-encrypted service request is routed by the task scheduler to either an internal or external model container for prediction. HGA-IDHA encryption is performed on the response before it is sent back to the model container. When a model's prediction is off, the federated module will bring it online for federated training optimization.

When online federated training optimization begins, the federated clients retrieve the matching model from the federated server. Using their own data, the clients train the model independently before sending the encrypted parameters to the centralized server through HGA-IDHA. When combining data from several clients, the federated server uses a method called federated averaging [30]. Each federated client receives an updated set of model limits. Until the model is trained to completion, the online federated training optimization process is cycled again.

4.4.2 Workflow

This diagram illustrates the process as a whole. A user service request begins with a user action on the user platform. The task scheduler receives the encrypted service request. Second, the task scheduler's brains interpret the request and pair it with an internal or external model container. The selected model will complete the forecast and send back the user's encrypted result. Finally, the processing hub verifies that the user is pleased with the outcome; if not, it issues a warning to the federated component. To optimize the model, the federated server conducts online federated training with K clients and stores the results in the associated model container as a self-built model. The task scheduler then gives the user the best possible outcome.

4.4.3 Robustness

In this part, we examine the reliability of the federated education network. Since the user cannot get direct access to the model container, the processing centre uses HGA-IDHA encryption to increase the security of the request and protect the confidentiality of the model. The task scheduler uses the weighted algorithm [31] for load balancing if there are too many requests and the queueing time is too long. In addition, load-balancing calculations are carried out with the aid of the distributed computing framework Spark [32]. Spark may significantly enhance performance when the user wants to query models in two independent model containers. The encrypted prediction results are returned by the model container. This prevents harmful links or code from replacing the original data. The system was designed to be easily expanded. It's flexible enough to accommodate a growing number of users, different kinds of knowledge fusion models, and other parties involved in federated online learning and instruction.

4.4.4 Encryption using hybridization of genetic procedure and extended form of Diffie-hellman algorithm (HGA-IDHA)

We conclude that there are still problems with security assaults based on our review of the relevant literature. The cloud is becoming vulnerable to a wide variety of threats as its use grows ever more widespread. Due to the gaps that prevent widespread use of cloud computing, few people are aware of its benefits. The voids reflect the attack problems and risks that make customers wary of the cloud service.

Genetic algorithms are a type of explore-based optimization method. Optimized Genetic algorithm is a heuristic search strategy that provides the best answer for the dilemma of the alternative approach by making radical adjustments to create a new one and choosing the most promising person.

Evolutionary concepts such as combination crossover and mutation, as well as other bio-inspired operators, are being processed as part of this shift towards Darwin's survival of the fittest. The offspring are then numbered according to their fitness, and the population as a whole grows. The healthiest parents are selected based on their children's fitness scores. It is frequently employed to locate optimal or almost optimal answers to challenging problems.

