Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

AN EXPERIMENTAL INVESTIGATION ON DIFFERENT EPOCHS AND SPLITTING DATA RATIOS FOR STUDENT AUTHENTICATION SYSTEM USING CONVOLUTIONAL NEURAL NETWORK (CNN) BASED FACE RECOGNITION

Shaiful Bakhtiar Rodzman[1*], Norafaf Afifah Hanazilah[2], Rajeswari Raju[3], Khairunnisa Abdul Kadir[4], Mohd Azim Zainal[5], Siti 'Aisyah Sa'dan[6]

[1,4,5] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA (UiTM) Pahang Branch, Raub Campus
Email: shaifulbakhtiarrodzman@uitm.edu.my, khairunnisa.kadir@uitm.edu.my, azim90@uitm.edu.my
[1] Multidisciplinary Information Retrieval (MuDIR), Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia
Email: shaifulbakhtiarrodzman@uitm.edu.my
[2,3] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA (UiTM) Terengganu Branch, Kuala Terengganu Campus
Email: norafaf24@gmail.com, rajes332@uitm.edu.my
[6] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Negeri Sembilan Kampus Seremban
Email: sitiaisyah@uitm.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 14.01.2025
Revised date: 23.01.2025
Accepted date: 27.02.2025
Published date: 20.03.2025

To cite this document:

Rodzman, S. B., Hanazilah, N. A., Raju, R., Abdul Kadir, K., Zainal, M. A., & Sa'dan, S. A. (2025). An Experimental Investigation On Different Epochs And Splitting Data Ratios For Student Authentication System Using Convolutional Neural Network (CNN) Based Face

Abstract:

In today's interconnected world, traditional username and password-based authentication methods are insufficient to safeguard sensitive data. This challenge is noticeable in Malaysian academic institutions, where these methods face vulnerabilities such as security breaches, forgotten passwords, and low user satisfaction. Weak passwords, reuse, and fake credentials further expose users to cyberattacks, highlighting the need for improved security and user experience. Face recognition using Convolutional Neural Networks (CNN) offers a promising solution, combining enhanced security with user-friendly identity verification. This study evaluates the performance of CNN based face recognition for improving authentication systems in Malaysian educational institutions. Experiments demonstrated the effectiveness of Student Authentication System Using CNN Based Face Recognition, achieving a maximum Average Recognition Accuracy of 100% and a minimum of 83% using varying epochs and data-splitting ratios. In conclusion, this approach has the potential to enhance security, usability, student experience, staff productivity, and institutional reputation.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

Recognition. *Journal of Information System and Technology Management, 10* (38), 147-161.

DOI: 10.35631/JISTM.1038010

Keywords:

Face Recognition, Deep Learning, Convolutional Neural Network (CNN), Artificial Intelligence

Introduction

Nowadays in digital world, traditional username and password-based authentication methods are no longer sufficient to protect personal information and sensitive data (Miller, 2023). This particularly concerns academic institutions in Malaysia, where data security and user experience challenges exist. Authentication systems have an important role in securing user identities and information, from unlocking their devices to accessing sensitive data (Thosar & Singh, 2018). The most secure authentication systems use a combination of two or more factors to prevent unauthorized access, such as passwords, PINs, biometric data, or tokens (Varshini, 2022). For instance, multi-factor authentication combines a one-time code, a biometric scan and a password, whereas two-factor authentication requires users to enter a password and a one-time code from a mobile app (Rosencrance et al., 2023).

Traditional authentication methods, such as username and password-based systems, are susceptible to security breaches and may not provide the optimal user experience (Rittenhouse & Chaudhry, 2016). Passwords can be forgotten, guessed, or stolen, and their importance is decreasing as more advanced cyber threats arise (Mathew et al., 2016). Moreover, the registration process, which involves the creation of user accounts and storage of vital information such as usernames, email addresses, and passwords, can be vulnerable to attacks (E-Envoy, 2002). Therefore, there is a need to explore alternative authentication methods that can provide better security and user experience.

One such alternative is AI-based authentication, which uses machine learning to learn and adapt over time (Townsend, 2023). AI-based authentication systems can verify a user's identity based on unique factors, such as facial features, and can become more accurate and secure as they are used (Nikolova, 2023). Convolutional Neural Network (CNN) Based Face Recognition systems are highly accurate, achieving recognition rates of over 99% (Saragih & To, 2022). Artificial Neural Networks (ANN), or CNNs, are very good at tasks involving image processing and recognition (Sarvakar et al., 2023).

