

---

**Implementing an Information Verification System to Prevent Academic Fraud by Employees Using a Hybrid of ANN and RF Algorithms****Lebogang V. Lebopa<sup>1</sup>, Tonderai Muchenje<sup>2</sup>, Topside E. Mathonsi<sup>3</sup>, Solly P. Maswikaneng<sup>4</sup>**llebogangv@yahoo.com<sup>1</sup>, muchenjet@tut.ac.za<sup>2</sup>, MathonsiTE@tut.ac.za<sup>3</sup>,maswikanengps@tut.ac.za<sup>4</sup><sup>1,2,3,4</sup> Department of Information Technology, Tswane University of Technology

---

**Article Information**

Received : 14 Jun 2025

Revised : 1 Jul 2025

Accepted : 1 Aug 2025

---

**Keywords**Academic Fraud,  
Qualification  
Verification, Artificial  
Neural Networks,  
Random Forest,  
Information Verification  
System

---

**Abstract**

Academic fraud, particularly the falsification of qualifications, poses a growing threat to organizational integrity and professional credibility. This study proposes an Information Verification System (IVS) to combat employee credential fraud using a hybrid of Artificial Neural Network (ANN) and Random Forest (RF) algorithms. The method follows a two-step process: first, ANN extracts key certificate features, such as digital signatures, logos, and serial numbers, then RF classifies the certificate as authentic or fraudulent based on these features. Tested on 4,830 certificates from Mopani TVET College, alongside 1500 replicas, the system achieved near-perfect results: 98.90% accuracy, 96.75% precision, 99.33% recall, and a 98.03% F1-score, outperforming Recurrent Neural Networks (RNN), Support Vector Machines (SVM), and Logistic Regression models. By integrating with institutional databases, the IVS offers a scalable, secure solution to automate verification processes so that only legitimate qualifications are accepted. These results suggest that the proposed IVS offers a scalable and secure solution for institutions and employers, significantly improving the efficiency and reliability of academic credential verification.

---

## A. Introduction

Academic fraud, especially forged qualifications, undermines trust in educational and professional systems globally. The rising demand for credentials has driven an increase in counterfeit certificates, with the South African Qualifications Authority (SAQA) recording a 41% rise in identified fraudulent qualifications in the year 2022 [1]. The escalating prevalence of counterfeit diplomas is often seen as a consequence of economic or social crises, where individuals fabricate certificates to secure employment. Recent studies, however, show that fraudulent diploma production is not limited to low-level positions, it also involves activists, government members, officials, and even prospective university students [2]. Current verification methods, which are typically manual, expensive, and lack transparency, find it challenging to match the advancements in complex forgery techniques. This study addresses these gaps by developing an IVS that uses a hybrid ANN-RF algorithm to detect fraudulent academic certificates efficiently and accurately.

## B. Related Work

The verification of academic credentials has historically relied on manual processes, which suffer from prolonged processing times, scalability constraints, and limited automation [3]. According to a survey, one in three employers in the United Kingdom (UK) do not request candidates for their degree certificates, and of those who do, 76% of employers assume the certificates are legitimate and do not verify their authenticity [4]. Numerous researchers have explored the issue of fraudulent academic certificates and proposed potential solutions. A study by Boukar et al. [5] incorporated the usage of Java Database Connectivity (JDBC) and My Structured Query Language (MySQL) connector jar files to create a web-based solution aimed at substituting the customary manual verification procedure. This new approach involves obtaining certificate data in JavaScript Object Notation (JSON) format from institutions and storing it in a database. Doing so eliminates security risks and the potential for mistakes caused by human error when verifying the certificates. The database was queried using a Structured Query Language (SQL) command to fetch the appropriate data. The outcomes are analysed and displayed in a JSON format utilizing the GSON jar file and JSON library functions. Nevertheless, the inclusion of NoSQL functionalities in MySQL proved to be a significant drawback for their system as it caused a decrease in operational speed.

Saleh et al. [6] identified this problem and went a little further to propose a blockchain Hyperledger fabric framework to assess the educational certificates of the students. They also deliberated on the fact that the issuing process of the degrees and certificates is not transparent and up-to-date, which led to the issuance of fake certificates as well. Their proposed framework introduced a secure and decentralized approach to certificate management, ensuring authentication, authorization, and privacy. Blockchain technology, through its immutable and tamper-proof ledger, played a crucial role by recording certificate issuance in a way that cannot be altered or forged. The decentralized nature of the blockchain also eliminated the need for a central authority, making the verification process faster and more trustworthy. This also ensured that the job seeker was

trained enough to take on the job tasks. However, the system was not thoroughly tested, leaving opportunities for future work, particularly to address its limitations in scalability and its ability to manage a high volume of verification requests.

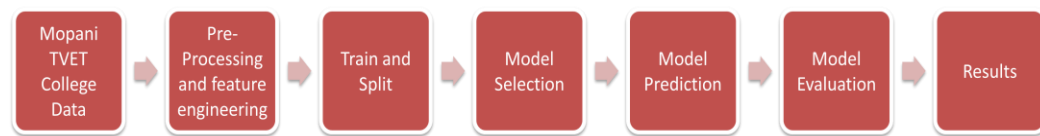
The study by Yusuf et al. [7] enabled an end-user to define a certificate template and template format without the requisite of Extensible Markup Language (XML) knowledge by clicking a few buttons and typing from the system Graphical User Interface (GUI), verifying the certificate, and generating one or more certificates simultaneously. In the system, students' details are imported into the system using an Excel file thus, making the system partly automated and inefficient. Kewale et al. [8] proposed a Radio-frequency identification (RFID)-based verification system that uses a unique identifier and a cryptographic key to authenticate digital certificates. The certificate is scanned, and its data is sent to a central server using an RFID reader system. The authenticity of the certificate is then verified by the central server using the cryptographic key. The accuracy of the system was verified by testing it on a subset of certificates, and it yielded excellent results. Nevertheless, there were possible disadvantages associated with the utilization of RFID technology for the purposes of issuing and verifying academic certificates. There was a concern that the utilization of RFID technology might lead to unauthorized retrieval of personal information, as the RFID tag holds delicate data.