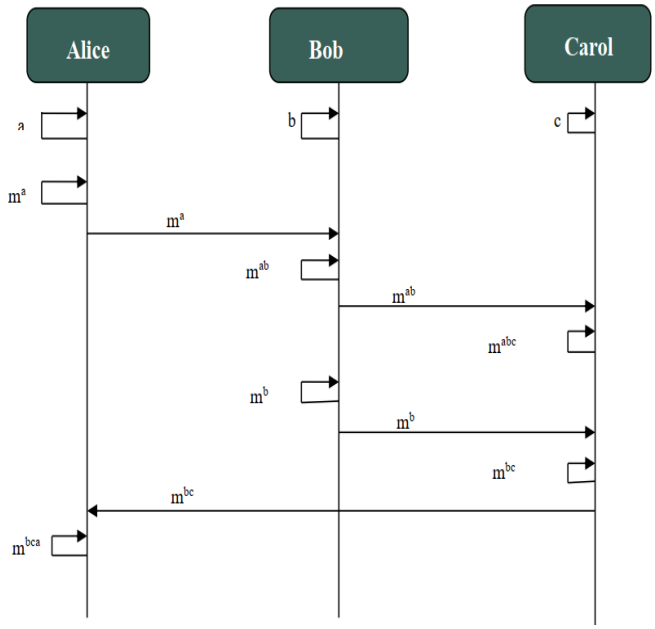

Figure 2. Three parties protracted Diffie Hellman key conversation

Extended versions of Diffie Hellman allow several users to interact with one another, similar to the sender-receiver-only nature of the original protocol. Both the sender and the recipient will need a private key in order to complete the encryption and decryption processes, respectively. In the expanded version of the Diffie Hellman algorithm, the private identification key of each participant is used to generate a shared secret key between them, allowing the server to communicate with only those users in possession of that shared secret key. Users end up exchanging keys, and the protocol is validated in such a way that, ultimately, each user should obtain a secret key by appending their identification key. The number of operations and exponentiation in the modified Diffie Hellman algorithm is lowered from N2 to 3N-2 and N to log 2(N)+1, respectively.

Figure 2 depicts the method in action, showing how an enhanced version of the Diffie-Hellman algorithm may be combined with an optimized Genetic algorithm to create a safe path in an otherwise insecure network. If an intrusion is detected during transmission, the process is repeated, and if none occurs, communication continues as usual.

Clarification of the flow diagram is given below

- Initially, the number of populations to be subjected to the selection process is taken into account with the goal of obtaining an optimal path from among them.
- Then, the optimized pathways undergo the crossover technique to get even more refined results.
- Crossover between optimized routes yields the optimized one; mutation on the optimized one, resulting in some variation in the individual, makes the path distinct.
- After obtaining the one-of-a-kind item, the fitness function is utilized to determine if the person lives up to standards.
- If any outside interference is discovered when

checking an individual's fitness function, the check will fail. If the procedure is not interrupted, it will resume and split the number of users into two groups, giving each group a unique private key or user key.

- To create a one-of-a-kind secret key, users must first trade their private keys with one another. If a user has that secret key, the server will only send data to them, even if the network isn't optimal. A safe transfer within an untrustworthy network is planned.

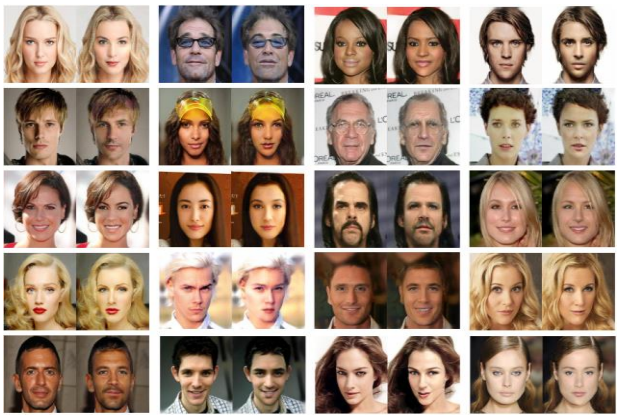

Figure 3. Illustrations of face anonymization samples

Key exchange Diffie-Hellman key conversation parties, allowing for more accurate data correlation across the board. The number of characters needed for this exchange of keys is rather small. When a secret key is used for both encryption and system, as it is in the Diffie-Hellman key exchange, security is hard to crack.

Algorithm for Diffie-Hellman key exchange

Step 1: The secret key between the user and server is identified by using Diffie Hellman key as $A^{pd} = B \in M$, where A^{pd} is a computed data from both the user and server;

Step 2: The map of B is given to the group G by user and server then the data is received as $B_g = G$, where G refers to the group of facial information;

Step 3: By multiplying M and B_g, the message ($M \in G$) is encrypted as:

$M * B_g = Y$, and the encrypted message Y is transmitted to the user;

Step 4: The user decrypts the message by computing B_g inversely and receives the message M as, $Y = B_g^{-1} = M$, where M is a decrypted message.

Figure 3 shows the sample images of original as well as re-identified faces.

Each pair consists of an actual photograph on the left and a synthetic representation of the same photograph on the right. Perceptually, the results reveal that face identities are changed in a natural way, and in the meantime, most of the non-identity-related information is shared between each pair of photos.

5. RESULTS AND DISCUSSION

5.1 Evaluation metrics

Area under the curve (AUC), accuracy, precision, recall, F1-score, and specificity were calculated. Statistics like true positives (TP), false negatives (FN), false positives (FP), and true negatives (TN) are used to determine how well a test performs. Here, TP and TN represent the proper number of margin positive and margin negative photos, respectively, whereas FP and FN represent the incorrect number of margin negative images incorrectly accepted as margin positive.

