Identifying Fake Profiles Using Artificial Neural Networks

Theory of Neural Networks

Premkanth Raavi

https://github.com/PremkanthRaavi/Theory-of-Neural-Networks

Supervisor: Dr. Georgios C. Anagnostopoulos

INTRODUCTION

- **Rapid Growth in Social Network Use:** Mobile technology and internet access have greatly expanded global use of social networks like Facebook and Twitter, integrating them into daily life.
- **Proliferation of User Profiles:** The ease of access has resulted in billions of active profiles, increasing social interactions and information sharing across diverse platforms.
- **Emergence of Fake Profiles:** Fake profiles, created by bots or malicious entities, are becoming prevalent, posing serious threats such as spamming, phishing, and misinformation.
- **Security Risks and Challenges:** These profiles exploit genuine user networks, leading to identity theft, data breaches, and undermining platform integrity.
- **Technological Efforts in Detection:** Advanced AI and neural network technologies are being employed to detect and combat fake profiles, though challenges remain due to continuously evolving malicious tactics.

PROBLEM STATEMENT

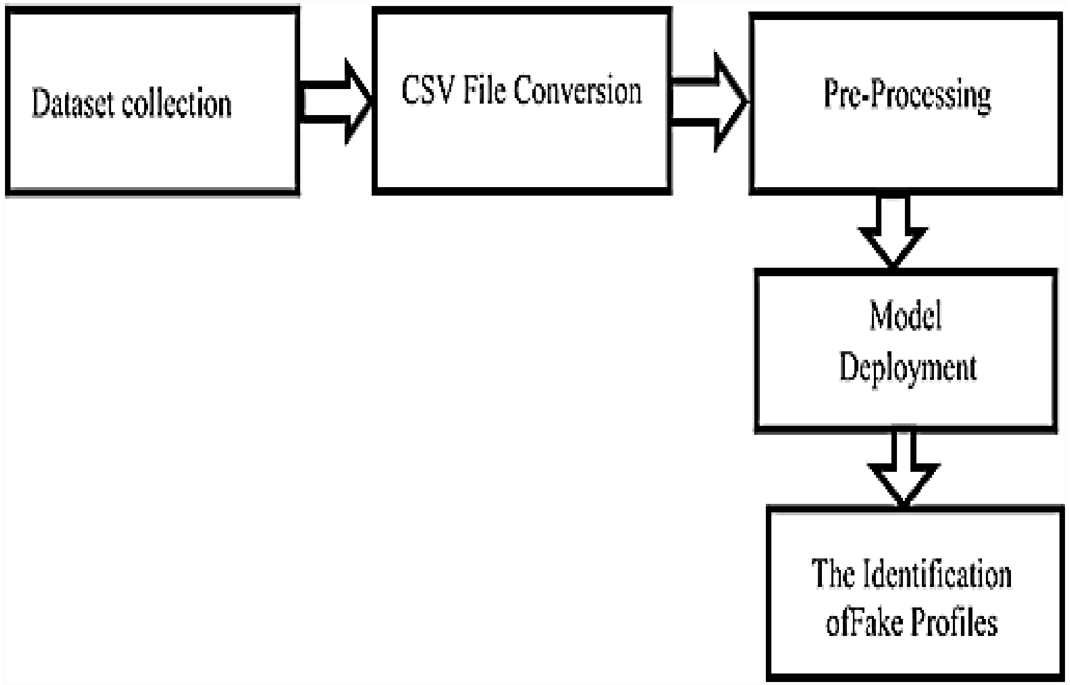
- **Increased Use of Social Networks:** More people are using online social networks via smartphones, making these platforms central to their social lives.
- **Problem of Fake Profiles:** As the number of users grows, so does the number of fake profiles. These profiles can be used for fraudulent activities, spreading misinformation, or damaging reputations.
- **Inefficiency of Current Detection Methods:** Current methods for identifying fake profiles, such as manual reviews or basic algorithms, are either too slow, expensive, or not accurate enough.
- **Potential of Advanced Technology:** Using advanced machine learning techniques, especially artificial neural networks, could potentially improve the detection of fake profiles by analyzing complex data like user behavior, connections, and profile details.