Wellem et al. [9] proposed a certificate verification system that uses a combination of Quick-Response (QR) codes and watermarks. Each certificate has its own distinct watermark embedded within the system, which can be utilized for the purpose of confirming its genuineness. The system is equipped with a QR code, which can be scanned to obtain supplementary information about the individual holding the certificate. The system underwent testing using a small group of certificates, and it demonstrated a strong ability to accurately verify them. However, the primary concern lies in the fact that individuals possessing the appropriate tools and expertise can eliminate or modify watermarks, thus enabling the creation of counterfeit certificates. Moreover, watermarking could lead to the possibility of certificate forgery, as attackers may be able to replicate the watermark and create counterfeit certificates.

This study addresses these gaps by proposing a hybrid ANN-RF model that combines ANN's deep feature extraction capabilities with RF's ensemble classification strengths, tailored specifically for academic certificate verification. This approach aims to overcome the limitations of manual processes and emerging technologies by offering a scalable and accurate solution.

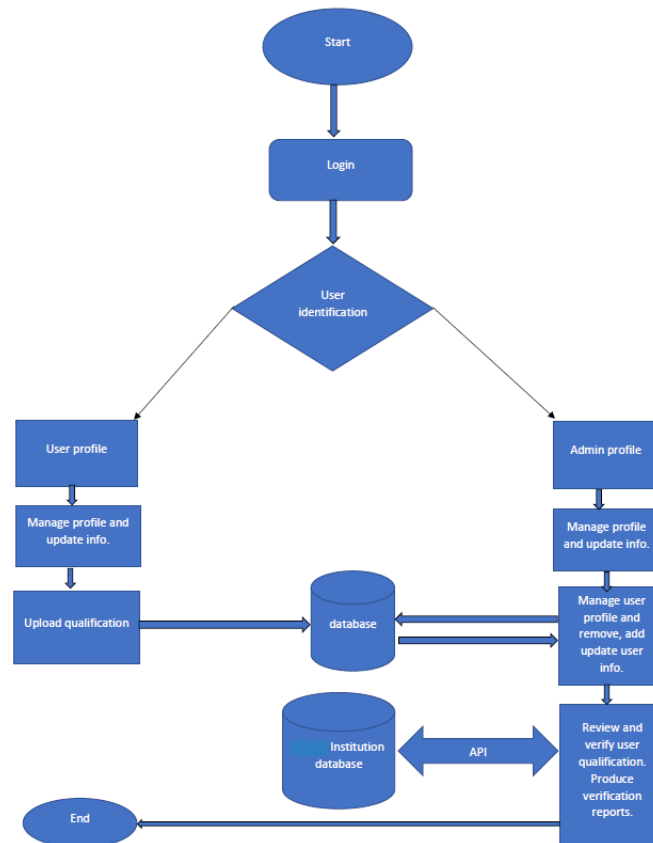
### **C. Methodology**

This section presents the methodology applied in this research. As presented in Figure 1, the study made use of Python and the 7-step experimentation, namely data collection, data pre-processing, feature engineering, splitting the dataset, model selection, model evaluation, and results.