Accuracy: The accuracy scores reveal the proportion of times the models correctly predicted the outcomes.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{11}$$

Precision: A simple count of "how many of the selected data items are relevant" is displayed. To rephrase, precision measures how accurate the method is by counting how many "positive" observations actually are. Accuracy, then, is a measure of how reliably a model predicts events with positive margins. The following Eq. (12) can be used to determine the level of accuracy achieved.

$$Precision = \frac{TP}{TP+FP} \tag{12}$$

Recall: "How many appropriate data items are chosen" is what this shows. How many of the good observations may be attributed to the algorithm's predictions is displayed? The recall is calculated by dividing the number of correct identifications by the combined number of correct and incorrect identifications (Eq. (13)): As shown in Eq. (13), recall is the percentage of margin positive photos that were correctly identified.

$$Recall = \frac{TP}{TP+FN} \tag{13}$$

Specificity: Calculates (using Eq. (14)), how well it does at identifying margin negative photos.

$$Specificity = \frac{TN}{TN+FP} \tag{14}$$

F1 score: The F1 score is a weighted average of the recall and accuracy scores (Eq. (15)).

$$F1 - Score = 2 * \frac{Precision \times Recall}{Precision+Recall} \tag{15}$$

Table 1. Analysis of proposed FL model for 60%-40% training and testing data

Models	Accuracy	Precision	Recall	F1-Score	Specificity
DBN	85.5	87	86	86	86
RNN	87	91	87	88	87
CNN	91.5	91.5	91.5	91.5	95
FL-DCNN	95.2	95	96	95.16	96.80

Table 2. Comparative analysis of the proposed model for facial detection by using 80%-20% of the data

Models	Accuracy	Precision	Recall	F1-Score	Specificity
DBN	87.30	90.3	88.56	88.50	88.50
RNN	92.67	91.45	91.67	91.39	90.67
CNN	91.34	90.78	91.78	91.39	96.27
FL-DCNN	96.5	97.0	97.0	97.0	98.7

