Detecting Malicious Attacks in Smart Power Grids: A Machine Learning Approach

Alyssa Traina, Salma Aboelmagd and Abdulrahman Takiddin

Introduction

With the rapid growth of Machine Learning comes a major push for modern technical systems to increasingly rely on AI-driven solutions to enhance data security and integrity. This includes smart power grid systems, where energy consumption data is vulnerable to manipulation by malicious users. These users may alter their energy usage records, leading to data inconsistencies and financial discrepancies for power providers. This process is also known as false data injection. One solution to this issue involves leveraging machine learning models to detect anomalies in user consumption patterns and classify suspicious behavior.

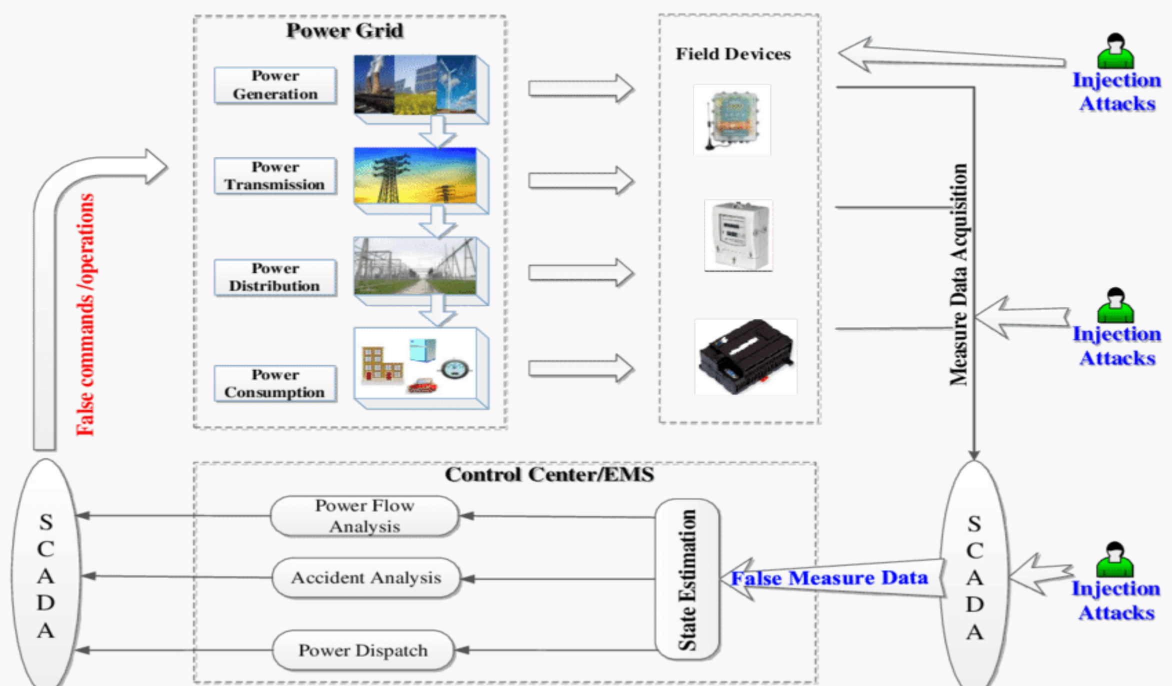


Figure 1: Shows a False Data Injection (FDI) Attack

Methods

• *Data Collection:*
A sample dataset from the 2009–2010 Irish Smart Metering Trials was used to test machine learning models. The data contains user energy consumption behavior at 30-minute intervals collected from different users which provided a basis for benign samples. Simulated attack functions were performed on random user energy consumption data and a column was added to the dataset to label the benign data with '0' and attack data with '1'.

