International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.547 ISSN: 1308-5581 Vol 14, Issue 05 2022

Face Recognition Based Website Authentication Using Deep Learning Approaches

Running Title: -Face Recognition Based Website Authentication

Mohamad Amir Dliwati[1*],Dinesh Kumar[2],Chandan Srivastava[3].
[1, 2] Computer Engineering Department, AI & Bigdata, Marwadi University, Rajkot, India.
[3]Data, Machine Learning, and Artificial Intelligence, Rajkot, India.

***Corresponding Author:**Mohamad Amir Dliwati
Computer Engineering Department, AI & Bigdata, Marwadi University, Rajkot, India.
mohamad.dliwati106128@marwadiuniversity.ac.in

Abstract:
When the internet became available to everyone and in every house, a big problem started to reveal for us, "The Information" The Internet gave us access to almost everything, but in return it allowed everyone to reach us as well. With the development of applications and projects that run and work on the Internet, hackers developed their tools to break through privacy and reach our data to steal bank accounts, credit card numbers, and all Personal data available on our computers. As we know, access to the Internet was not available to everyone, as it was restricted to a certain segment of users, such as governments, companies, andcommercial and industrial activities. Later, the Internet changed the way people communicate with each other, the way we explore the world, and the way we organize and run our businesses. From this point, governments and companies have begun working on making the internet available to everyone and everywhere. From this point, the importance and security for websites Applications and providing the users for protecting their data and their privacy, but we do not forget that authentication is the first step for protecting and encrypting our data resources. That gives the client comfortable and security when using these websites. This paper will discuss developing a security system that combines face recognition algorithms that are based on deep learning techniques by hyperparameters such as (Adam) for authenticating websites. Therefore, face recognition became the most important technique for identifying hackers. By applying algorithms integration, our research aims to obtain faster, more accurate, and safer results to determine the identity of the user, and whether he is making a security breach or not, and if it is identified as a threat, his image is circulated to the concerned security centers to take the necessary measures.

Key Words: Deep Learning, Face Detection, Classification Algorithms, Website Authentication, Features Extraction.

I. INTRODUCTION

The network and internet have entered most aspects of our life through electronic devices, e-commerce, communication, virtual learning, and government services. When everybody becomes using the Internet, the experts have concerns and the development of security ways for protecting the web applications from hackers. And they have concerns about databases and how to make a way that is difficult for professional hackers to steal users' data. Web and network security have become a concern for researchers and web developers because of the development of hacker tools. Most researchers consider application authentication or account verification the basic step to protect applications. There are many algorithms that have been proposed for verifying users login to their accounts, such as, {CAPTCHA or Zigzag word} it is differentiating user and a robot, security questions, e-mail recovery, mobile number, and guessing images [1]. However, face recognition is one approach that is gaining the trust of almost experts insecurity.

Therefore, in our research and our paper, we suggest a face recognition approach to perform application authentication.

A face recognition approach has a sequence of steps see that in Figure 1.

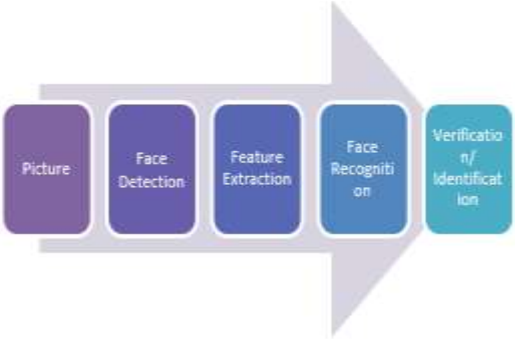


Figure 1 Structure of a public face recognition system.

This paper result toaims best from traditional algorithms [2] and investigates face recognition using Google's famous feature extraction algorithms (InceptionV3) and the use of neural network algorithms for hetclassification of publicly available data sets. The paper is organized as follows: the second section includes background information about our data set, the third section explains the architecture of neural networks (Activation functions, Optimization) and deep learning (Hyperparameters), and the results and discussion are presented in the fourth section and finally, in the fifth section, some conclusions are drawn.