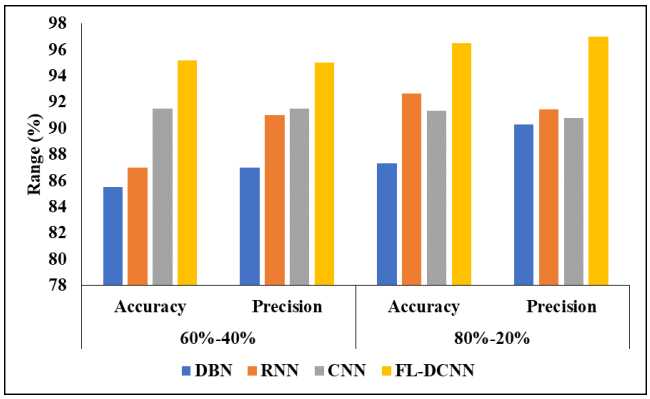

Figure 4. Analysis of projected perfection with existing procedures

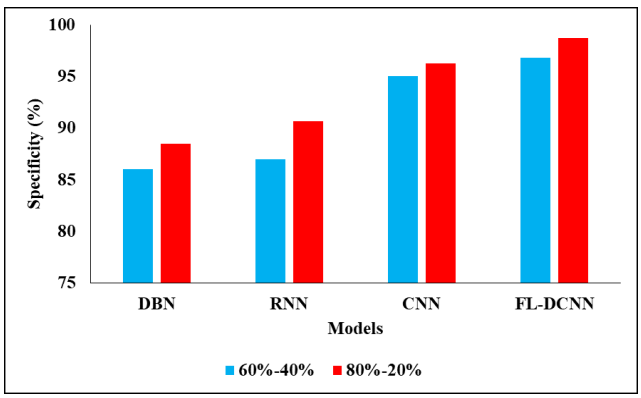

Figure 5. Specificity investigation

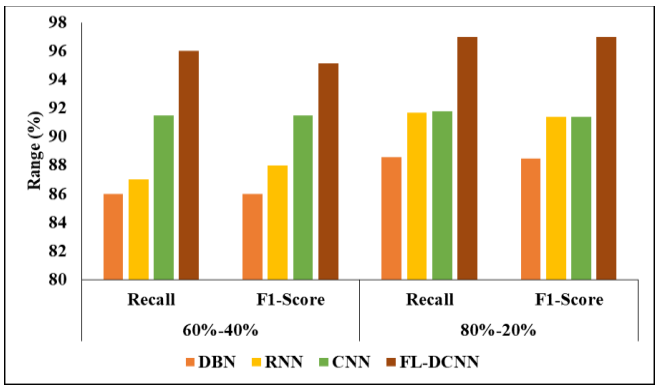

Figure 6. Comparative analysis of the projected model in terms of numerous metrics

Table 1 represent the Analysis of the proposed FL model for 60%-40% of training and testing data. The analysis of the DBN model reached an accuracy of 85.5 and a precision value of 87 and also a recall value of 86, an F1-score value of 86, and the finally Specificity value of 86, respectively. And then, another model of the RNN model reached an accuracy of 87 models reached the accuracy of 91 and a precision value of 87 and also the recall value of as87 and the F1-score value of 88, and the finally Specificity value of 87, respectively. And then, another model of the CNN model reached the accuracy of 91.5 and the precision value as 91.5 and also the recall value as 91.5 and the F1-score value as 91.5, and the finally Specificity value as 95, respectively. And then, another model of the FL-DCNN model reached an accuracy of 95.2 and a precision value of 95 and also a recall value of 96, an F1-score value of 95.16, and the finally Specificity value of 96.80, respectively.

Table 2 represents the comparative analysis of the proposed model for facial detection using 80%–20% of the data. In the analysis concept, the DBN model reached an accuracy of 87.30, a precision value of 90.3, a recall value of 88.56, an F1-score value of 88.50, and a final specificity value of 88.50, respectively. And then another model of the RNN model reached an accuracy of 92.67, a precision value of 91.45, a recall value of 91.67, an F1-score value of 91.39, and finally a specificity value of 90.67, respectively. And then, another model of the CNN model reached an accuracy of 91.34 and a precision value of 90.78, as well as a recall value of 91.78, an F1-score value of 91.39, and a final specificity value of 96.27, respectively. And then another model of the FL-DCNN model reached an accuracy of 96.5 and a precision value of 97.0, as well as a recall value of 97.0, an F1-score value of 97.0, and a final specificity value of 98.7, respectively. The results analysis is shown in Figures 4-6.

6. CONCLUSION

In order to preserve the confidentiality of images, we offer the FL-DCNN basis, which is the first to use deep neural networks in conjunction with differential privacy techniques. The first step in our strategy is face recognition, then HGA-IDHA-based data security. Our research article provides a decentralised learning architecture for face recognition that complies with data privacy regulations and is capable of knowledge fusion via parameter aggregation. The system's task scheduler helps with multi-user access by spreading out the processing burden. The efficiency gains from computation are conditional on the distributed computing infrastructure. The encryption methods are the backbone of the federated training process, protecting the confidentiality of requests and outputs. The second step adds HGA-IDHA directly to the individuality representation to guarantee privacy protection while leaving the attribute representation alone to reliably maintain visual similarity. Furthermore, the privacy budget is flexible. Thus, different anonymization outcomes may be achieved. Our untried results show that our approach outperforms both baseline and state-of-the-art solutions in terms of privacy protection and picture usefulness. In addition, our approach generalises well. We plan to dig more into the tension between user privacy and legitimate reuse of creative content in the future. It would be intriguing to see whether this work could be applied to videos while maintaining temporal consistency. The trained network may be further evaluated with more comprehensive and evenly dispersed data sets in the future.

7. FUTURE WORK

Explore and develop more efficient and secure encryption techniques that are specifically tailored for protecting facial images during the federated learning process. Consider techniques like homomorphic encryption and advanced cryptographic protocols to enhance security. Apply the proposed method to real-world applications where facial image data needs to be protected, such as in healthcare (patient facial recognition), finance (identity verification), and surveillance (privacy-preserving monitoring).