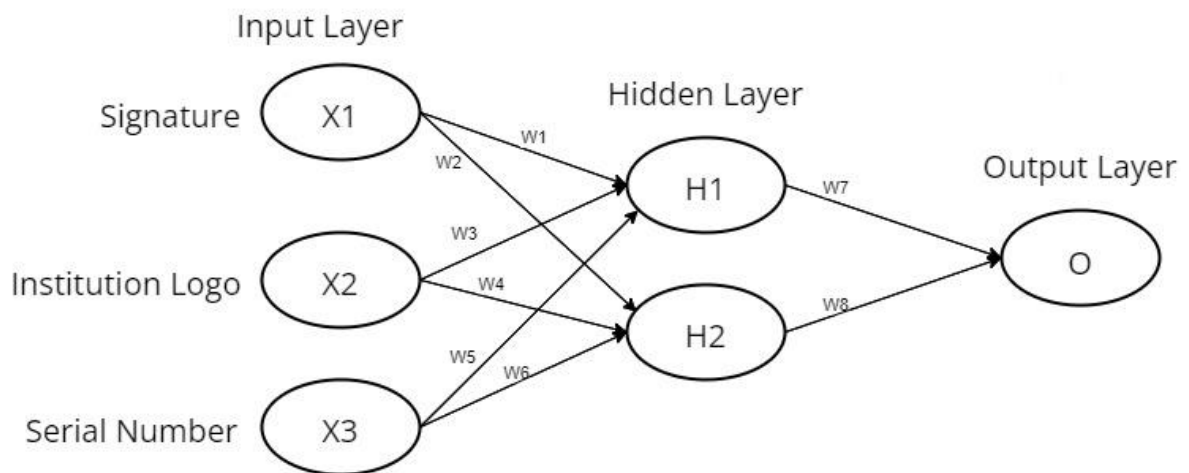
**Figure 1.** Model Evaluation Process

The selection of a hybrid ANN and RF approach in this study is based on the complementary strengths of both algorithms in handling complex and high-dimensional data, particularly in image classification tasks. To integrate the ANN-RF algorithms into the verification system, a two-step process is followed. Firstly, the ANN algorithm is used to extract and learn the features from the certificate, and the RF algorithm is used to classify the certificate as either authentic or fraudulent based on the learned features. By combining these algorithms, this will ensure higher accuracy as the strength of one algorithm can compensate for the weakness of the other. The training data for the ANN-RF algorithm consisted of a total of 4830 certificates from the Mopani TVET College. For the purposes of the study, 1500 replicas were designed using the Microsoft Word tool. These replicas were carefully crafted to accurately reflect the variability and characteristics of the original dataset, ensuring a balanced representation across different categories within the certificates. The data was split into 80% for training and 20% for testing, with preprocessing (resizing, grayscaling, normalization) performed using Scikit-learn and Keras. The prototype was implemented using various software tools. The user interface was developed in HTML, while MySQL managed the database of academic certificates. Programming languages such as Java and Python were used to integrate the system components. The hybrid ANN-RF algorithm was implemented by first using an ANN, with layers including a convolutional layer, max pooling, flatten, and dense layers for feature extraction, followed by a Random Forest classifier (configured with 100 trees) for classification. A simulation prototype was developed using the TomCat server 10.0. Experiments were conducted in a controlled environment using Jupyter Notebook within Anaconda Navigator.



**Figure 2.** Proposed System Workflow

Figure 2 illustrates the proposed system workflow, and it outlines the entire process of the academic certificate verification system from start to finish. It details the roles of administrators and users, beginning with certificate submission and proceeding through data processing, verification, and feedback stages. The administrator possesses full privilege rights over the system, allowing them to manage and oversee all critical functionalities. Specifically, the administrator can view, delete, and verify qualifications, as well as access and review user feedback. Additionally, the administrator has the authority to upload consent forms and manage administrative roles by updating existing admin accounts or adding new ones. On the user side, individuals have the ability to update their personal accounts, download consent forms for processing, and upload their qualification documents for verification purposes.



**Figure 3.** IVS ANN Model

The diagram in Figure 3 provides a detailed view of the ANN used in the system for feature extraction. The ANN consists of three layers, namely an input layer, a hidden layer, and an output layer. The process begins with the input layer, which is the first layer in the network, and it directly receives the data. The certificate features that are extracted to serve as system inputs for the verification process are the digital signature, institution logo, and serial number.

The hidden layer performs complex computations on the inputs received from the input layer. It looks for inconsistencies in image quality, such as color variations or resolutions. Nodes in the hidden layer receive inputs from the input layer, apply weights and biases to these inputs, and pass them through an activation function to produce an output. The output layer is the final layer in the network. It produces the final prediction of whether the certificate is authentic or fraudulent based on the patterns learned in the hidden layer.

The ANN computes the output using the following equation:

$$y = f(w_1x_1 + w_2x_2 + w_nx_n + b) \quad (1)$$

**Where;** y: The output of the artificial neural network.

$x_1, x_2, \dots, x_n$ : Are the input features extracted from the certificate (Digital signature, institution logo, and serial number).

$w_1, w_2, \dots, w_n$ : Are the weights associated with each input feature.

b: Represents the bias term

f: Represents the activation function (sigmoid or ReLU)

The ANN output  $y$  is then passed into a Random Forest classifier, which predicts the certificate class using:

$$f(x) = \operatorname{argmax}_k (\sum_{t=1}^T I(h_t(x) = k)) \quad (2)$$

**Where;**  $f(x)$ : Represents the final prediction of the random forest classifier for input features  $(x)$ .

$T$ : The number of decision trees in the forest.

$x$ : The input features are extracted from the certificate (student's name, institution name, degree type, date of issue, certificate number, and language analysis).

$k$ : Number of classes.

$I$ : An indicator function that returns 1 if the argument is true and 0 if false.

The final classification decision combines both models as:

$$\text{RF Output} = f(x)y \quad (3)$$

**Where;** RF Output: Represents the outcome of verification (Certificate is authentic or fraudulent).

$f(x)$ : Output of the RF prediction.

$y$ : Output of the ANN.

---

### Algorithm 1: ANN-RF Algorithm

---

```
// Define the ANN and RF models
private ANNModel annModel;
private RFModel rfModel;

// Process raw image files into a suitable format
private ImageData processImage(File rawImage) {
    return processedImageData;
}

// Define the dataset
```

```
double[][] dataset = new double[][]  
  
// Train the ANN model  
annModel = new ANNModel();  
annModel.train(dataset);  
// Train the RF model  
rfModel = new RFModel();  
rfModel.train(dataset);
```

**Process:****1: Run equation (3.1) - ANN for feature extraction**

$$y = f(w_1x_1 + w_2x_2 + w_nx_n + b)$$

**2: Run equation (3.2) - Input ANN output to RF**

$$f(x) = \operatorname{argmax}_k (\sum_{t=1}^T I(h_t(x) = k))$$

**3: Output of the ANN-RF algorithm**

RF Output = f(x)y

**4: if (RFOutput == 1) {**

5:   System.out.println("The academic certificate is authentic.");

**6: else**

7:   System.out.println("The academic certificate is fraudulent.");

**8: end**

---

**D. Experimentation**

The experimentation phase involved a detailed simulation setup:

- **Data Collection and Preparation:** A dataset comprising 4830 certificates from Mopani TVET College was used. In addition, 1500 replica certificates were generated using Microsoft Word to simulate fraudulent documents. Images were preprocessed, resized to 100 × 100 pixels, converted to grayscale, and normalized.