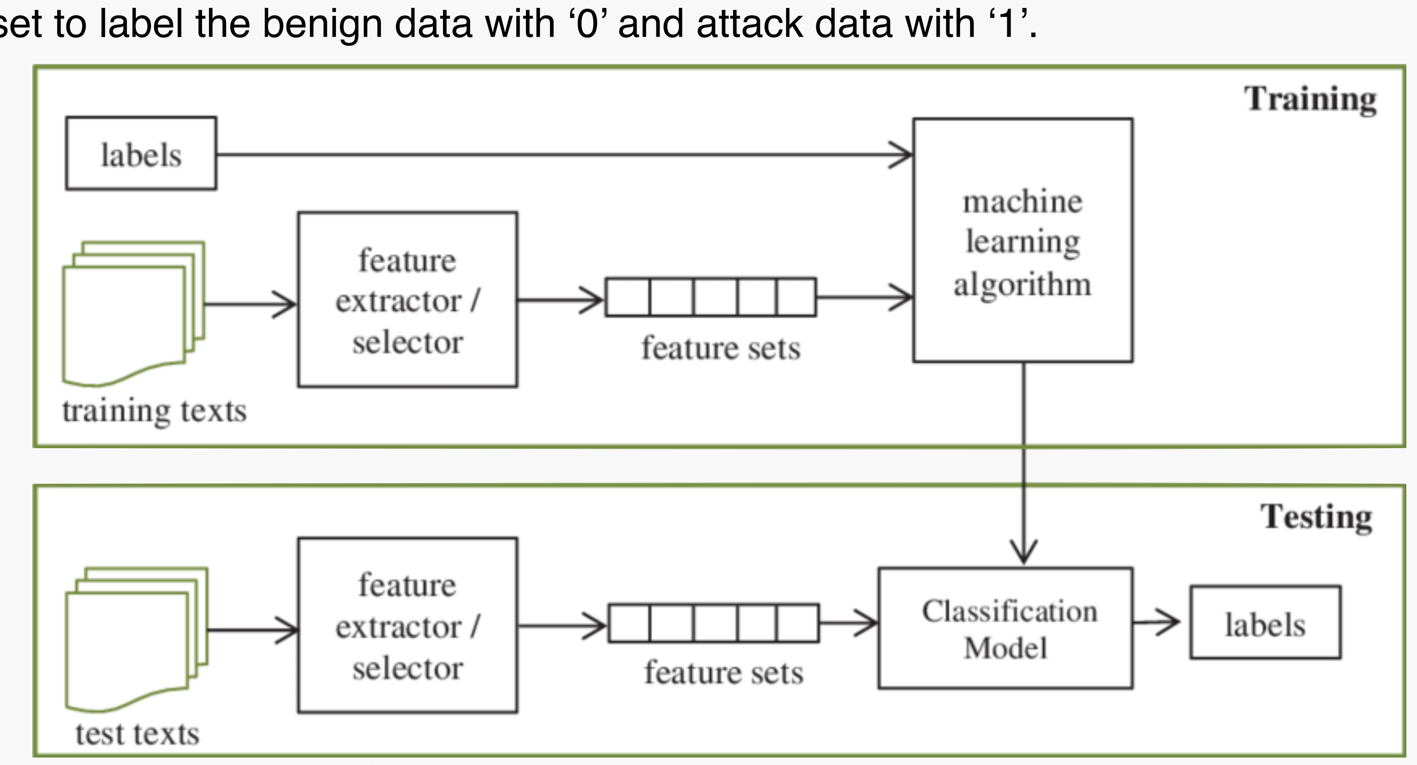


Figure 2: Shows the general procedure during the training and testing phases.

• *Shallow Learning*

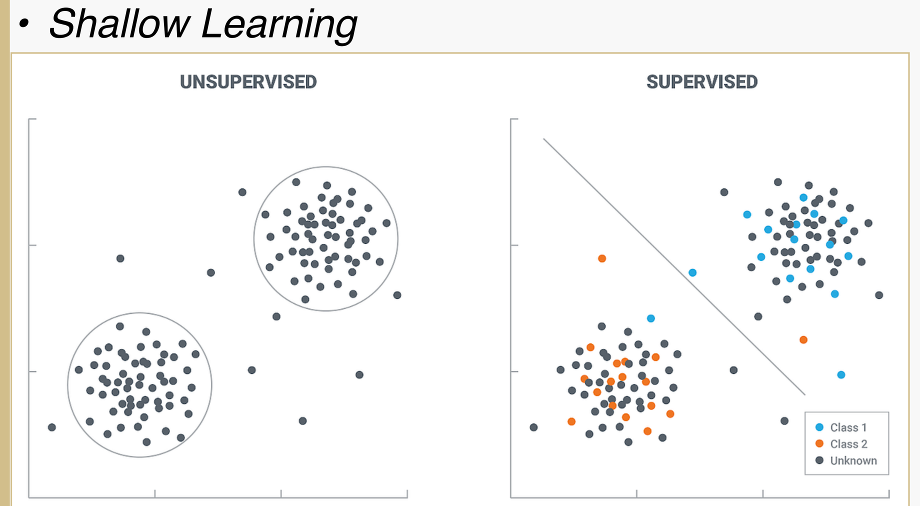


Figure 3: Models the difference between unsupervised learning and supervised learning classification algorithms.