REFERENCES

[1] Naseri, R.A.S., Kurnaz, A., Farhan, H.M. (2023). Optimized face detector-based intelligent face mask detection model in IoT using deep learning approach. Applied Soft Computing, 134: 109933. https://doi.org/10.1016/j.asoc.2022.109933

[2] Alzu'bi, A., Albalas, F., Al-Hadhrami, T., Younis, L.B., Bashayreh, A. (2021). Masked face recognition using deep learning: A review. Electronics, 10(21): 2666. https://doi.org/10.3390/electronics10212666

[3] Kumar, K.K., Kasiviswanadham, Y., Indira, D.V.S.N.V., Bhargavi, C.V. (2023). Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN). Materials Today: Proceedings, 80: 2406-2410. https://doi.org/10.1016/j.matpr.2021.06.373

[4] Macherla, H., Kotapati, G., Sunitha, M.T., Chittipireddy, K.R., Attuluri, B., Vatambeti, R. (2023). Deep learning framework-based chaotic hunger games search optimization algorithm for prediction of air quality index. Ingénierie des Systèmes d'Information, 28(2): 433-441. https://doi.org/10.18280/isi.280219

[5] Wang, M., Deng, W. (2021). Deep face recognition: A survey. Neurocomputing, 429: 215-244. https://doi.org/10.1016/j.neucom.2020.10.081

[6] Mamieva, D., Abdusalomov, A.B., Mukhiddinov, M., Whangbo, T.K. (2023). Improved face detection method via learning small faces on hard images based on a deep learning approach. Sensors, 23(1): 502. https://doi.org/10.3390/s23010502

[7] Tabassum, F., Islam, M.I., Khan, R.T., Amin, M.R. (2022). Human face recognition with combination of DWT and machine learning. Journal of King Saud University-Computer and Information Sciences, 34(3): 546-556. https://doi.org/10.1016/j.jksuci.2020.02.002

[8] Chen, W., Huang, H., Peng, S., Zhou, C., Zhang, C. (2021). YOLO-face: A real-time face detector. The Visual Computer, 37: 805-813. https://doi.org/10.1007/s00371-020-01831-7

[9] Boyd, A., Tinsley, P., Bowyer, K.W., Czajka, A. (2023). Cyborg: Blending human saliency into the loss improves deep learning-based synthetic face detection. In 2023 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, pp. 6097-6106. https://doi.org/10.1109/WACV56688.2023.00605

[10] Li, X., Lai, S., Qian, X. (2021). DBCFace: Towards pure convolutional neural network face detection. IEEE Transactions on Circuits and Systems for Video Technology, 32(4): 1792-1804. https://doi.org/10.1109/TCSVT.2021.3082635

[11] Ali, W., Tian, W., Din, S.U., Iradukunda, D., Khan, A.A. (2021). Classical and modern face recognition approaches: A complete review. Multimedia Tools and Applications, 80: 4825-4880. https://doi.org/10.1007/s11042-020-09850-1

[12] Veesam, V.S., Ravichandran, S., Babu, G.R.M. (2022). Deep neural networks for automatic facial expression recognition. Revue d'Intelligence Artificielle, 36(5): 809-814. https://doi.org/10.18280/ria.360520

[13] Rajeshkumar, G., Braveen, M., Venkatesh, R., Shermila, P.J., Prabu, B.G., Veerasamy, B., Bharathi, B., Jeyam, A. (2023). Smart office automation via faster R-CNN based face recognition and Internet of Things. Measurement: Sensors, 27: 100719. https://doi.org/10.1016/j.measen.2023.100719

[14] Sethi, S., Kathuria, M., Kaushik, T. (2021). Face mask detection using deep learning: An approach to reduce risk of Coronavirus spread. Journal of Biomedical Informatics, 120: 103848. https://doi.org/10.1016/j.jbi.2021.103848

[15] Hariri, W. (2022). Efficient masked face recognition method during the COVID-19 pandemic. Signal, Image and Video Processing, 16(3): 605-612. https://doi.org/10.1007/s11760-021-02050-w

[16] Kulkarni, S., Shrivastava, P., Bodineni, P.L., Ambhore, N., Choudhari, D., Chaudhari, D. (2023). Attendance Monitoring system using face recognition. Scandinavian Journal of Information Systems, 35(1): 115-123.

