

TIME SERIES ANALYSIS : FAKE IMAGE DETECTION

Afiya Irfan Mulla¹, Danish Mukhtar Shaikh², Dr Rakhi Gupta³, Nashrah Gowalkar⁴

^{1,2}Student, Master of Science in Information Technology, Kishinchand Chellaram, HSNC University, Mumbai, India

³Head of IT Department, HSNC UNIVERSITY Mumbai, India.

⁴Asst Professor, IT Department HSNC University Mumbai, India.

DOI: <https://www.doi.org/10.58257/IJPREMS36865>

ABSTRACT

Fake image detection is a rapidly growing area for research to protect against misleading information as nowadays the spread of fake images on social media platforms is increasing rapidly which threatens the security of individuals and businesses. In this research an important aspect of fake image detection that the paper discusses is “Time Series Analysis”. This technique inspects how information or activity changes over time, the robustness of this technique is discussed and how it plays a vital role in fake image detection. This research will be a valuable resource for researchers functioning on fake image detection. This paper concludes that time series analysis helps to detect unusual patterns that can indicate when fake images are being used , making it a valuable tool for fake image detection.

Keywords: — Time Series Analysis, Fake Image Detection, GANs, Deep Learning, Image Processing, Temporal Analysis, Sequential Data, Anomaly Detection, AI, Machine Learning.

1. INTRODUCTION

Fake Image detection appears to a critical filed in computer vision with extensive application in media , digital forensic and security. Techniques such as Deepfakes and GANs (Generative Adversarial Networks) to an increasing extend ,the need for comprehensive method to identify forged images becomes vitally important. By leveraging temporal patterns in image series, the study proposes a methodology for analyzing features that distinguish between real and fake image sequences. The results indicate that time series methods can effectively highlight inconsistencies in fake images that are not visible in single-frame analysis.

1.1PURPOSE: Time series analysis checks the consistency over time of how the images are manipulated , for example change in pixel should follow natural or expected patterns. To explore the use of time series analysis in detecting fake images. To identify and model temporal patterns that distinguish real from GAN-generated images. To evaluate the performance of time series-based methods against conventional image detection models. To develop a framework for analyzing image sequences for anomalies. To propose improvements in the detection of advanced fake images using temporal and sequential data.

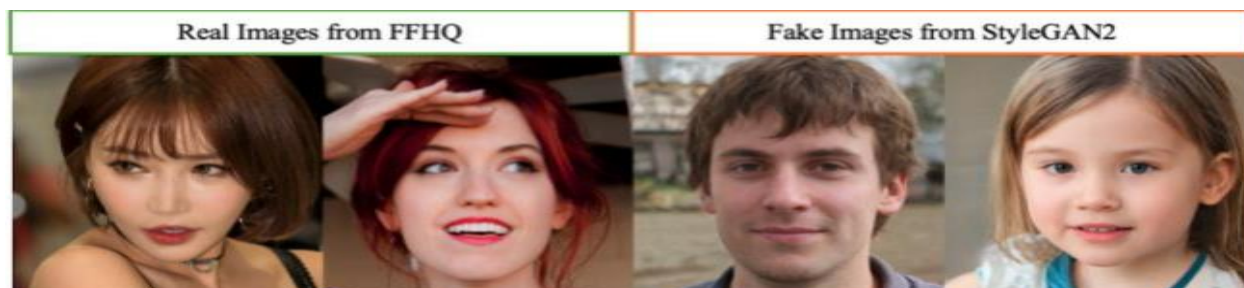


Figure :- Two Real Images From Ffhq (Karras, Laine And Aila 2019(Left) [7]And Two Fake Images From Style – Gan2 (Karras Et Al. 2020) (Right) [8]

2. LITERATURE REVIEW

A survey of detection and mitigation of fake images done by Dilip .S states that Fake image detection is a classification problem. The final output is identifying whether the image is fake or not. The process starts with gathering various types of tampered images manipulated using single or multiple alterations and then, after processing, classifying them as real or false. The fake image detection process at a high level comprises handcrafted feature sets and self-learning neural networks. A fake image detection workflow using handcrafted features. Initially, a set of tampered images is collected. Then, each image may undergo pre-processing activity, like gray scaling and cropping. In the feature extraction phase, various image features are extracted relating to the image. These features can be device-specific, image intrinsic, or semantic/statistics characteristics of an image. Forensic methods use handcrafted intrinsic features of images, while other methods use other characteristics. Feature preprocessing may or may not be applied to reduce features to achieve

computational efficiency. [1] The field of fake image detection has evolved significantly with advancements in deep learning, especially the emergence of GANs. Several traditional and modern approaches have been explored to combat the generation of fake images. According to Goodfellow et al. (2014), GANs work by using two neural networks the generator and the discriminator—in a competitive manner, which results in high-quality image outputs. This makes detecting fake images a challenging task for standard detection methods that rely on pixel-level analysis.[2] A notable study by Marra et al. (2019) emphasizes the limitations of static image-based detection methods. They suggest that temporal inconsistencies in image sequences can be exploited to identify GAN-generated content. Similar work by Hu et al. (2020) explores the use of frequencydomain analysis to reveal unnatural patterns in fake images. These studies highlight the potential of moving beyond single-image analysis and incorporating temporal features.[3] Research into time series analysis for images is relatively scarce but promising. Time series approaches like AutoRegressive Integrated Moving Average (ARIMA), Long Short-Term Memory (LSTM), and Hidden Markov Models (HMMs) have been used extensively for forecasting and anomaly detection in other domains (Box et al., 2015). Implementing these methods in fake image detection is a novel concept that this study aims to investigate.[4]

