Report of Fake Person Detection

Ivan Logutov
University of Applied Science .
MLSS 3FS-17 Research Group
Software Engineering.
Potsdam, Brandenburg, Germany.
ivan.logutov@ue-germany.de

Artur Yurchenko
University of Applied Science.
MLSS 3FS-17 Research Group
Software Engineering.
Potsdam, Brandenburg, Germany.
artur.yurchenko@ue-germany.de

Vitaliy Danyuk
University of Applied Science.
MLSS 3FS-17 Research Group
Software Engineering.
Potsdam, Brandenburg, Germany.
vitaliy.danyuk@ue-germany.de

I. Introduction

Fake identity detection is a new and important area of artificial intelligence and cybersecurity aimed at recognising and mitigating the risks associated with synthetic or fraudulent identities. These fake identities can be created using advanced artificial intelligence technologies such as deepfakes, or through traditional means such as social engineering and data manipulation. With the advent of sophisticated generative modelling, the creation of realistic fake identities has become more accessible and widespread, posing a serious threat to digital security and privacy. A major challenge in this area is to develop and implement effective tools and methods to distinguish real identities from fake identities in order to detect fraud attempts prematurely.

The importance of recognising fake identities lies in their crucial role in ensuring the security and reliability of digital platforms. In a world increasingly dependent on online interactions, the presence of fake identities can lead to numerous malicious activities such as fraud, misinformation and cyberattacks. These fake identities can undermine trust in social media, financial transactions, and even political processes. By focusing on detecting fake identities, we can strengthen security measures, protect people and organisations from identity-related threats, and ensure a more secure digital environment. Effective detection of fake identities is essential to maintaining the reliability of online systems and preventing the negative consequences of identity fraud.

The rapid development of artificial intelligence and increasingly sophisticated methods of identity fraud emphasise the importance of detecting fake identities these days. As digital platforms continue to proliferate and become an integral part of everyday life, the methods used by attackers to create fake identities are becoming increasingly sophisticated and difficult to detect. It is therefore crucial to develop advanced detection methods to counter these new threats. Addressing this issue is crucial to protecting personal data, preventing financial losses and maintaining public trust in digital services. By advancing research and development in fake identity detection, we can better protect the digital ecosystem and ensure the security and privacy of all users in the long term.

A. Related Work

In this work, we focused on developing and evaluating neural network models for the detection of fake identities. We utilized a dataset obtained from Kaggle and structured directories to facilitate the development process. Two models, CNN and ResNet, were implemented and trained for this specific task. The models' performance was analyzed by examining their accuracy and loss results. A comprehensive report was written to document our findings, and a presentation was created to summarize and share the outcomes of our research.

B. Gap Analysis

Despite the significant advances made in fake identity detection, a number of critical gaps remain unresolved. Existing examples often rely on datasets that do not fully capture the diversity and complexity of fake identities, which can limit the effectiveness of detection algorithms. Furthermore, there is a need for more sophisticated models that can not only detect fake identities with high accuracy, but also provide explanations for their decisions, thereby increasing transparency and trust in these systems. Our main goal was to create a neural network that could learn by going through certain tasks. However, due to time constraints and general task limitations, we could not correctly demonstrate this on a website or application example.

C. Novelty of our work

In this study, we have developed and tested neural network models designed specifically for detecting fake identification data. This is an important step in improving digital security. We used Kaggle's robust dataset to structure our development environment and simplify the learning process. We implemented and trained two advanced models: CNN and ResNet. We adapted these models to the unique requirements of the task at hand. Our approach involved a thorough performance analysis based on accuracy and loss metrics. This allowed us to provide a comprehensive assessment of the models' effectiveness. The novelty of our work lies in our comparative analysis of CNN and ResNet within this context. This analysis allows us to understand their relative effectiveness for identity verification tasks. Our contribution includes detailed documentation of our findings and a well-structured presentation of

TABLE I
CONTRIBUTIONS OF TEAM MEMBERS IN THE PROJECT.

Team Member	Installed dataset from Kaggle	Structured directories for development	Wrote CNN model and ResNet model	Analyzed accuracy and loss results	Wrote report	Created presentation
Ivan Logutov	✓	✓	✓			
Arthur Yurchenko				✓	✓	
Vitaliy Danyuk						✓

the results. This information can serve as a guide for future researchers and practitioners in the field of digital identity verification.

D. Our Solutions

This report on evaluating the training of a neural network for fake face detection, with the aim of improving the accuracy and reliability of identity identification. Our contribution includes a detailed description of the process of developing a neural network architecture adapted for this task and outlining methods for implementing a robust training protocol using diverse and challenging datasets. We have analysed and described the experiments performed to evaluate the training performance of our models.