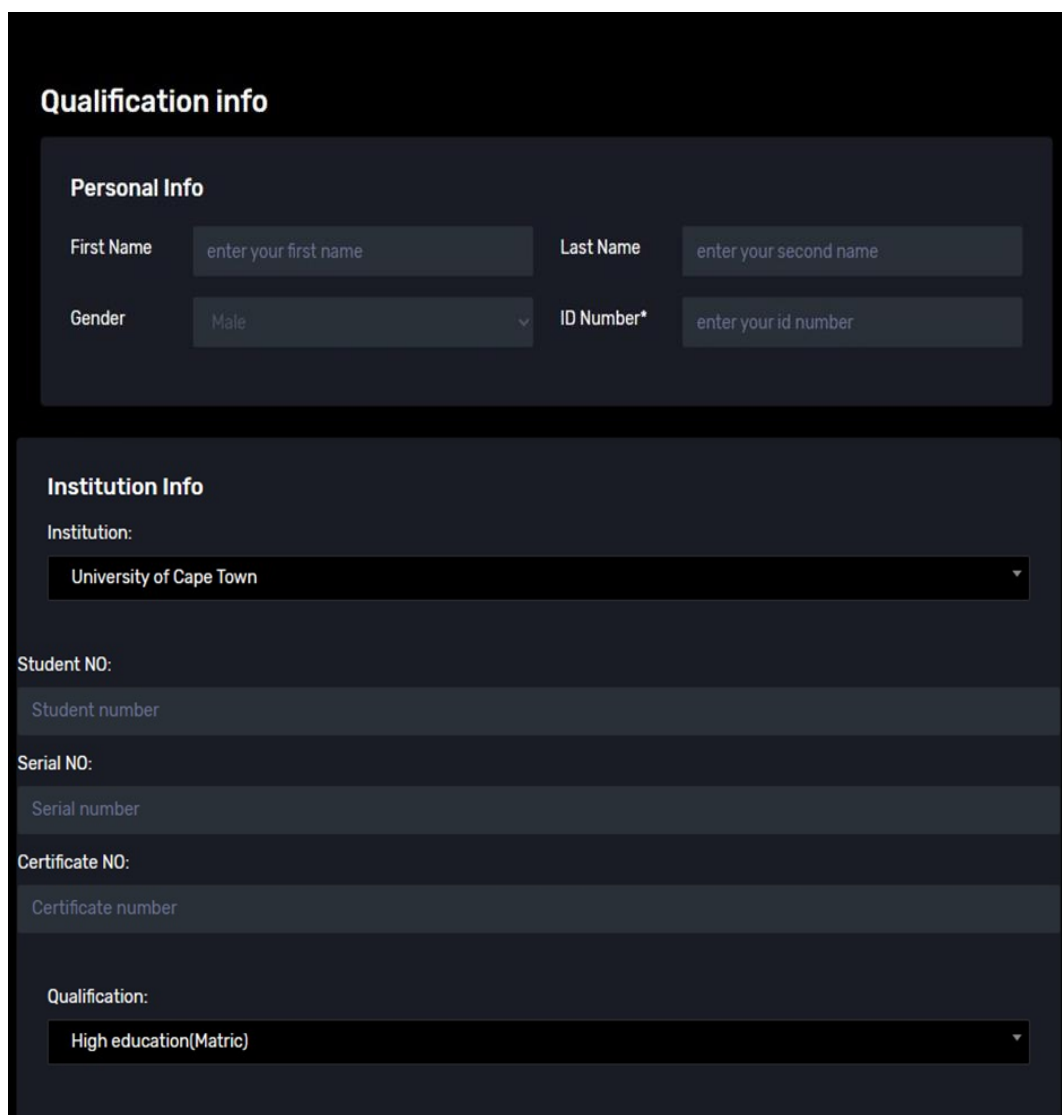
- **Model Architecture:** The ANN model architecture included an input layer with a Conv2D layer (32 filters, kernel size 3 × 3, 'relu' activation), followed by a MaxPooling2D layer (pool size 2 × 2), a Flatten layer, and a Dense hidden layer (64 units with 'relu' activation). The output layer consisted of 1 unit with 'sigmoid'



activation for binary classification. The RF classifier was configured with 100 trees and a random state of 42.

- **Training Procedure:** Training was performed over 10 epochs with a batch size of 32 in an Anaconda environment using Jupyter Notebook. The ANN model was compiled with the Adam optimizer and binary cross-entropy loss function. The RF model was trained using Scikit-learn's RandomForestClassifier after flattening the image data.

- **Simulation and Evaluation:** Performance was evaluated using standard metrics, and the confusion matrix confirmed zero misclassifications. Detailed training and validation curves were generated to monitor the learning process.



The image shows a web form titled "Qualification info" with two main sections: "Personal Info" and "Institution Info".