OBJECTIVE

- **Study Objective:** Develop a machine learning model using Artificial Neural Networks to identify fake profiles on platforms like Facebook and Twitter.
- **Model Application:** Train the model on distinguishing characteristics such as account age, user activity, and connection metrics.
- **Security Enhancement:** Automate the detection of fake profiles to enhance the security and integrity of social networks, reducing manual verification efforts and costs.
- **Research Impact:** Improve digital security technology, set a standard for future security measures, and make social media safer for user interactions.

METHODOLOGY

- **Objective:** Deploy ANNs to differentiate genuine from fake social network profiles.
- **Data Handling:** Analyze key features such as account age, gender, and user behavior, converting data to a format suitable for ANN.
- **Tools and Libraries:** Utilize Python, TensorFlow, NumPy, Pandas, Scikit-learn, Keras, and Matplotlib.
- **Process:** Train the ANN with historical data, validate its accuracy, and implement for real-time profile verification.

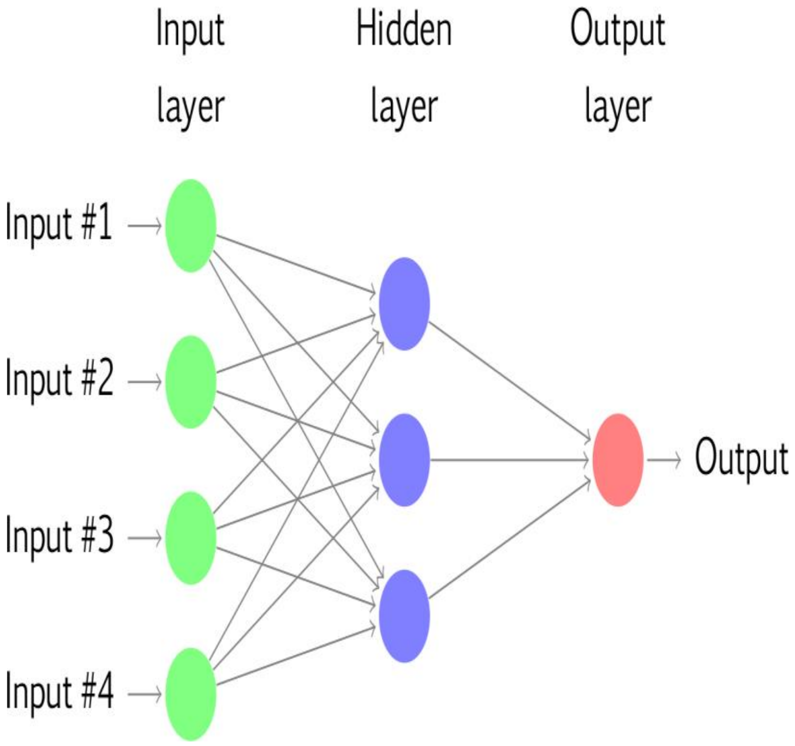


FEATURES OF FAKE PROFILE

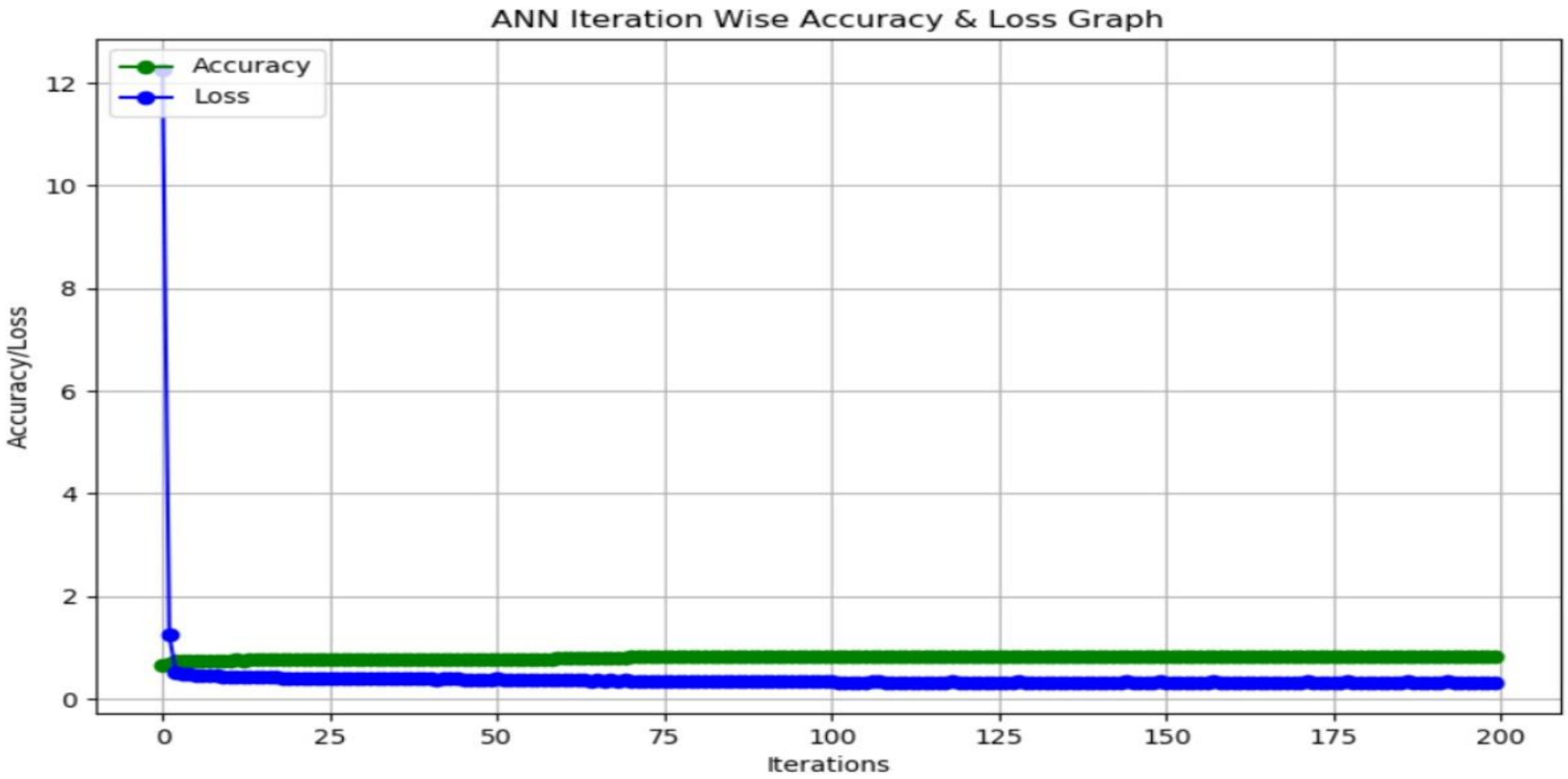
- **Profile Characteristics:** Fake profiles often display newer account ages, minimal postings, and fewer interactions with genuine users, alongside inconsistent and incomplete personal information.
- **Engagement and Content:** Characterized by low engagement rates, interactions primarily with other suspected fakes, and the use of generic or copied content across multiple profiles.
- **Static vs. Dynamic Data:** Static Data: Fixed details like name and birthdate, easily manipulated. Dynamic Data: Includes ongoing activities and interactions which are more challenging to falsify and crucial for effective detection.
- **Detection Methods:** Employing machine learning techniques, particularly ANN, to analyze both static and dynamic data, helping to distinguish between genuine and fake profiles based on behavioral patterns over time.
- **Behavioral Analysis:** Continuous monitoring and behavioral analysis to identify anomalies and patterns that deviate from those of genuine profiles, enhancing the accuracy of fake profile detection.

ANN MODEL - 01

- **ANN Architecture:** Model consists of multiple layers including input, hidden, and output layers, designed to process features such as Account Age, Gender, and Friend Count using ReLU and sigmoid activation functions.
- **Training Dataset:** Utilizes a mixed dataset of genuine and fake profiles from social networks, with features encoded numerically to train the ANN effectively.
- **Training and Validation Process:** Employs backpropagation for training with a controlled learning rate, and the model is validated on unseen data to ensure accuracy and prevent overfitting.
- **Performance Evaluation:** The effectiveness of the model is assessed through metrics like Accuracy, Precision, and Recall, and visualized through loss and accuracy graphs over training epochs.