[17] Dosi, M., Agarwal, S., Chaudhary, J., Manchanda, S., Balutia, K., Bhagwatkar, K., Vatsa, M., Singh, R. (2023). Seg-DGDNet: Segmentation based disguise guided dropout network for low resolution face recognition. IEEE Journal of Selected Topics in Signal Processing, 1-13. https://doi.org/10.1109/JSTSP.2023.3288398

[18] Zennayi, Y., Benaissa, S., Derrouz, H., Guennoun, Z. (2023). Unauthorized access detection system to the equipments in a room based on the persons identification by face recognition. Engineering Applications of Artificial Intelligence, 124: 106637. https://doi.org/10.1016/j.engappai.2023.106637

[19] Contardo, P., Sernani, P., Tomassini, S., Falcionelli, N., Martarelli, M., Castellini, P., Dragoni, A.F. (2023). FRMDB: Face recognition using multiple points of view. Sensors, 23(4): 1939. https://doi.org/10.3390/s23041939

[20] Lakshmi, N., Arakeri, M.P. (2023). Sketch-based face recognition using deep neural network for criminal investigation. In: Smys, S., Tavares, J.M.R.S., Shi, F. (eds) Computational Vision and Bio-Inspired Computing. Advances in Intelligent Systems and Computing, vol 1439. Springer, Singapore. https://doi.org/10.1007/978-981-19-9819-5_33

[21] Lv, X., Su, M.X., Wang, Z.K. (2021). Application of face recognition method under deep learning algorithm in embedded systems. Microprocessors and Microsystems, 104034, https://doi.org/10.1016/j.micpro.2021.104034

[22] Vijayalakshmi, S., Maheswari, J.U., Jananiyie, K. (2023). Face detection and recognition using machine learning techniques. Journal of Innovative Image Processing, 4(4): 316-327. https://doi.org/10.36548/jiip.2022.4.008

[23] Yang, Q., Liu, Y., Chen, T., Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2): 1-19. https://doi.org/10.1145/3298981

[24] Cheng, K., Fan, T., Jin, Y., Liu, Y., Chen, T., Papadopoulos, D., Yang, Q. (2021). SecureBoost: A lossless federated learning framework. IEEE Intelligent Systems, 36(6): 87-98. https://doi.org/10.1109/MIS.2021.3082561

[25] Li, Q., Wen, Z., He, B. (2020). Practical federated gradient boosting decision trees. In Proceedings of the AAAI Conference on Artificial Intelligence, 34(4): 4642-4649. https://doi.org/10.1609/aaai.v34i04.5895

[26] Yu, H., Liu, Z., Liu, Y., Chen, T., Cong, M., Weng, X., Niyato, D., Yang, Q. (2020). A sustainable incentive scheme for federated learning. IEEE Intelligent Systems, 35(4): 58-69. https://doi.org/10.1109/MIS.2020.2987774

[27] Karras, T., Aila, T., Laine, S., Lehtinen, J. (2017). Progressive growing of GANs for improved quality, stability, and variation. arXiv preprint arXiv:1710.10196. https://doi.org/10.48550/arXiv.1710.10196

[28] Liu, Z., Luo, P., Wang, X., Tang, X. (2015). Deep learning face attributes in the wild. In 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, pp. 3730-3738. https://doi.org/10.1109/ICCV.2015.425

[29] Chen, J.C., Patel, V.M., Chellappa, R. (2016). Unconstrained face verification using deep CNN features. In 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Placid, NY, USA, pp. 1-9. https://doi.org/10.1109/WACV.2016.7477557

[30] McMahan, B., Moore, E., Ramage, D., Hampson, S., y Arcas, B.A. (2017). Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and Statistics, pp. 1273-1282.

[31] Hirsch, P.D. (2019). Task scheduling using improved weighted round Robin techniques. U.S. Patent 10,324,755.

[32] Zaharia, M., Chowdhury, M., Franklin, M.J., Shenker, S., Stoica, I. (2010). Spark: Cluster computing with working sets. In 2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10), pp. 1-7.