The purpose of this study is to research on the viability and efficacy of using CNN-based facial recognition technology in Malaysian academic institutions as an alternative to conventional username and password-based authentication techniques.

Related Work

Facial recognition is a popular biometric method for identifying individuals, providing a convenient, non-invasive method for security, surveillance, access control, and identity verification. Deep learning technologies have significantly accelerated facial recognition progress, leading to highly precise and reliable systems. However, the effectiveness and dependability of facial recognition systems can be impacted by changes in illumination,

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010
posture, facial expressions, and occlusion, which persists despite these developments. Furthermore, in order to safeguard personal information and stop unwanted access, more reliable and secure solutions must be developed in response to growing privacy and security concerns.

Authentication System

Authentication refers to the process of confirming an individual's identity, device, or system to ensure that only authorized entities have access to a particular resource, system, or data. It entails verifying the credentials presented by an individual or entity to ensure they are who they claim to be, thereby preventing unauthorized access, data breaches, and other security threats (Farik et al., 2016). For instance, Ercan and Özbek (2021) developed a face authentication system using landmark detection, achieving 89.79% accuracy. Additionally, Labayen et al. (2021) combined recognition and monitoring technologies for student authentication and proctoring, utilizing AI algorithms such as face and voice detection, and computer lockdown technologies. These studies demonstrate the ongoing efforts to develop robust and accurate authentication systems for various applications.

Face Recognition

Face recognition is a biometric technique that automatically recognizes and verifies individuals based on their distinctive facial traits. The process starts with the user acknowledging a sense of familiarity and trying to recollect specifics from previous encounters (Said & Nasr, 2020). This technology uses sophisticated algorithms to analyze facial features, such as feature extraction, face detection, and matching. These particular algorithms identify faces, extract distinctive features like nose shape, jawline length, and eye distances, and compare them to a database of previously stored facial templates. Face recognition is an advanced kind of pattern recognition and computer vision, whereby matching algorithms compare the presented face to others in the system to assess how similar they are. This allows for identification or verification.

This technology is being utilized to enhance various aspects of our lives, including attendance management and security systems. Recent studies have proposed innovative solutions, such as a web-based attendance authentication system that combines facial recognition with blockchain technology, achieving a 98% accuracy rate (Azli et al., 2023). Another study developed a face recognition security system that effectively detects intruders and reduces human error in access control, achieving 98% accuracy in detection and 90% in recognition (Owayjan et al., 2020). Furthermore, a facial recognition-based student attendance system was suggested, which minimizes errors and eliminates manual labor by using the Haar Cascade Algorithm to identify student faces and accurately register attendance (Agarwal et al., 2021). These developments show how facial recognition technology has the power to completely transform a range of sectors and uses.

Deep Learning

Face recognition has greatly improved thanks to CNN, allowing contemporary models to outperform humans. (O'Toole & Castillo, 2021). By teaching artificial neural networks to identify patterns in massive datasets, a process known as deep learning, face recognition accuracy and reliability can be significantly increased. The automatic extraction of hierarchical features from facial photos is made possible by deep learning (Cao et al., 2018). As it learns and gets better over time, the network makes advantage of data augmentation techniques to increase the generalization and robustness of its models (Goodfellow et al., 2016). Deep neural

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010
networks enable face recognition systems to efficiently process complex visual data, enabling them to automatically learn and extract high-level properties from facial images (O'Toole & Castillo, 2021).

Methodology

Deep neural networks, or CNNs, are used to handle grid data, such as pictures and videos, mainly for tasks like pattern detection, object categorization, and image recognition.

According to Upreti (2022), An input, hidden, and output layer make up a CNN, as shown in Figure 1.

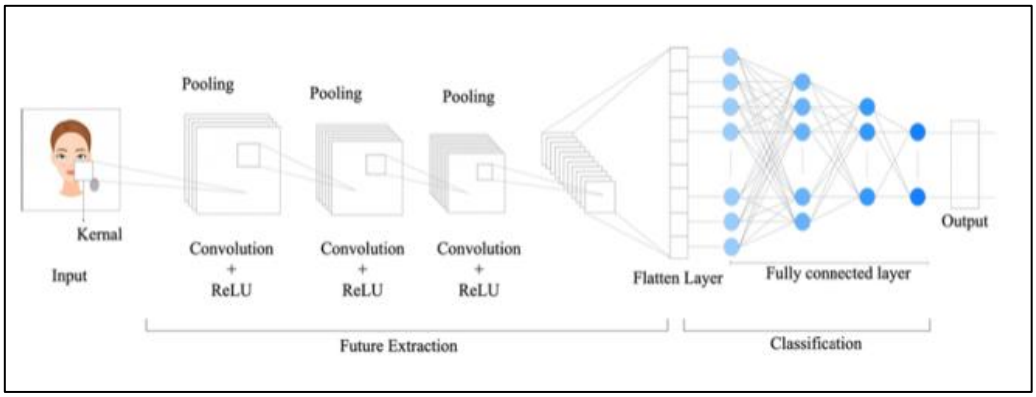

Figure 1: The architecture of Convolutional Neural Network (CNN)