II. Face Detection

Computer vision systems for conventional image data are not suitable because they include many elements.In this case, face detection becomes mandatory, and therefore an automatic face tracking system is required to develop, for example:

- FacesCovering: Among the most important examples of covered faces (glasses - beard - hands)
- Features Coverage: The presence of items such as birds, glass, or hats.
- Face features: Facial features differ greatly due to different gestures, circumstances, and photography.

Face detection is largely depending on identifying the geometric structure of the object as shown in Figure 2. Some approaches for face detection:

1. **Color images:**

It focuses on the three-color spaces. Which are RGM, YCbCr, and HST. They make a comparison between these three famous skin color detection algorithms and come up with a new algorithm depending on "skin color classification" and show their results. After that, they present an explanation of this three-color space [9].

2. **Images in motion:**

Real-time video enables detection the of faces [10].

III.Feature Extraction

Most people can recognize faces from the age of four years, so the process seems very easy.However, this topic is extremely complex as a human can distinguish people who are known to them even when their faces are in glasses, hats, or beards.This process sounds trivial but it poses a huge challenge for computers. Table 1 shows some of the feature extraction methods to detect faces. PCA is a famous algorithm see figure 2 applied to face detection [11].

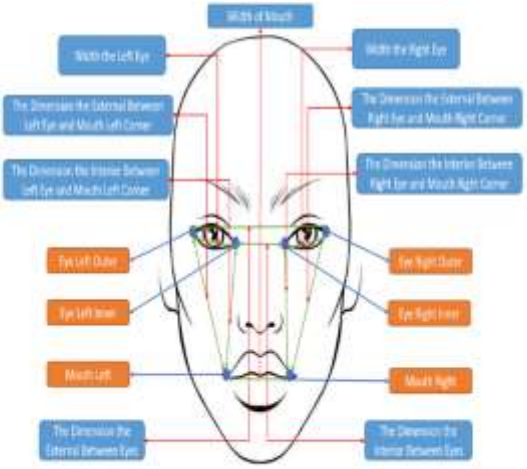

Width of Mouth
Width the Left Eye
Width the Right Eye
The Dimension the External Between Left Eye and Mouth Left Corner
The Dimension the External Between Right Eye and Mouth Right Corner
The Dimension the Interior Between Left Eye and Mouth Left Corner
The Dimension the Interior Between Right Eye and Mouth Right Corner
Eye Left Outer
Eye Right Outer
Eye Left Inner
Eye Right Inner
Mouth Left
Mouth Right
The Dimension the External Between Eyes
The Dimension the Interior Between Eyes

Figure 2 Feature Extraction

IV. Face recognition algorithms

1. Principal Component Analysis:

It is the method used to analyze data. Restore the original data to the original data set, as well, and are used to reduce data for normal computation [12].

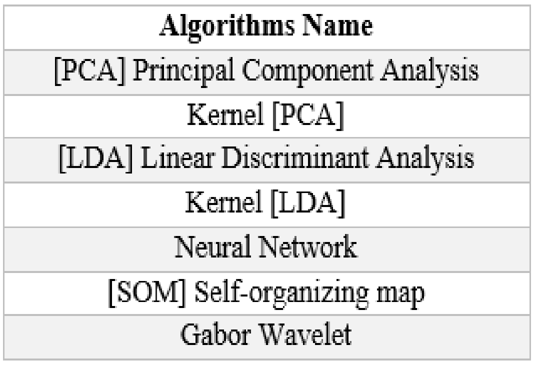
2. Support Vector Machines:

SVM is a learning algorithm and it is supervised learning, it is used in classification problems for its effectiveness and for having an excellent basis in data. It is of two types binary classification which categorizes only two groups and multi-class classification which classifies more than one group [13].

3. Logistic Regression:

This algorithm transforms the output using the sigmoid function to the Probability values, which will be categorized into one of the classes within this algorithm [14].

See table 1 for famous algorithms for face recognition.



Algorithms Name
[PCA] Principal Component Analysis
Kernel [PCA]
[LDA] Linear Discriminant Analysis
Kernel [LDA]
Neural Network
[SOM] Self-organizing map
Gabor Wavelet

Table 1 Face Recognition Algorithms

V. Dataset

We have used 30% of the data for testing and 70% for learning. The dataset contains (13,700) pictures of (1410) persons (users' faces), that are collected from internet resources such as https://www.kaggle.com/and many other resources. We have used 30% of the data for testing and 70% for learning.We merged several datasets together and obtained this dataset. We chose this dataset because the image resolution is good and varied.