• *Deep Learning*

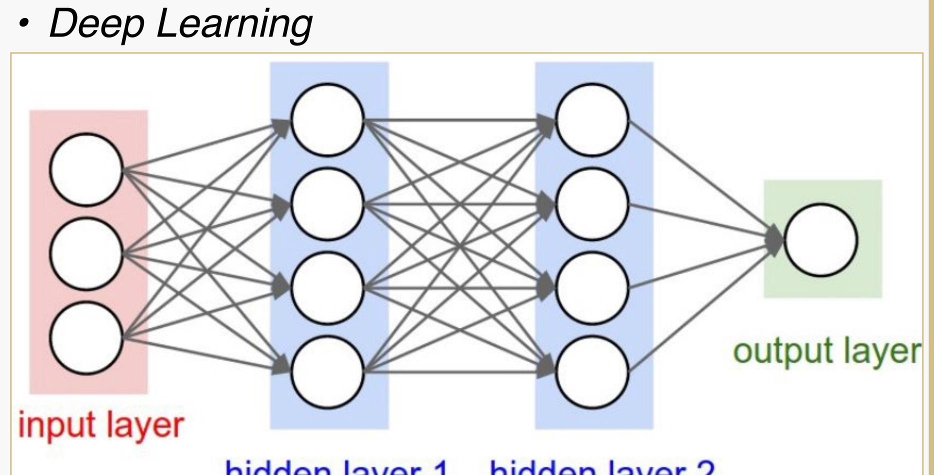
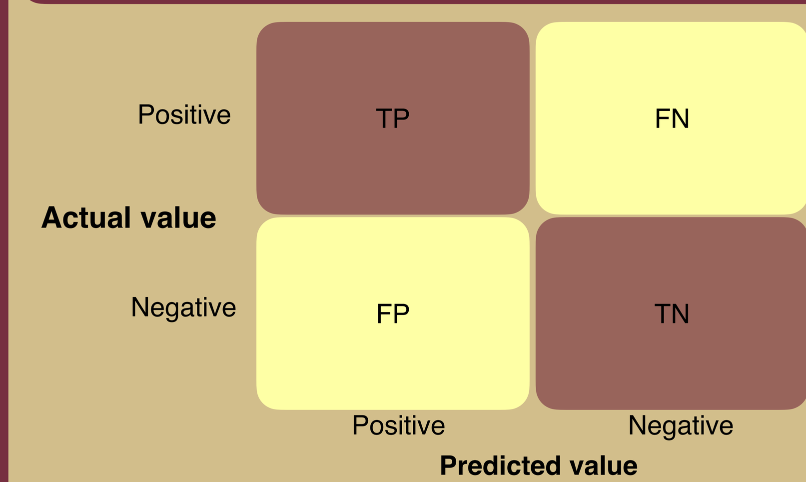


Figure 4: Models how a deep learning model processes data. Input cycles through several layers of the model before a final output "decision" is given.

Evaluation Metrics



Detection Rate: $TP/(TP + FN)$

False Alarm Score: $FP/(FP + TN)$

Figure 5: Shows a Confusion Matrix.