Furthermore, the input layer in a CNN receives raw data, which is then processed through layers to create hierarchical representations. Each layer has a unique function, enhancing the network's ability to identify patterns and spatial relationships. After that, the data is sent through hidden layers such activation functions, pooling layers, and convolutional layers. Convolutional layers complicate the input data, but activation functions add non-linearities and improve the model's ability to identify intricate relationships. Pooling layers down-sample feature maps, reducing computational effort Upreti (2022).

Convolutional Layer

The convolutional layer serves as a foundational element within a CNN, characterized by the presence of multiple filters or kernels. These filters, essentially matrices undergo convolution with the input image, facilitated by a receptive field that establishes localized connectivity. The filter values dynamically adjust during the learning process. The convolution operation involves applying an activation function to each calculation, with output dimensions determined by depth, stride, and zero paddings. Figure 2 illustrates the process, showing how filters interact with an input image.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

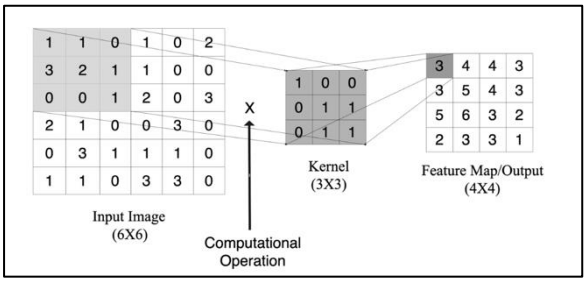

Figure 2: Process Of Convolution Operation

Pooling Layer

The convolutional layer's feature map input dimensions are decreased by the pooling layer, which comes after it. This reduction is achieved through max-pooling or average pooling, extracting maximum or average values from different sections of the feature map.

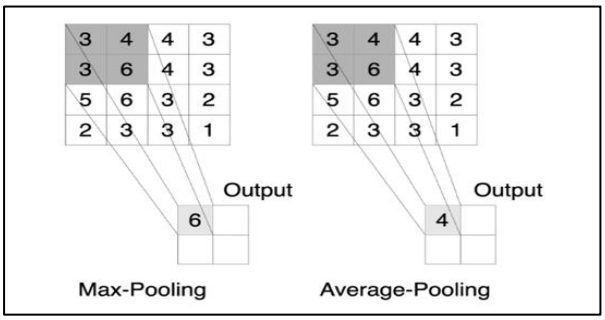

Figure 3: Pooling Layer Operation

Fully Connected Layer

A key element of neural network architectures is the fully connected layer, which guarantees information consolidation across the network. It connects each node to all feature map nodes from the last pooling layer on CNN as illustrated in Figure 4.

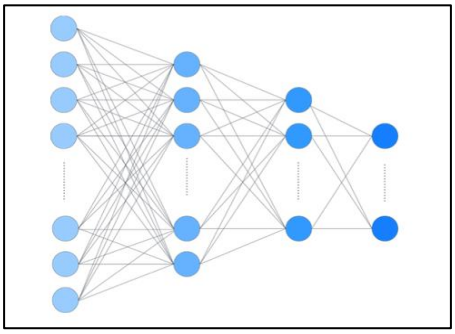

Figure 4: Fully Connected Layer

A CNN's fully connected layer creates a comprehensive neural network structure by connecting each neuron in its layer to those in the convolutional and pooling layers that came before it.

This layer uses the outcomes from these layers to categorize input images into different classes based on patterns learned from the training dataset. The output layer, which produces outputs based on the specific objective, is configured to produce four outputs. A softmax function,

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

which converts characteristics from the previous layer into probability values for various classes, creates the connection between the fully connected layer and the output layer.