In this dataset, we have pictures of faces from different countries and different skin colors and we have added several pictures of people with or without a beard and people with or without glasses.

After that we train our data of images on inceptionV3 for face detection and feature extraction finally, we got vectors for every user to save our results in a database and save models on our website.

The training takes a lot of time the chart 1 explains how much time we needed when we trained the data.

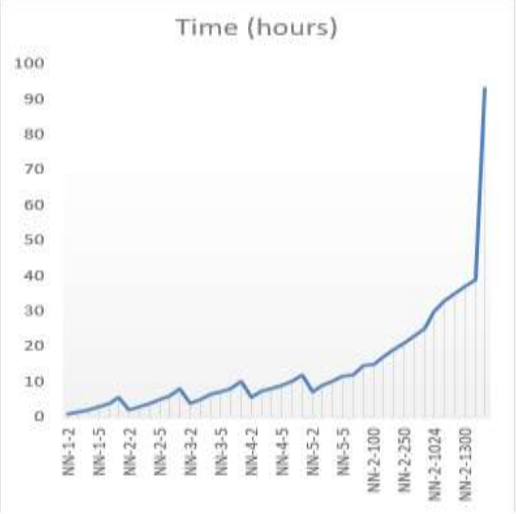


Chart 1 Time for Training Dataset.

VI. Neural Networks & Deep Learning

1. Neural Network:

This term is similar to the traditional education carried out by humans, for example, when we teach the child how to differentiate between living and inanimate objects, after a lot of training, practice, and provision of instructions, ~~he~~ will learn to differentiate between them by observing the properties that characterize the organism such as breathing and nutrition, and so the same applies to Learning the machine after providing it with a set of data and training it where after practice it will be able to make decisions on its own [3].

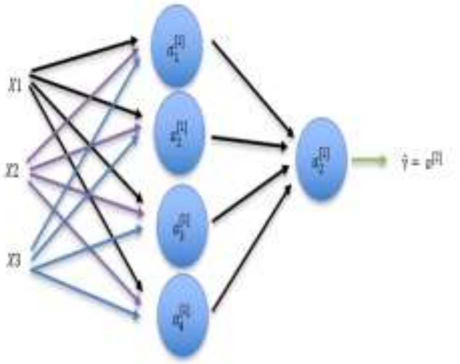


Figure 3 Neural Network Architecture.

So, the stages that the machine learning stage goes through are training, hen testing, or decision-making.

$$Z_1^{[1]} = w_1^{[1]} \intercal\, x + b_1^{[1]} a_1^{[1]} = \sigma\ (Z_1^{[1]})$$

2. Activation Functions:

In this paper, we will talk about the activation function. The idea of the activation function in the deep learning model is that it processes the output of the neuron or the node, depending on what you like to call it, whether it is a group of neurons and nodes or a single one of them, which is a mini-simulation for biological neurons, and between each layer and the other, we use the activation function so that we process the outputs coming out of the layer first. Have you ever asked yourself why the ReLu activation function takes a zero if less than zero, why for example, don't you follow a zero if less than 0.01 or follow? Zero if less than 0.01- and if you do not know what the ReLu function is at all, it is an activation function that is used in regression tasks so that the output is always higher than zero by it zeroing the output if it is less than zero and even if it is higher than zero it will return it as it is because the regression is not effective, for example, the money is negative and so on. Yes, you do not need the custom activation function in many cases, but you must learn how to deal with any case that you can meet, let us talk about the types that exist first. We have a large variety of activations are supported by Keras, TensorFlow, for example: (Sigmoid, Tanh, ReLu, leaky ReLu, Maxout) [4] see Table 1.