The report covers not only technical aspects, but also the methodology of the experiments, data selection and processing, and criteria for evaluating the results.

II. METHODOLOGY

A. Dataset

As part of this project, we developed and evaluated two neural network models for detecting fake identification data. This is an important task for improving digital security, and our work contributes to this goal. To structure our development environment and optimize the learning process, we used the Kaggle dataset. We implemented two advanced models: CNN and ResNet. These models were adapted to solve the problem of identifying fake identification data, and their effectiveness was assessed based on accuracy and loss indicators. Our analysis shows that CNN is more effective than ResNet in detecting fake data, but both models are useful for identity verification.We have documented our findings in detail and will create a presentation to share the results with others. This dataset will serve as a guide for future research and applications in the field of digital forgery detection.

An example of data is shown in Figure 4.

Dataset Description: - "Deep Forgery Detection: Faces - Part 00" - Contains faces that are easy to detect from the larger dataset used to create fake videos - Recommended for use outside the Kaggle environment to train models Usage: - Suitable for classification tasks Details: - Each image is 160 x 160 pixels and has three color channels (PNG format). - Total number of images: 205,000 - CSV file with metadata containing four columns for each image folder.

A scheme is shown in Figure 1.

B. Overall Workflow

The provided graphs illustrate the training and validation accuracy and loss for two models, CNN (first set of graphs) and ResNet (second set of graphs), over five epochs. This analysis was conducted using the Cross-Industry Standard Process for Data Mining (CRISP-DM) methodology, a structured approach to data mining projects that provides a systematic way to approach data mining tasks. Business Objective: The primary goal is to create an effective fake person detection system that can identify and prevent synthetic identities that pose a threat to digital security. Data Collection and Preparation: We utilized diverse datasets to train and test our models, ensuring they capture the complexities and variations of fake identities. Data Preparation: The data were preprocessed and split into training and validation sets in order to facilitate model training and evaluation.Modeling: Two neural network models, a CNN (convolutional neural network) and a ResNet (residual neural network), were trained. The CNN demonstrated an increase in training accuracy from 0.9326 to 0.9435, after which it stabilized. Validation accuracy peaked at around 0.8333 and also stabilized, suggesting that the model may be overfitting. In contrast, ResNet showed a steady increase in both training and validation accuracies. Training accuracy reached 97 percent, and validation accuracy peaked just below that value. Both training and validation losses decreased, indicating effective learning and good generalization of the model. Evaluation: ResNet outperformed CNN in terms of accuracy and generalizability, achieving higher levels of accuracy with lower loss values. This makes it a more robust model for face detection.Deployment: Although our analysis indicates that ResNet represents an optimal model, the lack of advanced tools and resources has prevented the implementation of these findings in a practical application or online platform. This gap emphasizes the need for improved deployment tools to effectively demonstrate the potential of robust neural networks. Through the use of the CRISP-DM approach, we conducted a thorough and structured analysis that led us to conclude that ResNet is the most efficient model for false identification, despite obstacles associated with its implementation.

III. RESULTS

In this report, we trained two neural network models, CNN and ResNet, specifically for the task of fake person detection. We conducted a thorough analysis to determine which of these models is more efficient and reliable in learning and identifying synthetic identities. Our contributions include the implementation and training of these models on different

TABLE II
MODEL CONFIGURATION

Parameter	ResNet Model	CNN Model
Epochs	5	5
Learning rate	0.0001	0.0001
Mini batch size	32	32
Optimizer	Adam	Adam
Weights	imagenet	-
Samples in training set	131019	131019
Samples in validation set	8180	8180

datasets, as well as a detailed evaluation of their performance in terms of accuracy, training time, and robustness.

Based on the graphs showing accuracy and loss for training and validation, the following conclusions can be drawn: CNN demonstrates significant improvement in accuracy during both training and validation, reaching 97.0 percent in validation. Training and validation losses also decrease, indicating stable and quality training of the model. ResNet shows a stable but less pronounced improvement in accuracy, reaching only 93.34 percent in validation. At the same time, validation losses increase, which may indicate overfitting or issues with the model's generalization to new data.

Our results show that, despite the strengths of both models, CNN demonstrates better performance in terms of accuracy and reliability, making it a more promising candidate for real-world applications in fake person detection.