System Architecture

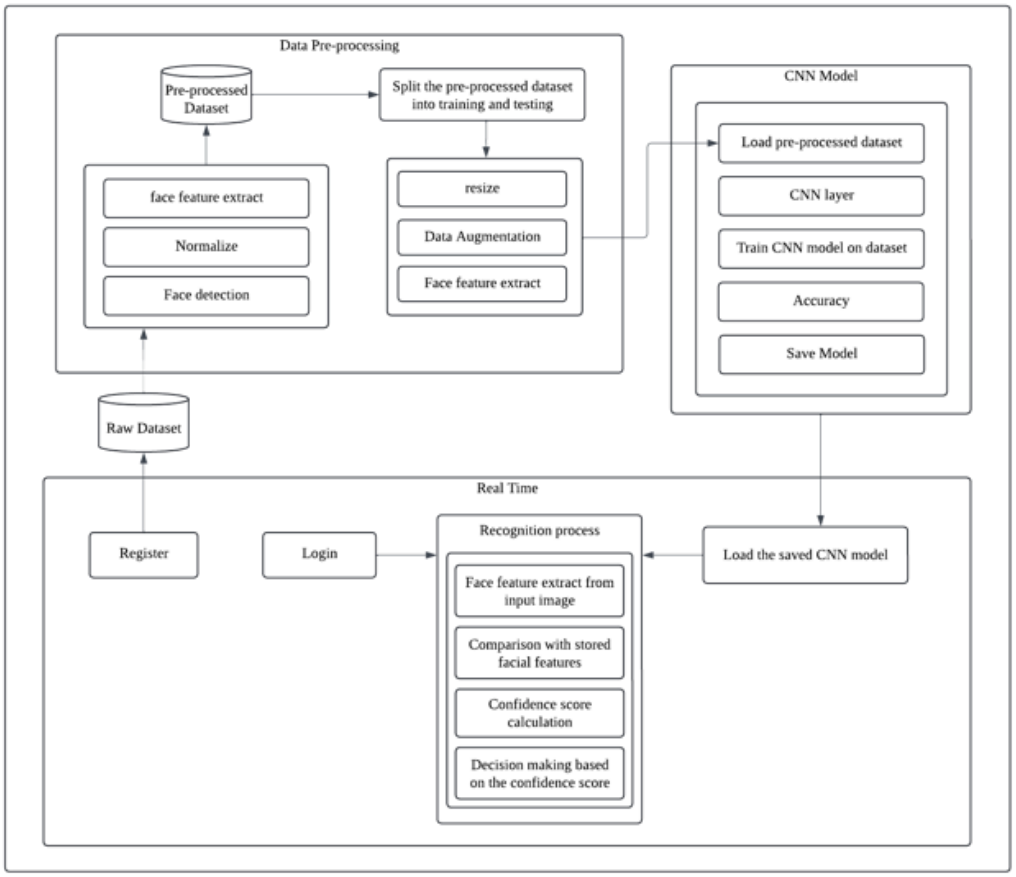

Figure 5: System Architecture

As in Figure 5, the student authentication system uses a CNN model to provide secure and efficient access control. It consists of two core functionalities: registration and login. During registration, users provide information and facial images, which undergo pre-processing for face detection, alignment, normalization, and feature extraction. The trained CNN model then analyses these features to predict an individual's identity, and if it surpasses a set threshold, the student is granted access.

The CNN model is a multi-layered sequence network, and each layer helps it learn and identify facial features with high accuracy. In order to extract and take into account spatial information, it begins with a Conv2D layer with 32 filters and moves on to a MaxPooling2D layer with 64 filters. The model transitions to fully connected layers, including a Flatten layer, Dense layer, ReLU activation function, and Dropout layer to prevent overfitting. Compiled with the Adam optimizer, an iterative optimization technique for neural network training that minimizes the loss function. For multi-class classification issues, the model is trained using a categorical cross-entropy loss function, which assesses the difference between the actual class distribution and the projected probability distribution. It assists a CNN model in assessing the gap between

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010
its predictions and the true labels, thereby facilitating improved accuracy in its predictive capabilities.

The system also integrates with a user interface and secure database for student information and authentication logs, prioritizing real-time processing and scalability for a growing student population.

Registration Process

During the registration process, the system guides the user through a series of steps to capture and store their facial images for authentication purposes. The registration process is as follows:

i. The user enters their 10-digit student ID into the provided input box
ii. The system validates the ID format to ensure it adheres to the specified criteria
iii. The system utilizes the webcam to detect and capture images of the user's face at predetermined intervals
iv. The captured facial photos are stored in the dataset with filenames indicating the capture sequence within a directory designated by the user's student ID
v. To increase the facial recognition model's accuracy, the training set's saved image will undergo pre-processing.

