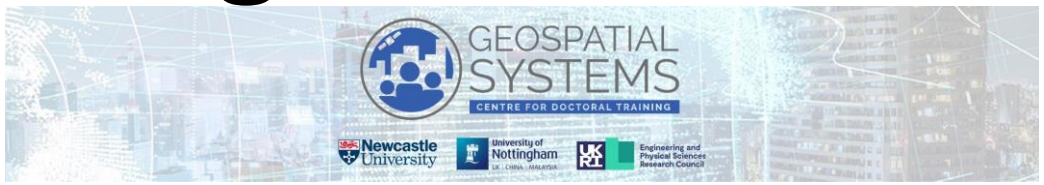
Context Aware Deepfake Detection for Satellite Images

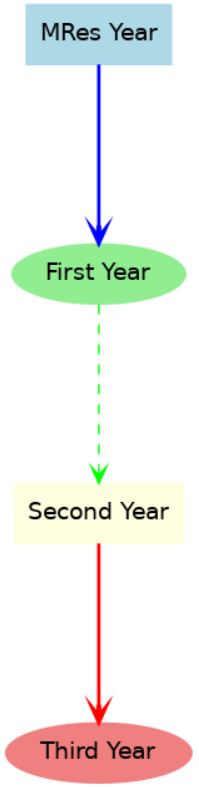
Matthew Chapman

Funder: Airbus Defense and Space

Geospatial CDT

Program



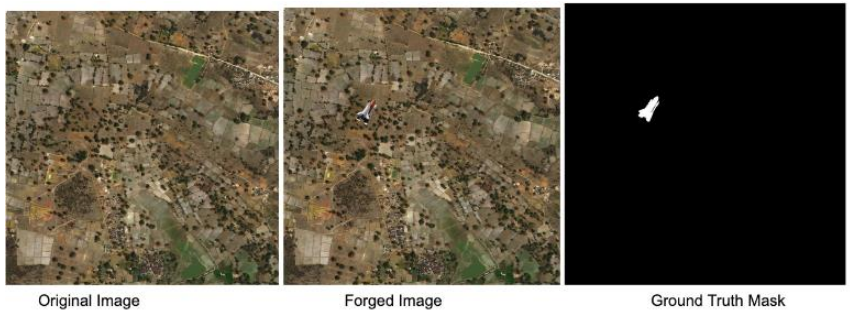


- 4-year program
- Includes an integrated MRes year
- Part of a joint CDT between Newcastle University and University of Nottingham

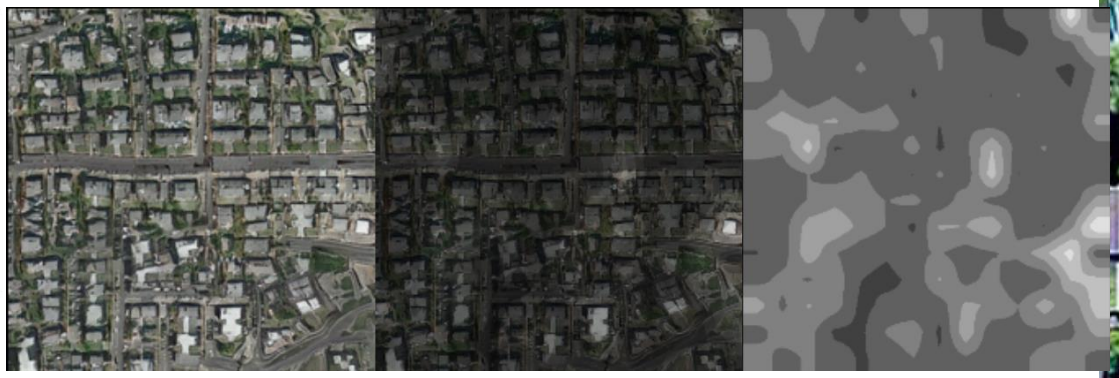
Current Research Question/Aims and Objectives

- The current research question is how can a robust and scalable methodology be developed for detecting and preventing maliciously manipulated images and artificially generated images.
- A suitable methodology will be created.
- A system will be created that follows the methodology.
- A dataset containing manipulated/synthetic satellite images will be created.