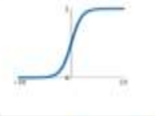
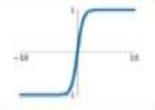
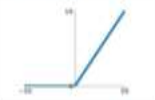
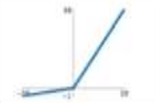
Activation Functions	Equation	Chart
Sigmoid	$\sigma(x) = \frac{1}{1+e^{-x}}$	
Tanh	$tanh(x)$	
ReLu	$max(0, x)$	
leaky ReLu	$max(0.1x, x)$	
Maxout	$max(w_1^T x + b_1, w_2^T + b_2)$	

Table 2 Activation Functions

3. Deep Learning:

Deep learning or DL is one of the techniques or branches of machine learning, but at this stage, complex equations are calculated and the best example of this is the game of chess where when you teach a machine how each piece moves, it is called machine learning, but when the machine calculates all the movements the potential and all the options available before moving the piece is exactly what is called deep learning [5] [6] [7].

A CNN is composed of several kinds of layers:

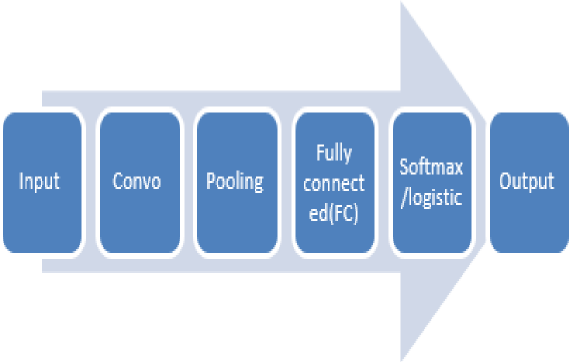


Figure 4 CNN Algorithm Architecture.

4. Optimization:

They are algorithms to speed up the learning process in neural networks(Momentum and RMSProp). Here are the updated equations But, in our research, these algorithms do not help us Because the learning speed is slow, so we used an algorithm ADAM [8] Because the learning speed is fast.

$$v_t = \beta_1 * v_{t-1} - (1 - \beta_1) * g_t$$
$$s_t = \beta_1 * s_{t-1} - (1 - \beta_2) * g_t^2$$
$$\Delta w_t = -\eta \frac{v_t}{\sqrt{s_t + \epsilon}} * g_t$$
$$w_t + 1 = w_t + \Delta w_t$$

VII. Results and Discussion

1. One Hidden Layer:

We are applying one hidden layer and (2) neurons to (7) neurons and finally, we got these results here we are testing what results we will get by using a hidden layer in classification with multiple neurons.
The best accuracy was one hidden layer and (7) neurons.

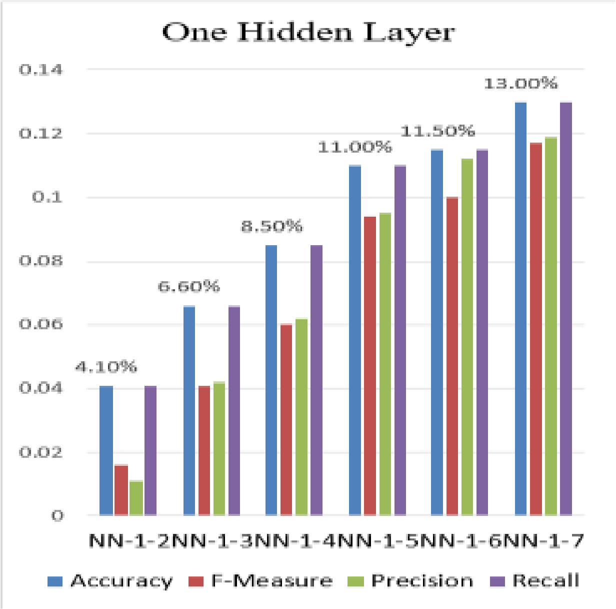


Chart 2 Training Result (one hidden layer).

2. Tow Hidden Layers:

We are applying two hidden layers and (2) neurons to (7) neurons and finally, we got these results.
The best accuracy was two hidden layers and (7) neurons here we are testing what results from we will get by using two hidden layers in the classification with several neurons because one layer did not give us good results.