Results

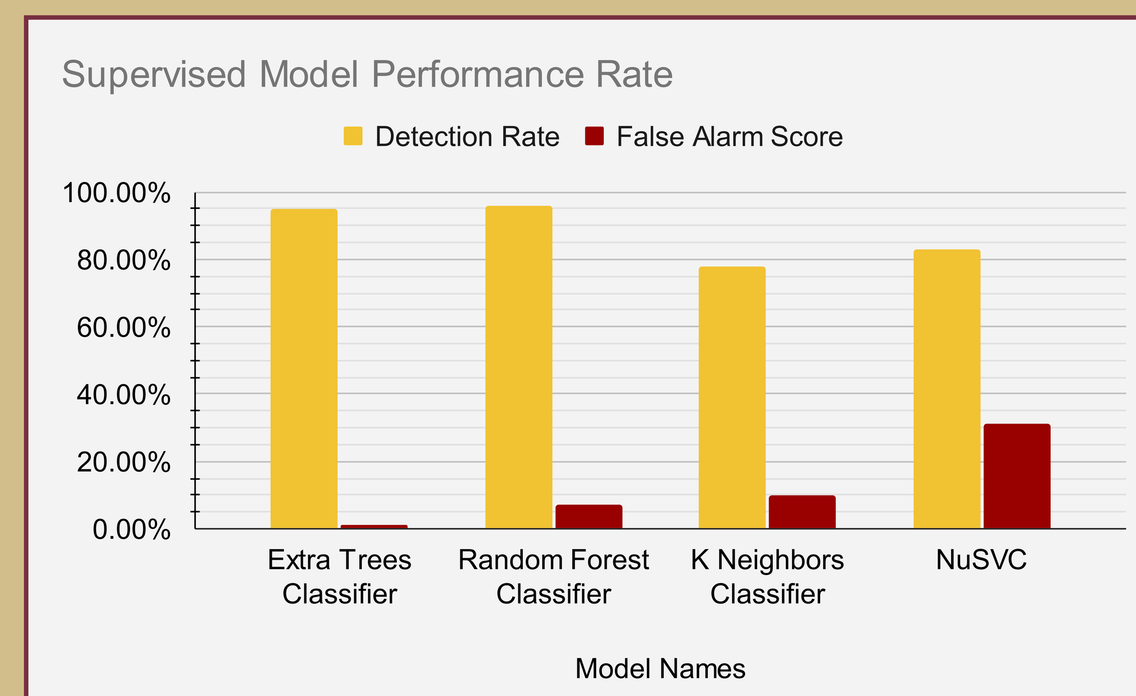


Figure 6: Shows the detection rate and false alarm scores for supervised learning models.

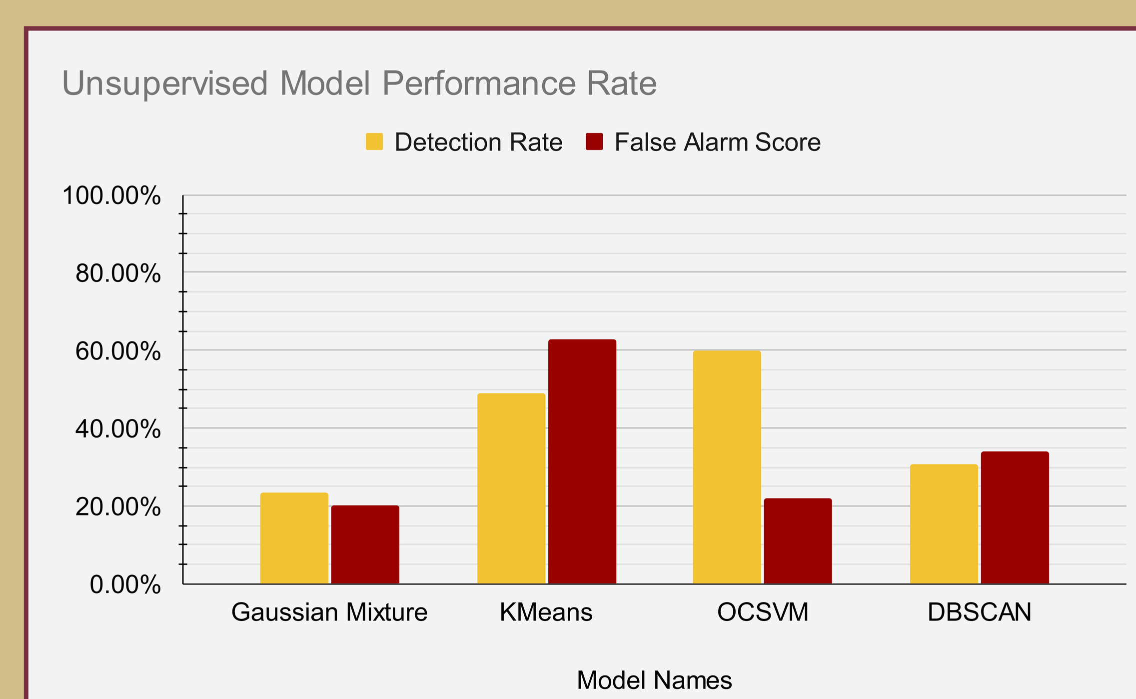


Figure 7: Shows the detection rate and false alarm scores for unsupervised learning models.