**Personal Info**

First Name	<input type="text" value="enter your first name"/>	Last Name	<input type="text" value="enter your second name"/>
Gender	<input type="text" value="Male"/>	ID Number*	<input type="text" value="enter your id number"/>

**Institution Info**

Institution:

Student NO:

Serial NO:

Certificate NO:

Qualification:

**Figure 4.** Qualification & Institution Information Page

The prototype system, which utilized results from the ANN-RF algorithm, was designed as a web-based application for validating certificates. It provides users with comprehensive access to qualification and institution-related details. As presented in Figure 4, the Institution Info area shows essential information such as the name of the issuing institution, the student number, serial number, and certificate number. It also includes a Qualification Info area, which has a Personal Info subsection where users can enter or see details such as the first name, surname, gender, and ID number of the certificate holder. This gives assurance that users can validate not only the academic credentials but also the personal identity that accompanies the certificate, enhancing the system's utility for accurate validation.

**Figure 5.** Certificate Verification Process Page

Figure 5 illustrates a section of the web-based application designed for certificate verification, enabling users to upload a scanned copy of their academic certificate for validation. The interface consists of two main areas: Certificate Info and Agreement Info. After the files are uploaded, users can continue by clicking the blue "SUBMIT" button to start the process or choose to cancel the action by clicking the black "CANCEL" button. This streamlined design ensures a user-friendly experience for submitting documents securely within the IVS.

## E. Results

The experimental results are derived from the rigorous testing of the integrated ANN-RF algorithm. Key performance metrics recorded include accuracy, precision, recall, and F1 score. As illustrated in Figure 6, the ANN-RF algorithm achieved 98.90% accuracy, 96.75% precision, 99.33% recall, and a 98.03% F1 score, with the confusion matrix demonstrating a minimal error rate. These results indicate highly effective classification performance for authentic versus fraudulent academic certificates. In contrast, the RNN model, which was also tested, achieved only 86.92% accuracy, 85.71% precision, 99.93% recall, and an 89.67% F1 score,

but was unable to correctly identify negative samples. The SVM model achieved 93.50% accuracy, 93.50% precision, 93.49% recall, and a 95.81% F1 score, indicating strong but slightly lower performance than ANN-RF. The Logistic Regression model recorded 91.56% accuracy, 91.77% precision, 91.56% recall, and a 93.42% F1 score, showing it performed adequately but less robustly than the hybrid model. While the SVM and Logistic Regression models performed well, their linear nature makes them more prone to overfitting. The ANN-RF algorithm, on the other hand, is better at handling complex, non-linear relationships, making it more robust and adaptable to real-world scenarios. Overall, the ANN-RF demonstrated superior performance, while the RNN model struggled to accurately identify negative samples.

The models were evaluated using the following metrics:

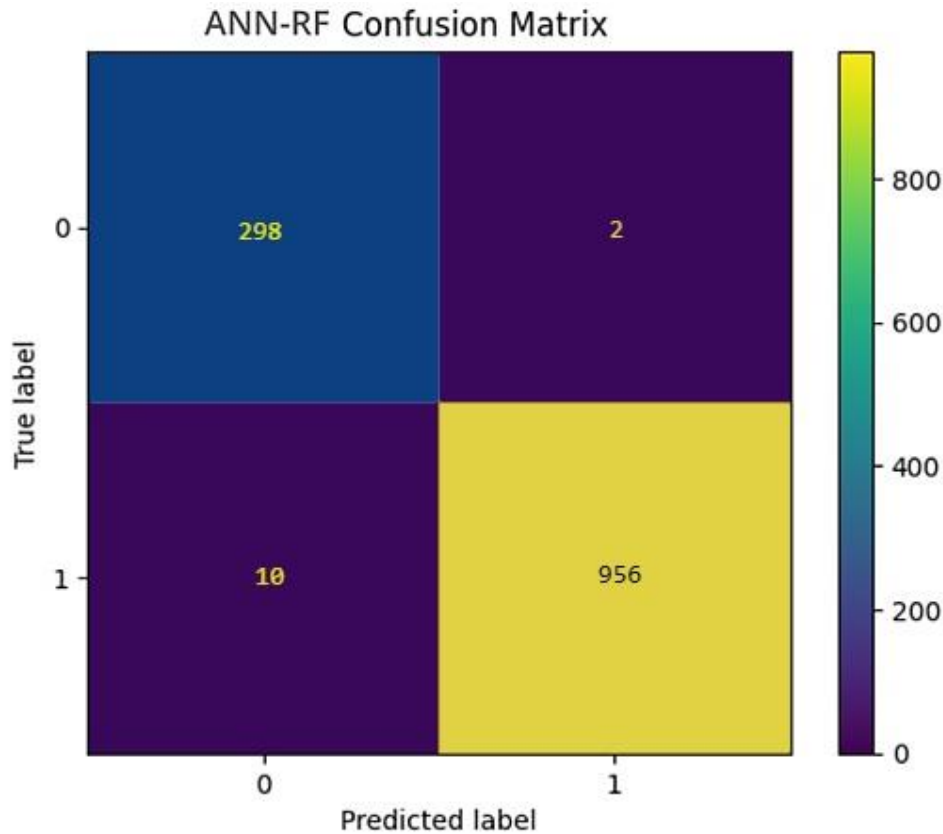
### 1. Confusion Matrix

A Confusion Matrix is a performance measurement for the classification of problems of machine learning, where the output can be two or more classes [10] confusion matrix is presented in a table form with the combinations of predicted and actual values.

In the context of this study, the confusion matrix was used to evaluate the performance of the proposed ANN-RF model in classifying academic certificates as either authentic or fraudulent.