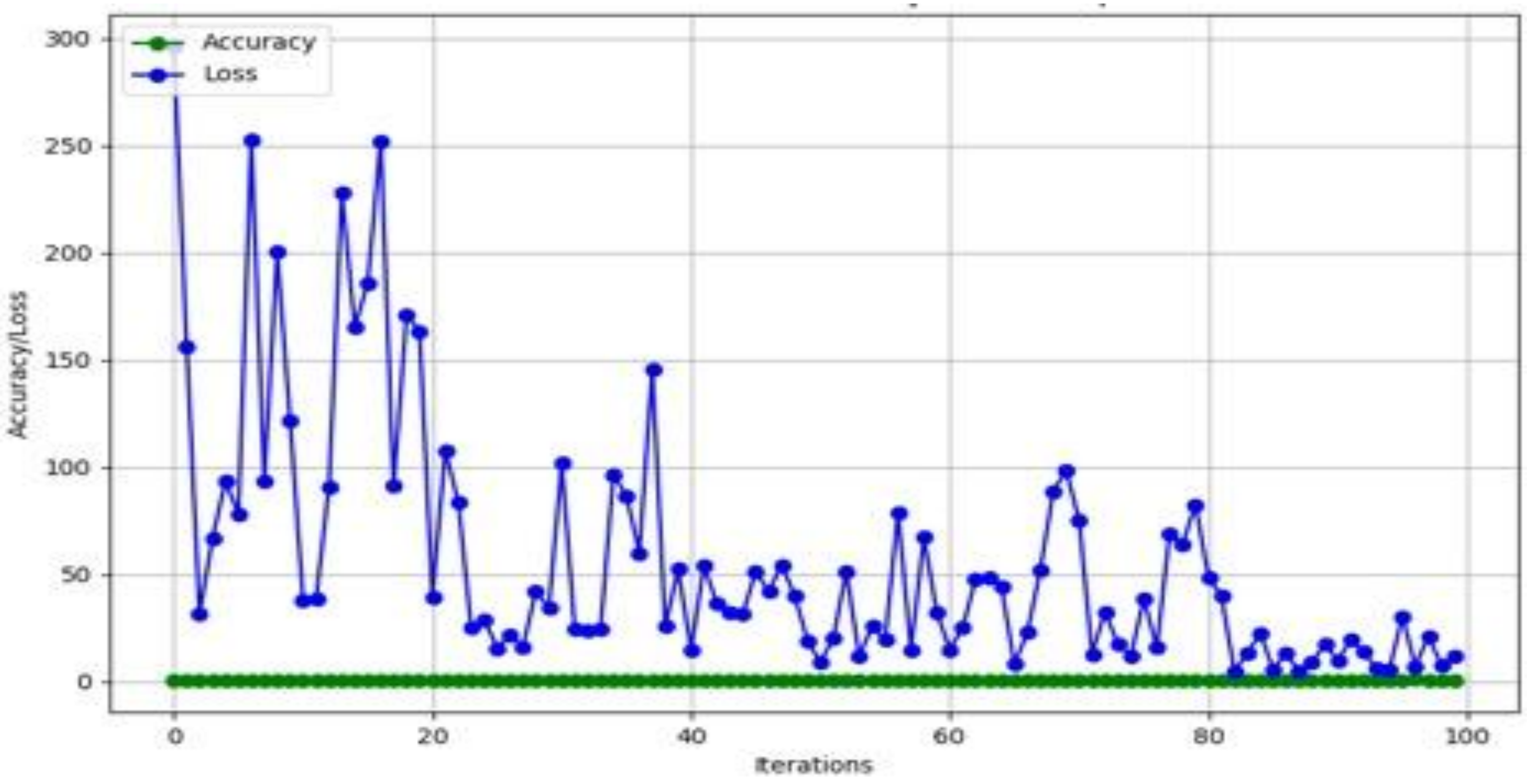
OUTPUT GRAPH FOR ANN



SVM MODEL - 02

- **Feature Selection and Preprocessing:** Select key features like user activity and post content; preprocess data for SVM suitability.
- **SVM Training:** SVM constructs a hyperplane to separate classes, maximizing the margin between nearest data points of each class using appropriate kernel functions for complex data.
- **Neural Network Integration:** Use neural networks to extract deep features from data, which are then inputted into SVM, combining pattern recognition with precise classification.
- **Model Optimization:** Employ cross-validation to prevent overfitting and tune SVM parameters like regularization and kernel choice for optimal accuracy.