3. METHODOLOGY

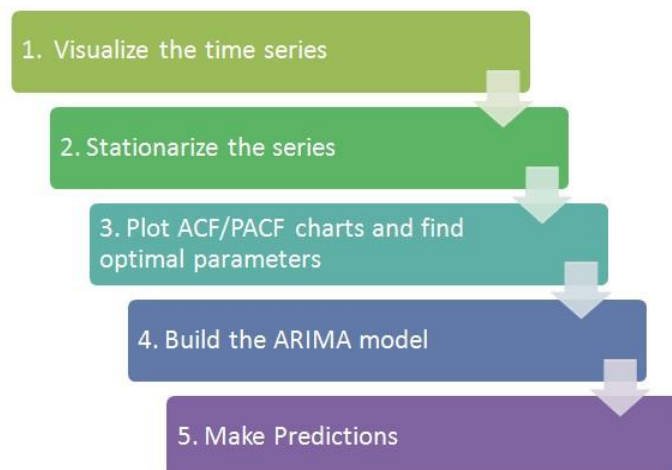
The research employs a combination of quantitative and qualitative methods to explore the effectiveness of time series analysis for detecting fake images. In the context of Time series analysis here we have studied the following two algorithm and how useful these algorithms are :

1. Long Short-Term Memory (LSTM) Networks LSTM networks are a type of recurrent neural network (RNN) that are particularly effective for sequence prediction problems. They can learn from the temporal dependencies in data, making them well-suited for time series analysis. Application: In fake image detection, LSTMs can analyze sequences of images or the changes in image features over time. For example, they can track changes in pixel intensity or color distribution to identify anomalies that may suggest manipulation.

2. Dynamic Time Warping (DTW) DTW is a technique used to measure similarity between two temporal sequences that may vary in speed. It aligns sequences in a non-linear way, allowing for flexible matching. DTW can be applied to compare sequences of image features over time. For instance, it can be used to detect discrepancies in a sequence of images that are supposed to depict a continuous event, highlighting any alterations or anomalies.

Feature	LSTM Networks	Dynamic Time Warping (DTW)
Type	Deep learning (RNN)	Classical algorithm
Data handling	Large datasets, raw sequences	Smaller datasets, predefined features
Learning process	Supervised learning (training)	Non- learning(direct comparison)
Feature Extraction	Automatic feature learning	Requires prior feature extraction
Computational Complexity	Higher, especially with training	Lower for small sequences, quadratic for long ones
Output	Predictions/classification	Similarity scores

A.Comparison Between Long Short-Term Memory (Lstm) Networks And Dynamic Time Warping (Dtw)



TIME SERIES ANALYSIS FLOW CHART [6]

4. RESULTS AND DISCUSSION

The research presents a timely and relevant exploration of using time series analysis to enhance fake image detection, addressing a critical issue of digital forensics, media integrity, and security. The paper effectively argues for the integration of temporal analysis into the detection methodologies traditionally dominated by static image evaluations. LSTM networks and Dynamic Time Warping (DTW) showcases a robust methodological framework. Both algorithms are well-justified:

- **LSTMs** can recognize temporal dependencies in sequences, which is essential for identifying subtle anomalies across frames.
- **DTW** provides a means of aligning sequences in a flexible manner, making it suitable for detecting alterations in time-varying data.

5. CONCLUSION

The research demonstrates that time series analysis provides a promising approach to detecting fake images, particularly when analyzing sequential data. While traditional static methods are limited in their ability to capture temporal anomalies, time series models such as LSTM can effectively identify irregular patterns in GAN-generated sequences. By incorporating temporal features, this methodology can enhance the accuracy of fake image detection and offer a robust framework for future developments in this domain.

6. REFERENCES

- [1] A Survey of detection and mitigation for fake images on social media platforms , Dilip Kumar Sharma¹;Bhuvanesh Singh² ; Saurabh Agarwal³;Lalit Garg⁴; Cheonshik Kim⁵; and Ki-Hyun Jung⁶ , Oct 2023 Available: <https://www.mdpi.com/2076-3417/13/19/10980>
- [2] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. Advances in neural information processing systems, 27. Marra, F., Gragnaniello, D., Cozzolino, D., & Verdoliva, L. (2019)
- [3] Detection of GAN-generated fake images over social networks. 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 384-389.
- [4] Hu, S., Li, W., Zhang, W., & Jiang, X. (2020). Exposing GAN-generated fake images with frequency analysis. IEEE Transactions on Pattern Analysis and Machine Intelligence, 43(3), 982-997.
- [5] Box, G. E. P., Jenkins, G. M., & Reinsel, G. C. (2015). Time series analysis: forecasting and control. John Wiley & Sons.
- [6] Samarth Vaish ,Nov 12,2019 Available at : <https://www.scribd.com/document/434533332/Time-series-analysisdocx>
- [7] Karras, T.; Laine, S.; and Aila, T. 2019. A style-based gen-erator architecture for generative adversarial networks. In Proceedings of the
- [8] IEEE/CVF conference on computer vi-sion and pattern recognition, 4401-4410. Available at : https://openaccess.thecvf.com/content_CVPR_2019/papers/Karras_A_StyleBased_Generator_Architecture_for_Generative_Adversarial_Networks_CVPR_2019_paper.pdf
- [9] [etworks_CVPR_2019_paper.pdf](https://openaccess.thecvf.com/content_CVPR_2019/papers/Karras_A_StyleBased_Generator_Architecture_for_Generative_Adversarial_Networks_CVPR_2019_paper.pdf)
- [10] [8] Karras, T.; Laine, S.; Aittala, M.; Hellsten, J.; Lehtinen, J.; and Aila, T. 2020. Analyzing and improving the image qual-ity of stylegan. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 8110-8119.