The confusion matrix for the ANN-RF model is structured in a table format with four key components:

- **True Positives (TP):** The number of correctly identified fraudulent certificates.
- **True Negatives (TN):** The number of correctly identified authentic certificates.
- **False Positives (FP):** The number of authentic certificates incorrectly classified as fraudulent.
- **False Negatives (FN):** The number of fraudulent certificates incorrectly classified as authentic.



**Figure 6.** ANN-RF Confusion Matrix

## 2. Accuracy

Accuracy simply measures how frequently the classifier makes correct predictions. In the case of verifying academic certificates, accuracy would indicate how often the system correctly identifies whether a certificate is fraudulent or authentic. The formula for calculating accuracy is given by

$$\bullet \quad \text{Accuracy} = \frac{\text{True Positives (TP)} + \text{True Negatives (TN)}}{\text{Total Instances}} \quad (4)$$

## 3. Precision

According to [11], precision is the proportion of True Positive cases divided by the total number of positively predicted units. True Positive are the elements that the model deemed as positive and they are positive, whereas False Positive are the cases that have been considered as positive by the model, but they are negative [11]. In this context, precision would measure how many certificates identified as authentic by the system are authentic. Precision is given by

$$\bullet \quad \text{Precision} = \frac{TP}{TP + FP} \quad (5)$$

## 4. Recall

Recall, also known as sensitivity, refers to the number of positive cases that were accurately predicted by the model [11]. Recall is useful in cases where a False

Negative is of higher concern than a False Positive. For certificate verification, the recall would indicate how many authentic certificates were correctly identified by the system. The equation for recall is given by

$$\bullet \text{ Recall} = \frac{TP}{TP+FN} \quad (6)$$

### 5. F1 Score

F1-Score is defined as a harmonic mean of recall and precision to attain an optimal solution (combining precision and recall) [12]. A high F1-Score indicates that both precision and recall are high, reflecting a good balance between identifying true positives and minimizing False Positives and False Negatives. The equation is given by

$$\bullet \text{ F1 Score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (7)$$

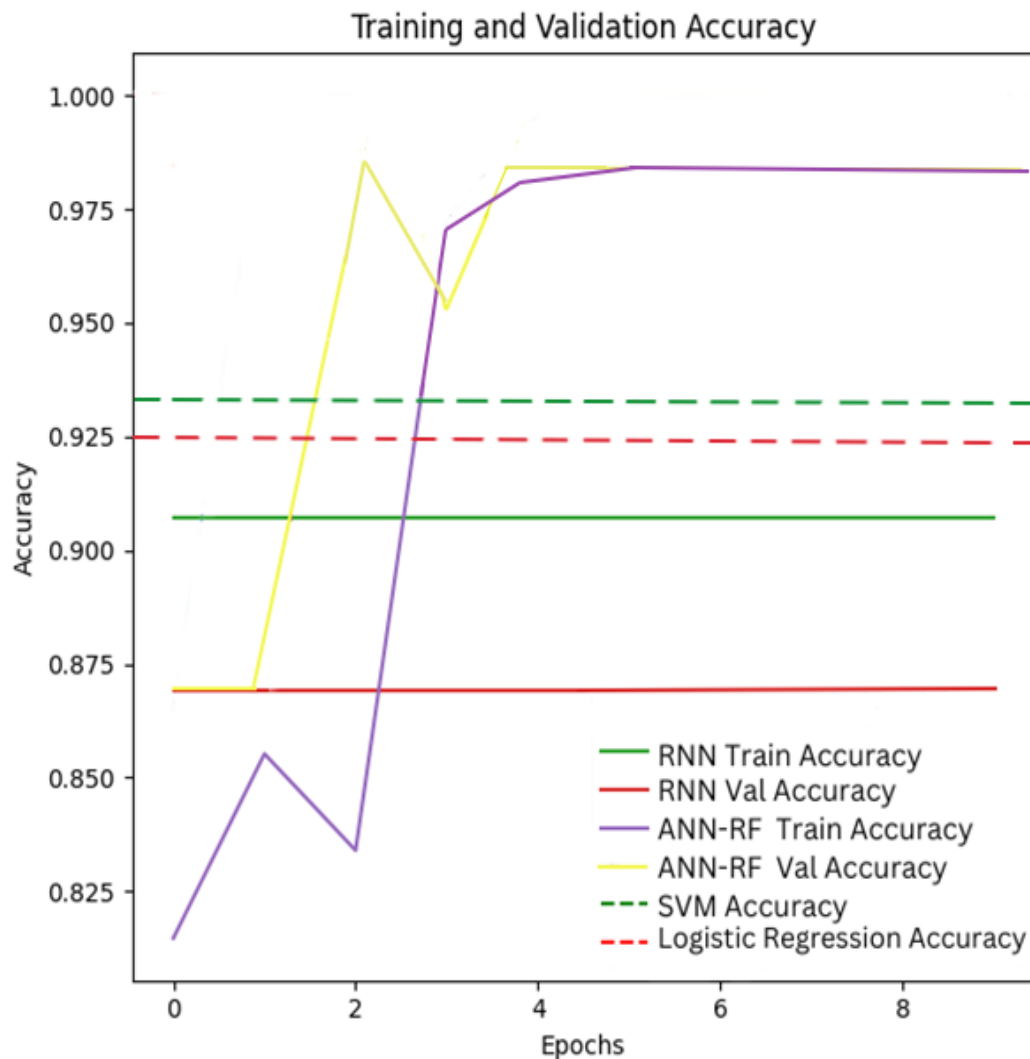
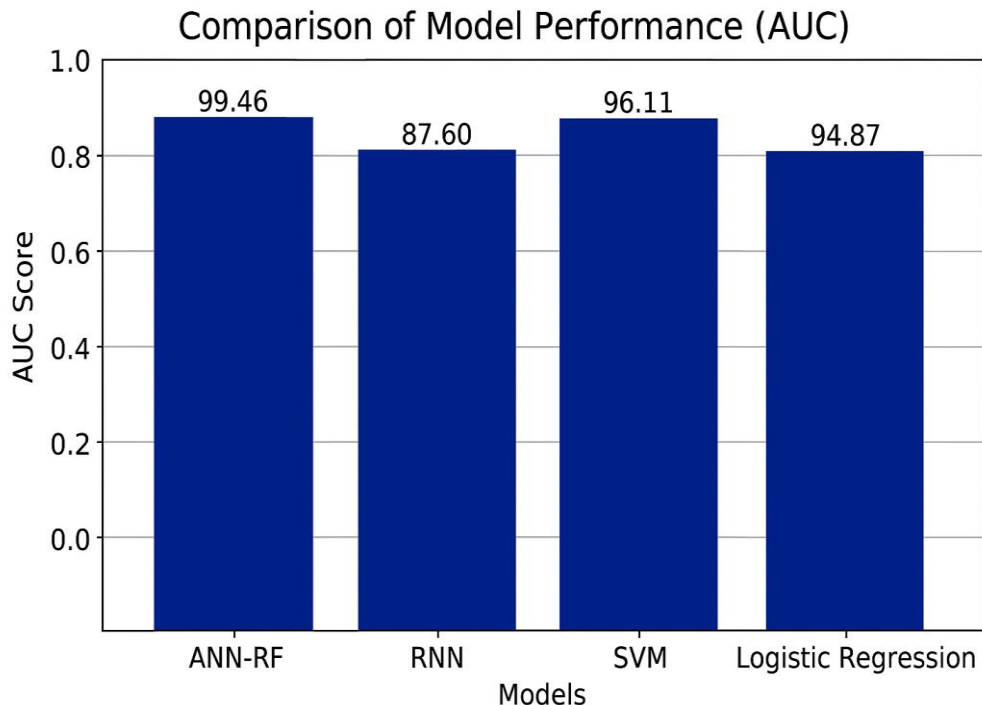