Login Process

The login process is initiated when a registered user presents their face to the webcam, allowing the system to verify their identity and grant access. The login process is as follows:

i. The registered user presents their face to the webcam.
ii. The system captures a single frame from the live webcam feed.
iii. The system leverages an OpenCV detector to detect any present faces within the captured frame.
iv. For each detected face, the system extracts facial features using the trained CNN model
v. The extracted features are compared against a database of known face encodings established during the registration process.
vi. If a match is found within a predefined threshold, the system signifies a sufficient degree of similarity between the captured facial features and a known user's encoding
vii. The system grants access and redirects the user to the homepage associated with the matching facial features.
viii. If no match is found within the threshold, the login attempt is deemed unsuccessful, and the user remains on the login page.

Dataset

The dataset used in this research was collected by capturing facial images of students from Universiti Teknologi MARA (UiTM) Kuala Terengganu, both male and female. The facial images were taken in a frontal view with a neutral expression, open eyes, and relaxed lips to minimize the possibility of spoofing attempts through expressions that alter the face geometry. The images were captured in JPEG format with 200 x 200 pixels resolution for a good balance between accuracy and efficiency. The dataset was collected through an interactive web application that employs a live video feed to take multiple snapshots of the registrant's face.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

Each registered student is assigned a unique directory within the dataset, containing a series of images captured during the registration process.

To guarantee data consistency and enhance model performance, the Convolutional Neural Network (CNN) model's training dataset underwent a number of pre-processing procedures. Images were resized to 200x200 pixels, normalized using pixel values, and face detection and cropping were performed using OpenCV's 'detectMultiScale' function. In order to improve variability and avoid overfitting—a machine learning behavior in which the model makes correct predictions for training data but not for new data—data augmentation was also used.

Random transformations like rotation, width and height shifting, trim, zoom, and flipping were applied using the Image Data Generator from Keras class in Python Data augmentation was also employed to increase variability and prevent overfitting, a machine learning tendency in which the model predicts training data correctly but not fresh data. These 450 sets of images are used for entire experiments.

Equations

System testing involves evaluating the functionality and performance of a prototype under various conditions. This is separated into prototype testing and system training. Using a pertinent dataset of facial photos, system training aims to improve the CNN model's face recognition capabilities. The percentage of successfully detected faces among all faces submitted for authentication is known as accuracy.. It is calculated as the ratio of correct identifications using classifiers (TP, FP, FN, TN) to the total number of identification attempts. The average recognition accuracy is calculated using a using the following formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Model Training And Evaluation Protocol

The CNN model was evaluated by dividing the dataset into training and testing subsets, with 80% allocated to the training and 20% to the testing subsets. The model is designed to extract features from facial images and classify them into student IDs. It consists of multiple convolutional and pooling layers, followed by fully connected layers. Convolutional layers extract features, while pooling layers reduce spatial dimensions to retain important ones. Fully connected layers use these features to make predictions about student IDs.

The model was trained using an augmented training dataset, Adam optimizer, and categorical cross-entropy loss function. To prevent overfitting, TensorBoard, an TensorFlow's Class open-source visualization toolkit in Python and EarlyStopping callbacks, a regularization technique that halts a neural network's training process before it reaches the maximum number of epochs or iterations, were defined. The model was trained for 50 epochs with a 32-batch batch size. Performance metrics like accuracy, precision, recall, F1-score, and loss were used to evaluate the model's performance. Accuracy measures the proportion of correctly classified instances, while precision, recall, and F1-score provide a more detailed understanding using the following formulas:

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F1 - Score = 2\,x\,\frac{Precision * Recall}{Precision + Recall} \quad (4)$$

The model's accuracy in predicting student IDs was evaluated on both training and validation datasets. The loss and accuracy metrics were computed, along with the confusion matrix, which outlines true positives, false positives, false negatives, and true negatives. This comprehensive evaluation protocol ensures the model's performance is thoroughly assessed and validated, providing a clear indication of its performance.

Results

Two experiments were conducted to evaluate the performance of the CNN Based Face Recognition System. Experiment 1 focused on the impact of training epochs on the model's accuracy. The number of epochs changed between 50 epochs and 100 epochs. Meanwhile, experiment 2 was conducted by training the data with different splitting number of data ratios. The data ratios were split by 80:20 and 90:10 with same numbers of data set. For the training result, the performance of the system was measured by the accuracy of the model

Experiment 1

For experiment 1, different number of epochs was used for training the model. The epochs changed to 50 epochs and 100 epochs. The data splitting was fixed with 80:20 ratios. The choice of 50 and 100 epochs for the experiment was based on the preliminary analysis of the data and a review of similar studies in the field. The number of epochs is hyperparameter that requires tuning, and there is no one-size-fits-all answer. However, increasing the number of epochs can result in improved model performance, as shown in Table 1.