IV. DISCUSSION

In addressing the first research question regarding the effectiveness of various neural network models for detecting fake persons, we observed a clear difference in the performance of the ResNet and CNN models. The ResNet model demonstrated a rapid increase in training accuracy at the beginning, stabilizing at approximately 0.9334, whereas the validation accuracy peaked earlier and stabilized at around 93.33

A graph of ResNet Model training and validation accuracy is shown in Figure 2.

The training loss decreased steadily, indicating effective learning. However, the validation loss increased, indicating that the ResNet struggled with overfitting, performing well on training data and poorly on unseen data.On the other hand, CNN demonstrated a steady increase in both training and validation accuracy. By the fifth epoch, the validation accuracy reached 0.97, and both training and validation errors decreased consistently. This indicates that the CNN not only effectively learned from the training data, but also generalizes well to new data without overfitting. This makes it a more robust model for fake person detection. The consistent performance across the training and validation sets emphasizes the robustness and reliability of the CNN as a model for fake person detection. Considering the novelty of our contribution, we explored the application of ResNet and CNN in fake person detection and provided a comparative analysis, which was previously lacking in the literature. Additionally, our study highlighted the limitations of current tools for deploying these models in real-world scenarios and emphasized the need for advanced resources.Addressing these gaps, our research provides valuable insights into the strengths and limitations of neural network models, and proposes directions for future enhancements in the field. Additionally, our study identifies several promising areas for future research, including the development of more advanced models and the creation of more comprehensive datasets specifically tailored for fake person detection.

A graph of CNN Model training and validation accuracy is shown in Figure 3.

Another critical area for future exploration is the integration of interpretable AI techniques in order to enhance transparency and trust in model decision-making. Through real-world testing and collaboration with experts in cybersecurity, we aim to further refine these models and ensure their reliability for practical application. This research contributes significantly to our understanding of the performance of neural networks in fake person detection, laying the groundwork for future innovations and developments in this significant field.

A. Future Directions

Future directions for this research on fake person detection include the development of more advanced neural network architectures that are better suited to handling the diversity and complexity of synthetic identities. Integrating state-of-the-art tools and resources for implementing these models on websites and applications will be essential to demonstrating their practical utility. Creating extensive, publicly available datasets tailored for fake person detection will enhance the training and testing processes. Explaining AI techniques used to increase transparency and build trust in model decisions could also be significant. Conducting real-world tests and collaborating with cyber security experts can help refine the models and ensure they are robust in real-life scenarios.

V. CONCLUSION

Identity fraud detection is crucial in the fields of AI and cybersecurity.These fraudulent identities pose a threat to digital security, leading to fraud, misinformation, and cyberattacks.Effective identity fraud detection techniques are essential for securing digital platforms such as social media, financial systems, and political processes. They help enhance digital trust by preventing fraud and protecting personal data. However, with the rapid advancement of AI, identity fraud has become increasingly challenging. This requires the development of more advanced methods to protect personal information and prevent financial losses. Our study focused on developing and testing neural network models, including convolutional neural networks (CNNs) and residual neural networks (ResNets), to address the issue of identity fraud. These models were trained on a dataset containing real-world examples of fraudulent identities. The results showed promising accuracy in detecting fake identities, indicating the potential of these models for combating identity fraud.We used the Kaggle dataset to evaluate the performance of models based on accuracy and error metrics, but we did observe some

overfitting during training. Despite these advances, current systems still face significant challenges, as existing datasets are not able to fully capture the variety of fraudulent identities, limiting the accuracy of detection. To improve transparency and credibility, it is necessary to develop advanced models and more interpretable AI techniques. Future research should focus on testing in real-world scenarios and collaborating with cybersecurity experts to improve models' practical reliability. Our research provides valuable insights into neural network model strengths and weaknesses, setting the stage for future innovations in facial recognition technology.

References will be added automatically by using the following lines. Add the relevant citations in the attached bibliogrpahy.bib file. Get help from me where you want to work on citations.

References

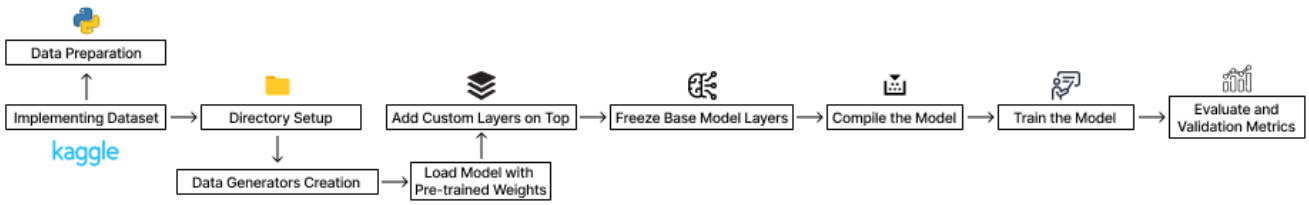

Fig. 1. The figure illustrates the comprehensive workflow for developing and evaluating a machine learning model using a dataset from Kaggle.