OUTPUT GRAPH FOR SVM

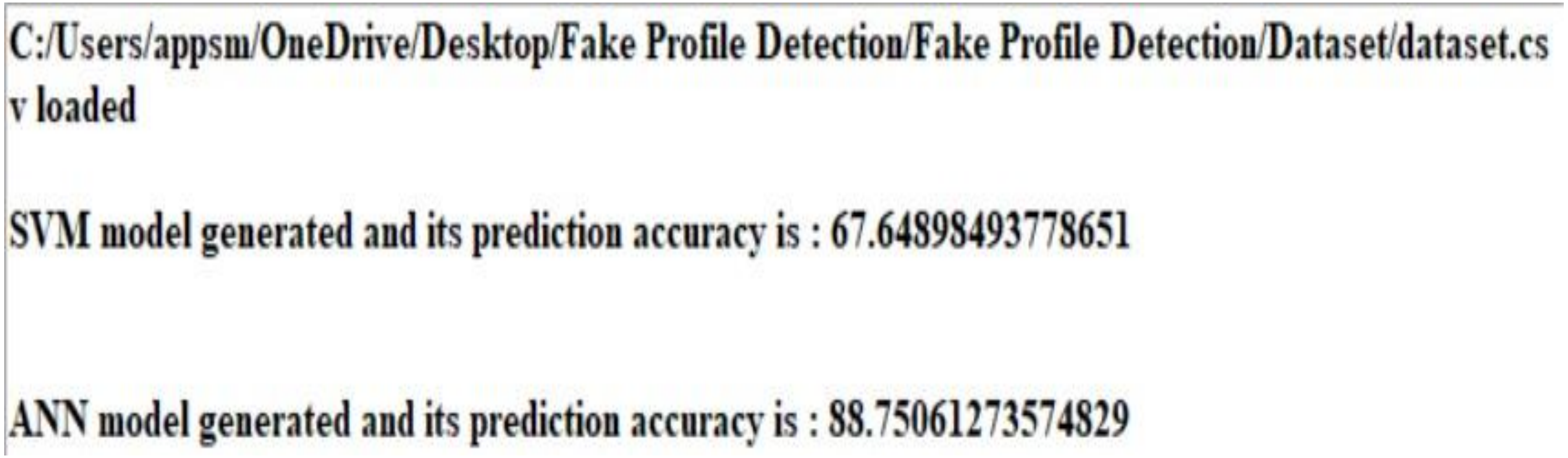


RESULTS

- High Accuracy: ANN models have shown high accuracy levels in detecting fake profiles. For instance, the final accuracy achieved after 200 epochs was 88.75%.
- Deep Learning Based: ANNs utilize layers of neurons to learn from the data, which is especially effective in handling large and complex datasets.
- Flexibility: ANN models can be adjusted and optimized for different types of datasets and features, showing robust performance across various tasks.

- Linear Classification: SVMs are particularly effective for linearly separable data and are less prone to overfitting compared to ANNs.
- Efficiency: SVMs can be more computationally efficient with smaller or less complex datasets.
- Kernel Trick: SVMs can use the kernel trick to handle non-linear data separations, which can be a significant advantage in certain scenarios.
- Accuracy: SVM models have shown the accuracy levels in detecting fake profiles. For instance, the final accuracy achieved is 67.64%.

RESULTS



```
C:/Users/appsm/OneDrive/Desktop/Fake Profile Detection/Fake Profile Detection/Dataset/dataset.cs
v loaded

SVM model generated and its prediction accuracy is : 67.64898493778651


ANN model generated and its prediction accuracy is : 88.75061273574829
```

THANK YOU!