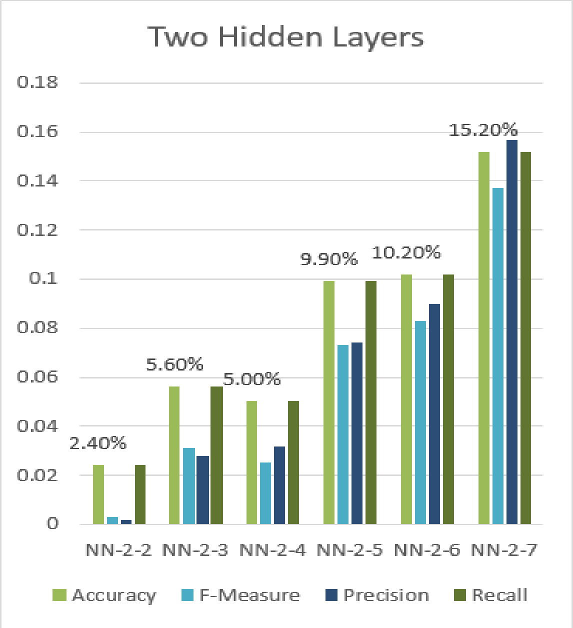


Chart 3 Training Result (tow hidden layers).

3. Three Hidden Layers:

We are applying three hidden layers and (2) neurons to (7) neurons and finally, we got these results.

The best accuracy was three hidden layers and (7) neuronshere we are testing what results from we will get using three hidden layers in the classification with several neurons because the two layers did not give us good results

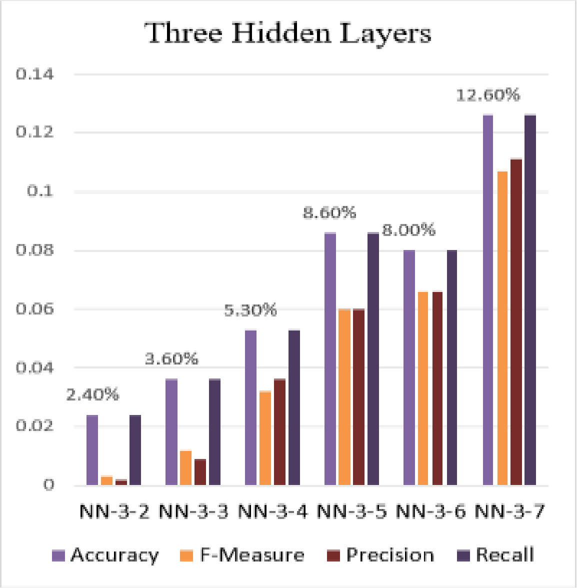


Chart 3 Training Result (three hidden layers).

4. Four Hidden Layers:

We are applying four hidden layers and (2) neurons to (7) neurons and finally, we got these results.

The best accuracy was four hidden layers and (6) neurons here we are testing what results we will get using four hidden layers in the classification with several neurons because three layers did not give us good results.

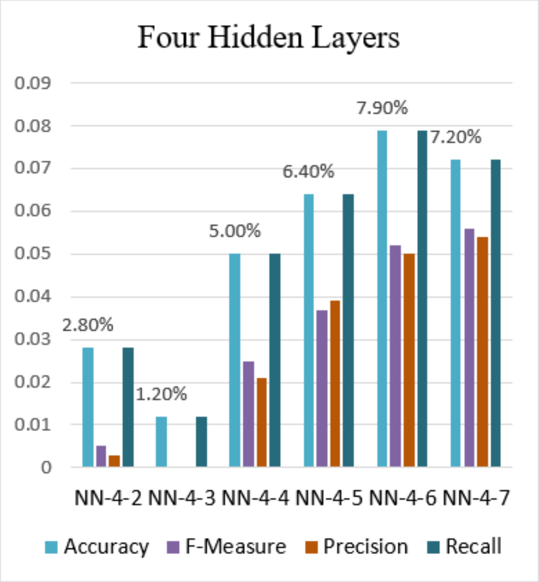


Chart 4 Training Result (four hidden layers).

5. **Five Hidden Layers:**

We are applying five hidden layers and (2) neurons to (7) neurons and finally, we got these results.

The best accuracy was five hidden layers and (7) neurons here we are testing what results from we will get using five hidden layers in the classification with several neurons because four layers did not give us good results.