Number of epochs: 50

The first experiment applied 50 epochs to a total of 390 training dataset face images. An early stopping callback function was used to avoid overfitting, and the epochs stopped at 32. The results achieved an accuracy of 94% for training and 83% for testing, with a validation loss of less than 3.0. Overall, the model's accuracy achieved for 50 epochs was 94%.

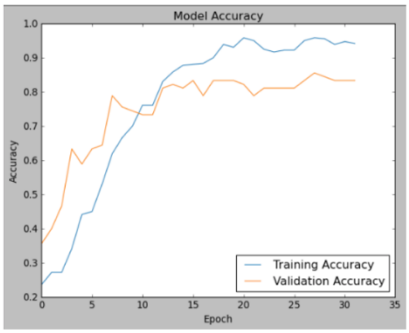

Figure 6: Accuracy Graph For Training And Validation

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

The plotted graph of the training and validation accuracy across 50 epochs is displayed in Figure 6. On the last epochs, the training accuracy began to rise from 0.2 to 0.9. On the last epochs of 32, the graph for validation accuracy began to rise from 0.3 to 0.8.

Figure 7: Training And Validation Loss Graph

In the meantime, the training loss and validation loss plotting graphs are displayed in Figure 7. On the last epochs, the training loss began to drop from 4.0 to 2.5. On the last 32 epochs, the validation loss began to drop from 4.7 to 3.0.

Number of epochs: 100

Next, 100 epochs were used for the model on a total of 360 training dataset and 90 testing dataset of face images. An early stopping callback function was applied to the model, where the epochs stopped at 52. According to the results, the model's validation loss was less than 0.6 and its training and testing accuracy was 89% and 92%, respectively. Over the course of 100 epochs, the model's overall accuracy was 94%.

Figure 8: Accuracy Graph For Training And Validation

The plotted graph of the training and validation accuracy across 100 epochs is displayed in Figure 8. On the last epochs, the training accuracy began to rise from 0.13 to 0.89. Regarding validation accuracy, on the last epochs of 52, the graph began to rise from 0.35 to 0.92.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

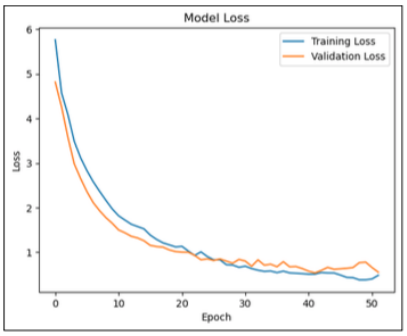

Figure 9: Training And Validation Loss Graph

In the meantime, the training loss and validation loss plotting graphs are displayed in Figure 9. On the last epochs, the training loss began to drop from 5.76 to 0.48. On the last epochs of 52, the validation loss began to drop from 4.81 to 0.55.

Experiment 2

Data Splitting by 80:20

During training, the data was split to 80:20, where a total of 360 images were used for training and 90 images were used for testing. The results show that the accuracy obtained was above 90% for both training and testing, with a validation loss of less than a certain value 0.4. Figure 10 shows the plotting graph of the training loss and the validation loss. The training loss started to decrease from 5.4 to nearly 0.34 on the 50 epochs. As for validation loss, the graph started to decrease from 4.7 until the final loss was 0.4.

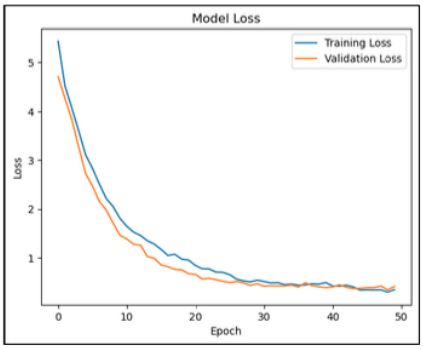

Figure 10: Training And Validation Loss Graph

Figure 11 shows the graph of training and the validation accuracy obtained from splitting data into 80:20. From epoch 1 until the final epoch, the training accuracy and validation accuracy both started to increase. However, the validation accuracy started to become unstable from epoch 10 to epoch 15, then it started to increase steadily again and achieved accuracy of more than 90%.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

Figure 11: Accuracy Graph For Training And Validation

Data Splitting by 90:10

The dataset was divided into 90:10 segments for this experiment. A total of 405 student face photos, or 90% of the data, were utilized for training, and 45 images, or 10% of the data, were used for testing. With a final validation loss of 0.2888, the model's accuracy for both training and validation was 95%, according to the results.