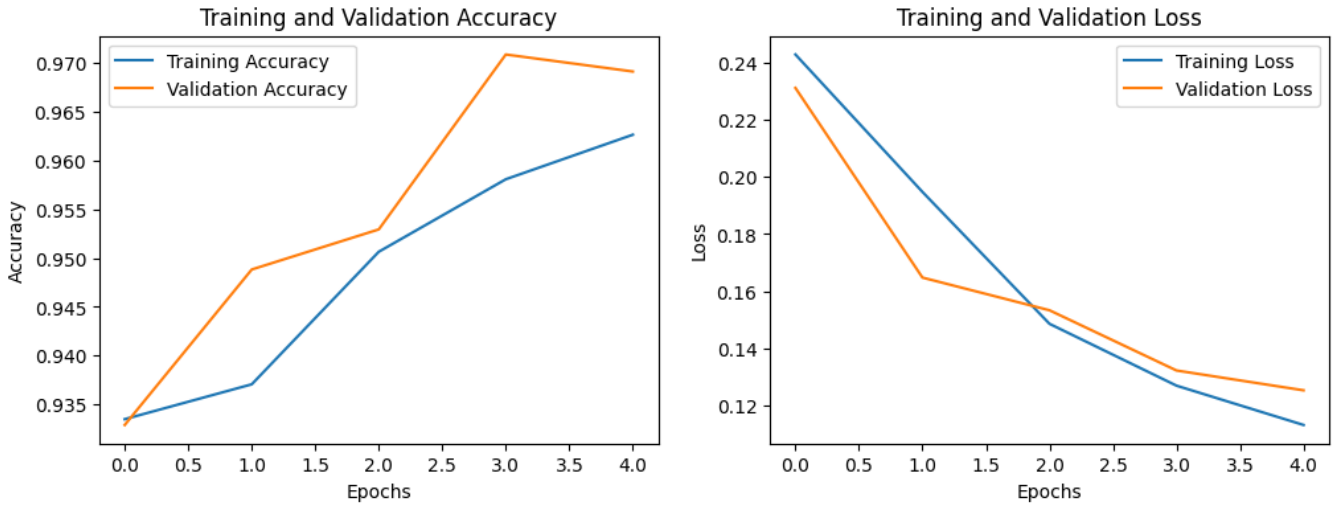

Fig. 2. The figure presents the training and validation performance of the CNN model over five epochs, depicting accuracy and loss metrics.

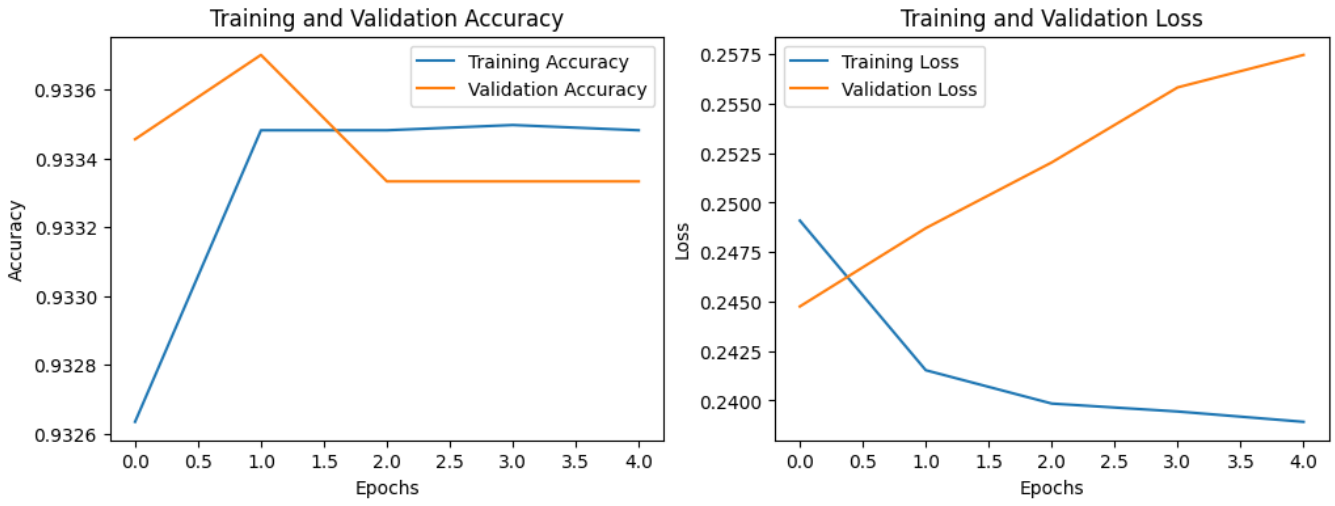

Fig. 3. The figure presents the training and validation performance of the ResNet model over five epochs, depicting accuracy and loss metrics.