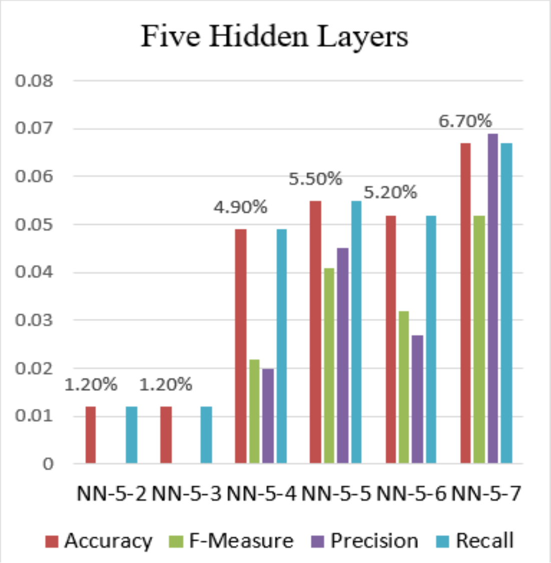


Chart 5 Training Result (five hidden layers).

After comparing the results, we found the best accuracy was two hidden layers and (7) neurons.

In the next step, we will increase the number of neurons for getting a new result best from the previous.

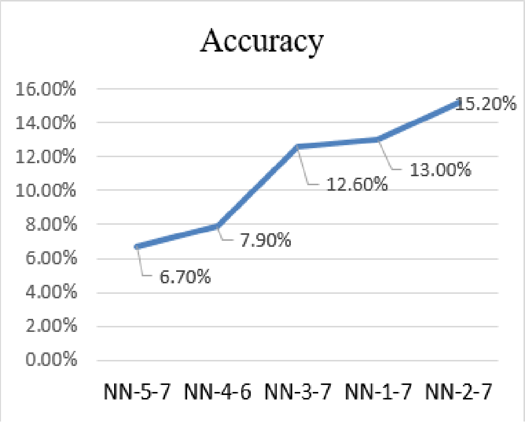


Chart 6 Training Result (Accuracy).

6. **Neurons (100-350):**

We are applying two hidden layers and (100) neurons to (350) neurons and finally, we got this result.

After trying the number of hidden layers, we concluded that the best option is two layers, and then we tried the number of neurons.

The best accuracy was two hidden layers and (350) neurons.

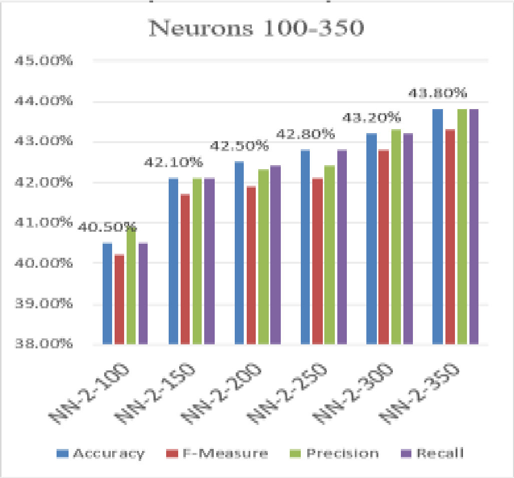


Chart 7 Training Result (Neurons 100-350).

7. **Neurons (1024-1400):**

We are applying two hidden layers and (1024) neurons to (1400) neurons and finally, we got these results.

After trying the number of hidden layers, we concluded that the best option is two layers, and then we tried the number of neurons.

The best accuracy was two hidden layers and (1300) neurons.

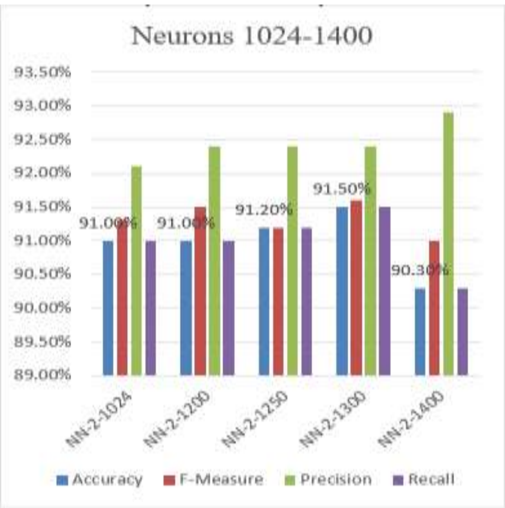


Chart 8 Training Result (Neurons 1024-1400).