Figure 7. Training Accuracy

The data analysis indicates that the hybrid approach not only improves the reliability of the verification system but also minimizes the time taken to verify certificates. Trends in training and validation accuracy and the loss function over the epochs are presented by graphs drawn with the help of the matplotlib library in Python, and show the excellent performance of the ANN-RF model. Each of the models was trained over the same dataset of images and compared its performance over a test set.



**Figure 8.** Model Performance Comparison

## F. Discussion

The results are evident that integrating ANN and RF algorithms significantly enhances the verification of academic certificates. The perfect performance metrics of the ANN-RF algorithm demonstrate its potential to eliminate fraudulent documents. The discussion emphasizes that while traditional verification systems are often time-consuming and error-prone, the hybrid approach offers a rapid and highly accurate alternative.

The integration allows the ANN to extract subtle features such as digital signatures and institution logos, which the RF classifier then uses to make a final, robust classification. The effectiveness of the system is also boosted by its ease of integration with institutional databases to make real-time verification possible. Though the ANN-RF model was found to be more effective than other evaluated alternatives, such as RNN, the discussion notes that further refinement may be needed to address scalability in real-world scenarios. The results not only outperform RNN, SVM, and Logistic Regression models tested in this study, but also expand upon findings in existing literature. For instance, Boukar et al. [5] proposed a web-based solution using database queries, while Saleh et al. [6]

introduced a blockchain-based framework to secure certificate authenticity. While both studies provided foundational methods for reducing academic fraud, they faced challenges with scalability and real-time deployment. This research improves upon those models by introducing a hybrid of ANN and RF, which delivers both high accuracy and operational speed. In doing so, it aligns with existing evidence supporting ensemble learning Kewale et al. [8] and Wellem et al. [9] and goes further by integrating visual pattern recognition, which was lacking in most prior works.

From a theoretical perspective, the study contributes to the understanding of ensemble machine learning models in document verification tasks, showing how the integration of ANN and RF enhances feature learning and classification robustness. Practically, the system can be adopted by educational institutions and employers to automate and improve the accuracy of qualification verification, reducing reliance on manual checks and minimizing human error. From a societal perspective, this system has the potential to inform policies for secure credential verification in education and employment, helping to combat academic fraud and restore trust in qualifications.

#### **G. Limitations and Future Works**

Despite the exceptional performance of the proposed IVS, there are several limitations that should be acknowledged. One of the primary concerns lies in the dataset used for training and testing, which was confined to a single institution, highlighting the need for broader validation. Furthermore, the experiments were conducted in a controlled simulation environment, and transitioning the system into real-world applications may introduce unforeseen challenges and environmental variables that could affect its performance.

Moreover, the system's reliance on current artificial intelligence technologies presents another constraint. As fraud techniques evolve, the model may require ongoing updates to remain effective. For future work, this study proposes extensive experimental evaluations of the proposed ANN-RF in a much bigger and more complex environment with a much larger dataset from various institutions and the deployment of the model. Additionally, integration of unsupervised learning to uncover hidden patterns and structures in the data that may not be apparent through supervised learning alone.