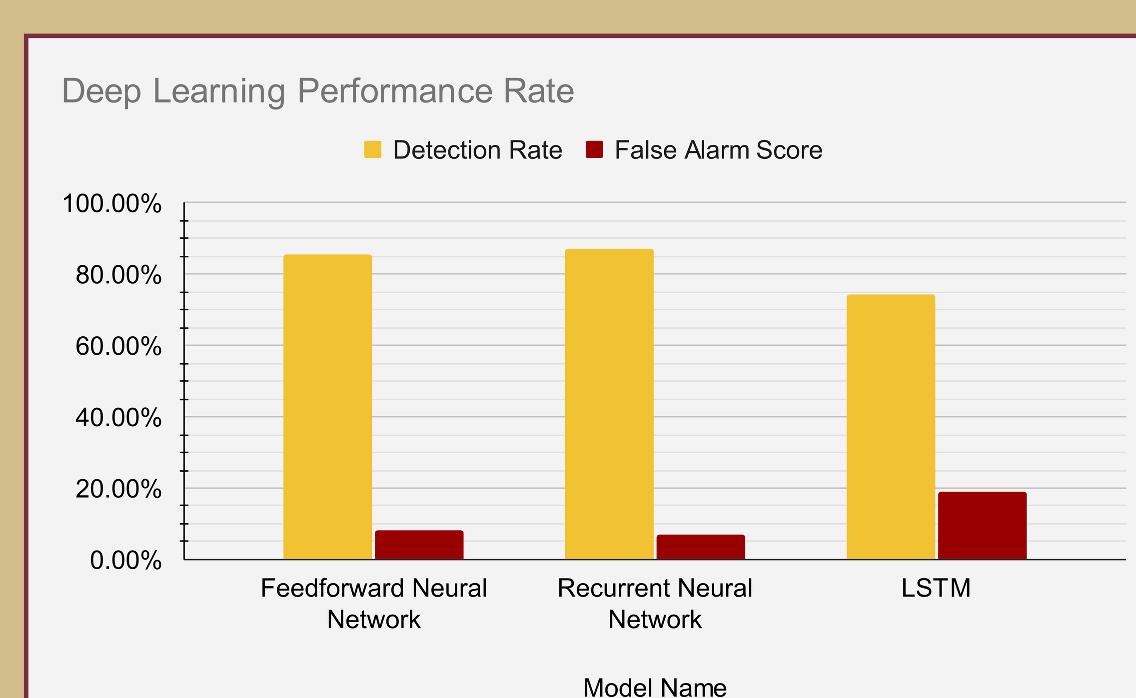


Figure 8: Shows the detection rate and false alarm scores for deep learning models.

Conclusion & Future Implications

For the shallow models, supervised learning models performed best due to their ability to train on labeled data with fewer parameters, reducing overfitting and capturing straightforward patterns. In contrast, unsupervised learning struggled with anomaly detection due to the absence of labels and the need for a threshold value to determine malicious data points. This led to difficulty determining strong clusters of benign data points during training and failure to distinguish between classes during testing. Deep learning underperformed compared to shallow learning, as the simple dataset led to overfitting and high sensitivity to parameters. Training times were also much higher because these models have more layers for data to travel through before a decision is output. Future research should focus on deep learning for its superior feature detection in complex datasets, which mimics real-world energy consumption data, with an emphasis on hyper-tuning parameters.