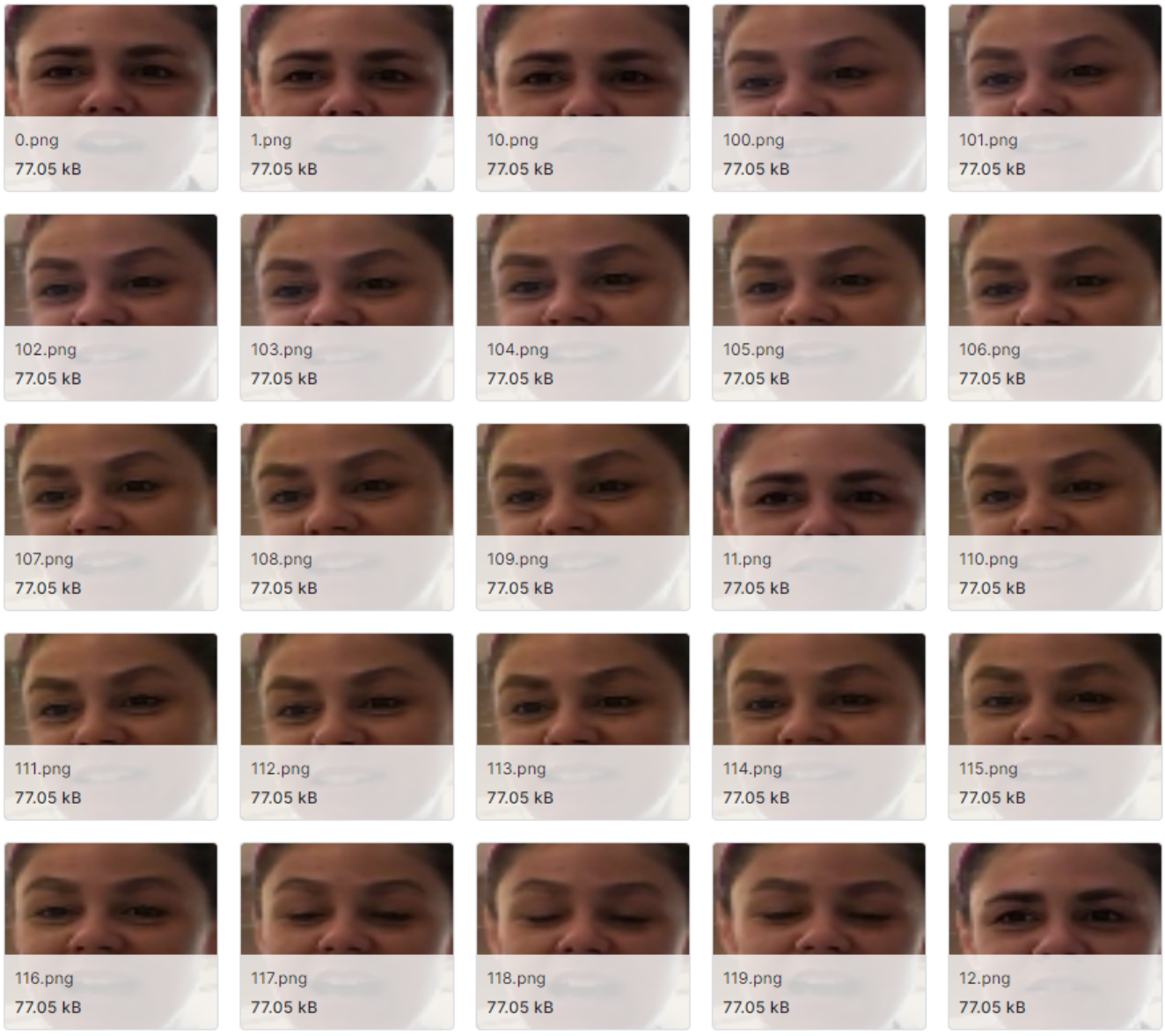

Fig. 4. The figure illustrates a sample of images from the dataset used for training and validating the models. Each image represents a facial close-up, likely utilized for tasks such as facial recognition or expression analysis