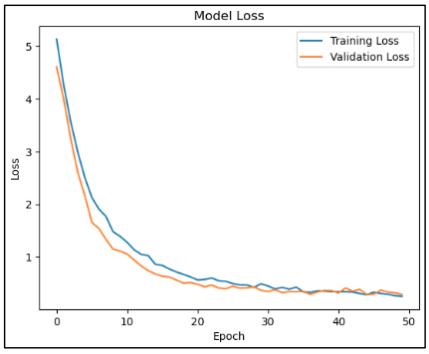

Figure 12: Training And Validation Loss Graph

Figure 12 displays the testing loss and validation loss graph. On the last epochs, the training loss began to drop from 5.1 to 0.25. Regarding validation loss, the graph began at 4.6 and dipped until it reached a final loss of 0.28.

Figure 13: Accuracy Graph For Training And Validation

The training and validation accuracy graphs derived from splitting 90:10 ratios are displayed in Figure 13. From the first epoch, both training and validation accuracy began to rise, reaching 95% accuracy in the last epochs.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

Evaluation

The experiment indicates that all of the approach are reliable in predicting the user's face. Nevertheless, the model's accuracy varies depending on the experiment. The model accuracy for each experiment is displayed in Tables 1 and 2 as follows.

Table 1: Accuracy Result On Different Epochs

Epochs	Accuracy
50	83%
100	92%

Table 2: Accuracy Result On Splitting Data Ratios

Ratios	Accuracy
80:20	99.7%
90:10	100%

Experiment 1 examined the impact of changing the number of epochs on the face recognition model's performance based on the experiment results. According to the findings, testing accuracy increased somewhat from 83% to 92% when the number of epochs was increased from 50 to 100. This implies that more training data is beneficial to the model and that finding the ideal number of epochs is essential to attaining high accuracy. On the other hand, Experiment 2 contrasted the model's performance with two distinct data splitting ratios, 80:20 and 90:10. According to the findings, the accuracy of the 90:10 ratio was somewhat higher than that of the 80:20 ratio.

This implies that, while less so than the number of epochs, the data splitting ratio also affects the model's performance. The amount of improvement seen in the two experiments is a significant difference. Testing accuracy improved by 9% in Experiment 1 when epochs were increased, whereas it improved by 0.3% in Experiment 2 when the data splitting ratio was altered. According to this, the number of epochs affects the model's performance more than the data splitting ratio.

This type of outcome also implies that the data splitting ratio and the number of epochs have a major influence on strengthening the authentication system's security features.

Conclusion

Using the Convolutional Neural Network (CNN) method, this study has effectively created an authentication system that focuses on the registration and login procedures. With an average identification accuracy of 83% to 100% under ideal circumstances, the system has proven its capacity to recognize faces effectively. The study's goals of examining the viability and usability of CNN-based facial recognition technology, creating an authentication system with the CNN algorithm, and assessing the system's performance have all been met.

The results of the study offer important insights into the creation and assessment of CNN-based facial recognition systems and have ramifications for the future development of more practical and safe authentication systems. Two tests were used to assess the system's performance, and the results indicate that the model gains from more training data and that obtaining high accuracy requires a precise number of epochs and data splitting ratio.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010

To improve the system's face recognition capabilities, it is advised that future research broaden the dataset, investigate more sophisticated face identification methods, and take pictures of the human face from various perspectives. The facial recognition system prototype can be enhanced to produce more accurate and dependable results by putting these suggestions into practice, which will ultimately improve its general usability and performance. Building on this basis, further research can improve the system's functionality and performance, resulting in the creation of more effective and safe authentication systems for Malaysian educational institutions.

Acknowledgment

College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Pahang Branch provided financial support, for which all authors are thankful.