Furthermore, the proposed ANN-RF algorithm could be integrated with blockchain technology to create a secure and immutable record of academic certificates. This would ensure that once a certificate is verified as authentic, it cannot be tampered with or altered. Secondly, efforts could be made to standardize the verification process across different countries and educational systems using the ANN-RF algorithm. This would facilitate the global recognition of academic qualifications. It is my recommendation that the prototype be deployed in higher learning institutions, as these institutions are ideal candidates to benefit from the system's capabilities. Additionally, organizations and recruiting agencies are the primary target users of the system, making them the most suitable entities to pilot the prototype and provide valuable feedback for further development. By implementing the system in these institutions, we can ensure that it is tailored to

meet the specific needs of educators, students, and recruiters, ultimately leading to a more effective and efficient experience for all stakeholders.

## **H. Conclusion**

This research has demonstrated the feasibility and effectiveness of a hybrid ANN-RF approach for verifying academic certificates. Based on the findings of the discussions and analysis, the proposed ANN-RF algorithm has demonstrated promising results, achieving optimal performance across all four evaluated metrics. The implications of this study are significant for both educational institutions and employers, as the proposed IVS can dramatically improve the integrity of academic verification processes. The key contribution of this research lies in the combination of ANN's deep feature extraction with RF's stable classification, which together deliver superior verification accuracy. This hybrid model introduces a creative and innovative approach compared to traditional manual checks or single-algorithm systems. Theoretically, the study advances the field by demonstrating how ensemble machine learning models can outperform traditional models in image-based verification tasks. Practically, it presents a scalable tool that can streamline HR and admissions processes by reducing manual workload and increasing trust in submitted qualifications. Societally, this model has the potential to support policy development around educational assessments and combat certificate fraud in hiring processes. While there are limitations that need addressing through further research, the study lays a solid foundation for future innovations in fraud detection and verification systems. Continued research and refinement will be crucial for adapting the system to evolving fraud tactics and ensuring its applicability across various domains. Consequently, the proposed ANN-RF algorithm has successfully achieved the objectives of this study and have also allowed it to accurately verify whether an academic certificate is authentic or fraudulent. The model has been trained effectively without underfitting or overfitting. Widespread adoption of this new technology for verifying the authenticity of educational degrees could be achieved through a globally recognized and rigorously applied verification process. And once fully developed and deployed, this advancement is expected to significantly mitigate the issue of counterfeit certificates and erroneous academic records, ultimately ensuring the integrity of academic certificates worldwide. The study's acknowledgment of these limitations and proposals for future work highlight its contribution to the field while pointing to necessary next steps for broader applicability.

## **I. Acknowledgment**

The authors would like to thank the SENTECH and Tshwane University of Technology for their financial support. The authors declare that there is no conflict of interest regarding the publication of this paper.

## **J. References**

- [1] SAQA, The South African National Qualifications Framework (NQF). [Online]. Available: <https://www.saqa.org.za/> (Accessed: Apr. 12, 2025).
- [2] S. Rahardja, I. Kosasi, M. Harahap, and M. Aini, "Counterfeit Diploma in Educational Institutions," *IJCS*, 2020.



- [3] A. A. Abbas, "Cloud-based Framework for Issuing and Verifying Academic Certificates," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 6, pp. 2743–2749, Dec. 2019.
- [4] R. Garner, "A third of employers never check job applicants' qualifications, survey finds," *The Independent*, 2018. [Online]. Available: <https://www.independent.co.uk/news/education/education-news/a-thirdof-employers-never-check-job-applicants-qualifications-survey-finds-9681286.html> (Accessed: May 20, 2023).
- [5] M. M. Boukar, S. Yusuf, and I. Muslu, "A Web Service Based Database Access for Nigerian Universities' Certificate Verification System," *Int. J. Comput. Tech.*, vol. 4, no. 1, 2017.
- [6] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain Based Framework for Educational Certificates Verification," *J. Crit. Rev.*, vol. 7, no. 3, pp. 79–84, 2020.
- [7] D. A. Yusuf, M. M. Boukar, and S. Shamiluulu, "Automated Batch Certificate Generation and Verification System," *IOSR J. Comput. Eng.*, vol. 24, no. 1, pp. 37–47, 2017.
- [8] P. Kewale, A. Gardalwar, P. Vegad, R. Agrawal, S. Jaju, and K. Dabhekar, "Design and Implementation of RFID Based E-Document Verification System," in *Proc. Int. Conf. Invent. Res. Comput. Appl.*, 2021, pp. 1–6.
- [9] T. Wellem, Y. Nataliani, and A. Iriani, "Academic Document Authentication using Elliptic Curve Digital Signature Algorithm and QR Code," *JOIV: Int. J. Informatics Vis.*, vol. 6, no. 3, p. 667, Sep. 2022.
- [10] E. Beauxis-Aussalet and L. Hardman, "Simplifying the visualization of confusion matrix," in *Proc. 26th Benelux Conf. Artificial Intelligence (BNAIC)*, Nov. 2014.
- [11] M. Grandini, E. Bagli, and G. Visani, "Metrics for Multi-Class Classification: An\_Overview," 2020. [Online]. Available: <https://doi.org/10.48550/arXiv.2008.05756>
- [12] M. Owusu-Adjei, J. B. Hayfron-Acquah, T. Frimpong, and G. Abdul-Salaam, "A systematic review of prediction accuracy as an evaluation measure for determining machine learning model performance in healthcare systems," *PLoS Digit. Health*, vol. 2, no. 11, 2023. [Online]. Available: <https://doi.org/10.1371/journal.pdig.0000290>