After trying the number of hidden layers, we concluded that the best option is two layers, and then we tried the number of neurons.
The best accuracy was two hidden layers and (1300) neurons.

VIII. CONCLUSIONS

After the tests that were done on the neural networks, we got the previous results. These results helped us to discover the best network structure, as the number of appropriate hidden layers and the number of neurons were discovered, as shown in Chart 9, where this structure will help us in the learning process faster, as shown in Chart1.
And we suggest continuing the research with unsolved problems in this research, for example (half faces and masks that are placed on the face).

IX. Reference:

1. Dliwati, M. A., & Almustafa, M. (2018). Integrating face recognition algorithms with typing speed for website authentication. Journal of Theoretical & Applied Information Technology, 96(13).
2. Dliwati, M. A., & Kumar, D. (2021, August). Face Recognition in the Context of Website Authentication. In 2021 Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-5). IEEE.
3. Lawrence, S., Giles, C. L., Tsoi, A. C., & Back, A. D. (1997). Face recognition: A convolutional neural-network approach. IEEE transactions on neural networks, 8(1), 98-113.
4. Agostinelli, F., Hoffman, M., Sadowski, P., & Baldi, P. (2014). Learning activation functions to improve deep neural networks. arXiv preprint arXiv:1412.6830.
5. Pouyanfar, S., Sadiq, S., Yan, Y., Tian, H., Tao, Y., Reyes, M. P., ... & Iyengar, S. S. (2018). A survey on deep learning: Algorithms, techniques, and applications. ACM Computing Surveys (CSUR), 51(5), 1-36.
6. Coşkun, M., Uçar, A., Yildirim, Ö., & Demir, Y. (2017, November). Face recognition based on convolutional neural network. In 2017 International Conference on Modern Electrical and Energy Systems (MEES) (pp. 376-379). IEEE.
7. Li, H., Lin, Z., Shen, X., Brandt, J., & Hua, G. (2015). A convolutional neural network cascade for face detection. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 5325-5334).
8. Reddi, S. J., Kale, S., & Kumar, S. (2019). On the convergence of adam and beyond. arXiv preprint arXiv:1904.09237.
9. Singh, Sanjay Kr.; Chauhan, D. S.; Vatsa, Mayank ; Singh, Richa"A Robust Skin Color Based Face Detection Algorithm," Tamkang Journal of Science and Engineering, vol. 6, no. 4, pp. 227-234, 2003.
10. M. C. Nechyba, L. Brandy, and H. Schneiderman."Lecture Notes in Computer Science.," Springer Berlin Heidelberg, pp. 126-137, 2009.
11. K. Pearson, "LIII. On lines and planes of closest fit to systems of points in space.," The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, vol. pp. 2(11), pp. 559-572, 1901.
12. Lu, Juwei ; Plataniotis, K. N. ; Venetsanopoulos, A. N. ; Z. Li, Stan, "Ensemble-Based Discriminant Learning With Boosting for Face Recognition," IEEE Transactions on Neural Networks, vol. 17, no. 1, pp. 166-178, 2006.
13. Inukollu, V. N., Arsi, S., & Ravuri, S. R. "Security issues associated with big data in cloud computing," International Journal of Network Security & Its Applications, p. 45, 2014.

14. Zhou, C., Wang, L., Zhang, Q., & Wei, X."Face recognition based on PCA and logistic regression analysis," Optik, Vols. 125(20),, pp. 5916-5919, 2014.

Mohamad Amir Dliwati Computer Engineering Department, AI & Bigdata Marwadi University Rajkot, India. mohamad.dliwati106128@marwadiuni versity.ac.in

Dinesh Kumar Computer Engineering Department, AI & Bigdata.
Marwadi University Rajkot, India dinesh.kumar@marwadieducatin.edu. in

Chandan Srivastava Data and Artificial Intelligence, Microsoft, Hyderabad, India chandan.iitk@gmail.com