References

Agarwal, H., Verma, G., Gupta, L., & Bca, B. (2021). Student attendance system based on the face recognition. *International Journal of Engineering and Advanced Science Technology*, *7*(9), 10. http://www.ijeast.com

Amrutha Varshini, K. (2022, November). THREE LEVEL PASSWORD SECURITY. *International Research Journal of Modernization in Engineering, 1*(1), 1–6. https://doi.org/10.56726/IRJMETS31390

Azli, A. M. B. M., Mammi, H. K., Din, M. M., & Abdul-Samad, A. (2023). Face-recognition based attendance authentication system. In *Proceedings of the 2023 International Conference on Data Science and Its Applications (ICoDSA 2023),* 367–372. IEEE. https://doi.org/10.1109/ICoDSA58501.2023.10276698

Cao, C., Zhang, Y., Wang, Y., & He, M. (2018). Deep learning and its applications in biomedicine. *Genomics, Proteomics & Bioinformatics, 16*(1), 7–21. https://doi.org/10.1016/j.gpb.2017.07.003

Ercan, V., & Özbek, M. E. (2021). A face authentication system using landmark detection. *Journal of Artificial Intelligence and Data Science*, *1*(1), 28–34.

E-Envoy. (2002, September). *Registration and authentication / Version 3.0 / Registration and Authentication e-Government Strategy Framework Policy and Guidelines*. UK Government. https://ntouk.files.wordpress.com/2015/06/registration-authenticationv3.pdf

Farik, M., Lal, N. A., & Prasad, S. (2016). A review of authentication methods. *International Journal of Scientific & Technology Research, 5*(11), 60–63. www.ijstr.org

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press. https://books.google.com.my/books?hl=en&lr&id=omivDQAAQBAJ&oi=fnd&pg=PR5&dq=%5B1%5D+Goodfellow,+I.,+Bengio,+Y.,+%26+Courville,+A.+(2016).+Deep+learning.+MIT+press.

Labayen, M., Vea, R., Florez, J., Aginako, N., & Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3079375

Mathew, M. E., George, J., Mathew, S., & Thomas, S. (2016). Colour lock system for user authentication. *International Journal for Scientific Research and Development, 2*(5), 48–52. https://doi.org/10.1234/5678

Miller, E. (2023, November 2). The state of higher education cybersecurity: Top insights and trends. *BitLyft*. https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 147-161
DOI: 10.35631/JISTM.1038010
Nikolova, I. (2023, October 31). How does artificial intelligence help in identity verification? *LinkedIn*. https://www.linkedin.com/pulse/how-does-artificial-intelligence-help-identity-ina-nikolova-ph-d-

O'Toole, A. J., & Castillo, C. D. (2021). Face recognition by humans and machines: Three fundamental advances from deep learning. *Annual Review of Vision Science, 7*, 543–570. https://doi.org/10.1146/annurev-vision-093019

Owayjan, M., Dergham, A., Haber, G., Fakih, N., Hamoush, A., & Abdo, E. (2020). Face recognition security system. *International Journal of Applied Computer Science, 15*(4), 120–135.

Rosencrance, L., Loshin, P., & Cobb, M. (2023, November 2). What is two-factor authentication (2FA) and how does it work? *TechTarget*. https://www.techtarget.com/searchsecurity/definition/ two-factor-authentication

Rittenhouse, R., & Chaudhry, J. (2016). A survey of alternative authentication methods. *Proceedings of the 2016 International Conference on Research in Applied Computer Science (RACS)*, 179–182. https://doi.org/10.2991/RACS-15.2016.31

Saragih, R. E., & To, Q. H. (2022). A survey of face recognition based on convolutional neural network. *Journal of Computer Vision*, 1–10.

Sarvakar, K., Senkamalavalli, R., Raghavendra, S., Santosh Kumar, J., Manjunath, R., & Jaiswal, S. (2023). Facial emotion recognition using convolutional neural networks. *Materials Today: Proceedings, 80*, 3560–3564. https://doi.org/10.1016/J.MATPR.2021.07.297

Said, E., & Nasr, M. (2020). Face recognition system. *International Journal of Advanced Networking and Applications, 8*(6), 4567–4574.

Thosar, D. S., & Singh, M. (2018). A review on advanced graphical authentication to resist shoulder surfing attack. *2018 International Conference on Advanced Computation and Telecommunication (ICACAT 2018)*, December 2018, 1–5. https://doi.org/10.1109/ICACAT.2018.8933699

Townsend, A. (2023, October 31). AI in authentication. *OneLogin Blog*. https://www.onelogin.com/blog/ai-authentication

Upreti, A. (2022). *Convolutional Neural Network (CNN). A Comprehensive Overview*. https://doi.org/10.20944/preprints202208.0313.v2

Varshini, K. A. (2022, November). THREE LEVEL PASSWORD SECURITY. *International Research Journal of Modernization in Engineering, 1*(1), 1–6. https://doi.org/10.56726/IRJMETS31390

Vea, R., & Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021. 3079375