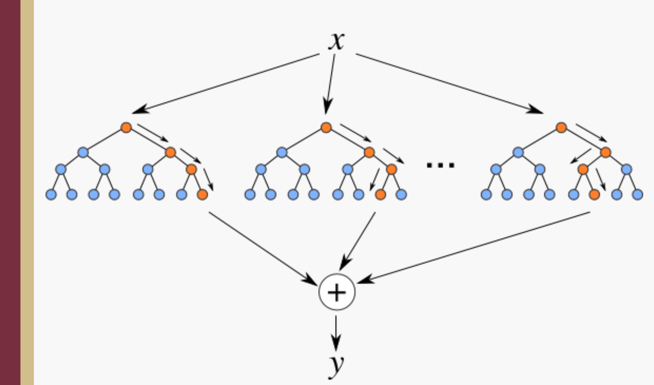


Figure 9: Random Forest Classifier

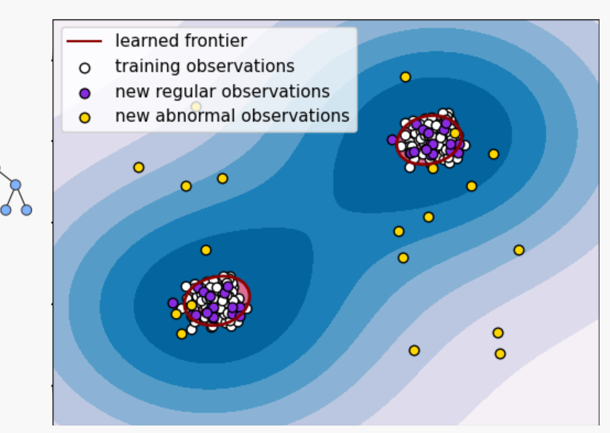


Figure 10: One Class SVM

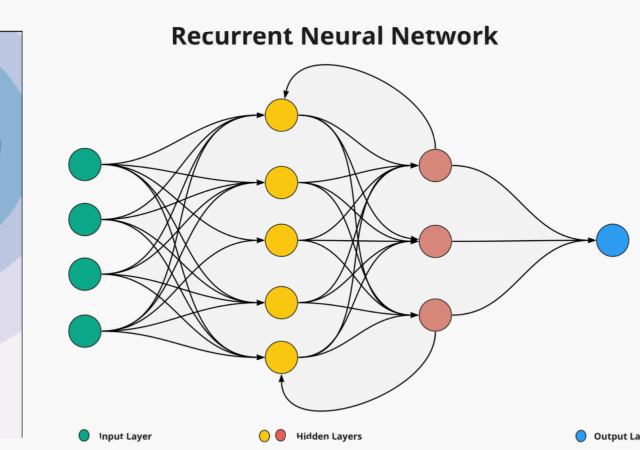


Figure 11: Recurrent Neural Network (RNN)

Acknowledgements

I would first like to thank my research mentors Dr. Abdulrahman Takiddin and Salma Aboelmagd for allowing me to play a role in this research. Their support throughout the process has provided me with a profound learning experience and an excitement towards this field of research.

Our work could not have been completed without the excellent computer lab provided by the Cyber-Physical Machine Learning Lab. Their resources allowed us to utilize the enhanced computational power necessary to obtain efficient results.

I would also like to acknowledge my UROP mentors Lily Dennis and Alexis Staveski for guiding me throughout the process of my research and the development of my presentation. They have provided excellent feedback on this project and significant encouragement throughout my research.

Being a student in UROP has been a rewarding experience that has strengthened my critical thinking and research skills which will allow me to make significant contributions in the future of science.

References

1. A. Ali, M. Mokhtar and M. F. Shaaban, "Theft Cyberattacks Detection in Smart Grids Based on Machine Learning," 2022 5th International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Cairo, Egypt, 2022, pp. 1-4, doi: 10.1109/ICCSPA55860.2022.10019036.
2. A. Takiddin, M. Ismail, U. Zafar and E. Serpedin, "Deep Autoencoder-Based Anomaly Detection of Electricity Theft Cyberattacks in Smart Grids," in IEEE Systems Journal, vol. 16, no. 3, pp. 4106-4117, Sept. 2022, doi: 10.1109/JSYST.2021.3136683.
3. "Irish Social Science Data Archive," UCD Library. [Online]. Available: http://www.ucd.ie/issda/data/commissionforenergyregulationcer/
4. M. Ezeddin, A. Albaseer, M. Abdallah, S. Bayhan, M. Qaraqe and S. Al-Kuwari, "Efficient Deep Learning Based Detector for Electricity Theft Generation System Attacks in Smart Grid," 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE), Doha, Qatar, 2022, pp. 1-6, doi: 10.1109/SGRE53517.2022.9774050.

Figures