Types of Manipulation/synthetic image generation



Splicing Source:Dashlab

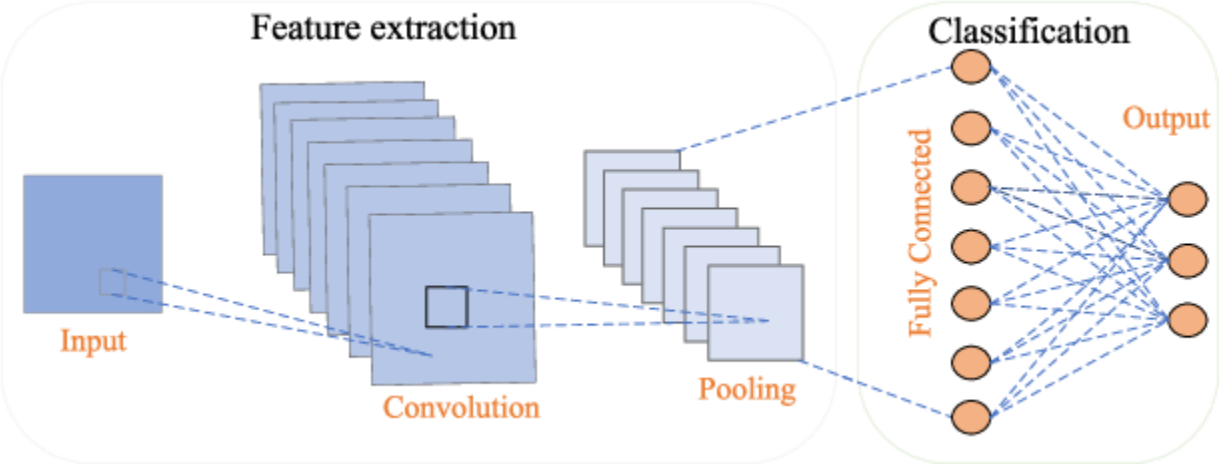


Generative Adversarial Network Source: DeepMedia.AI

Stable Diffusion

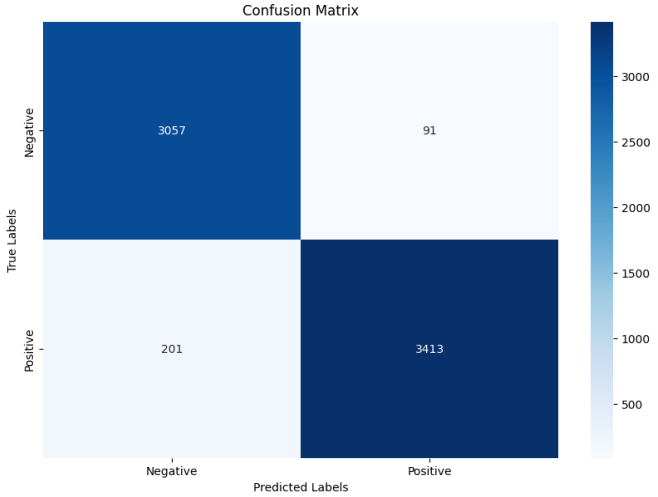
Challenges and Progress so far

- The main challenge so far is the lack of datasets of manipulated satellite imagery available
- Therefore, a new dataset will be created
- Literature review and research in progress
- Preliminary CNN network has been created and tested using existing CycleGAN data.



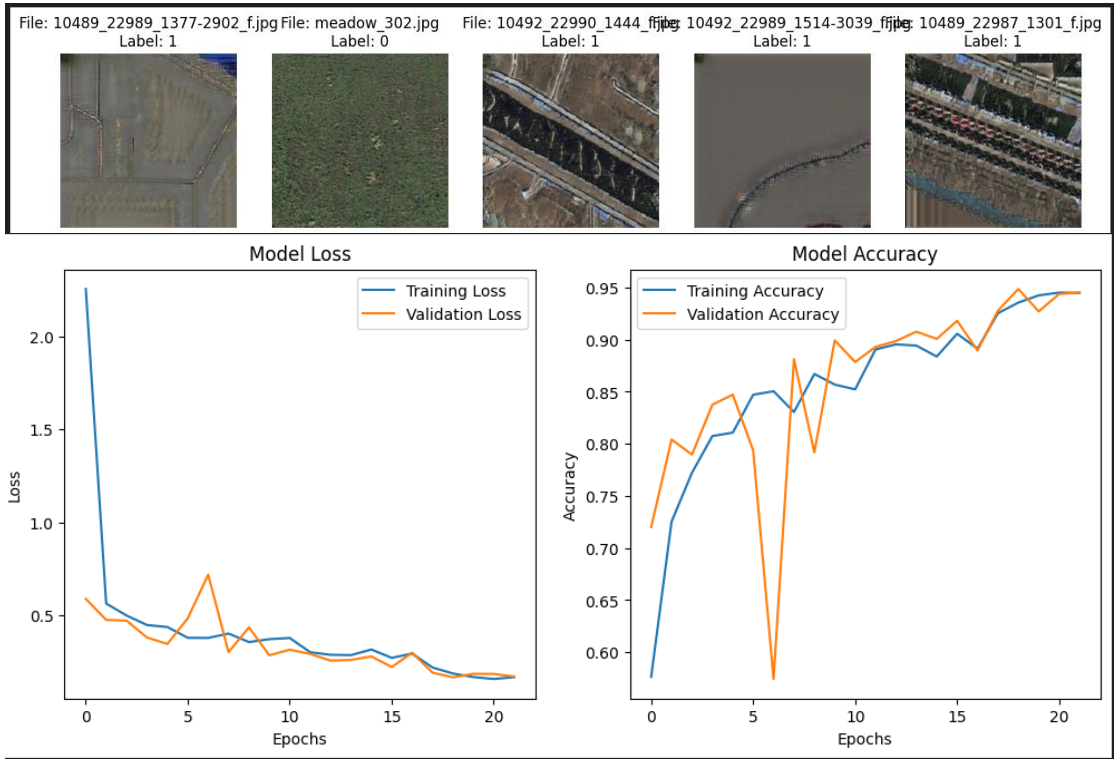
CNN Network Architecture and Performance

- The system was trained using CycleGAN Generated Images and RESIS45 feature detection dataset.



Layer No	Type of Layer	Neurons
1	Conv2D	64
2	MaxPooling2D	Na
3	Conv2D	128
4	MaxPooling2D	Na
5	Conv2D	256
6	MaxPooling2D	Na
7	Conv2D	512
8	MaxPooling2D	Na
9	Conv2D	1024
10	MaxPooling2D	Na
11	Conv2D	2048
12	MaxPooling2D	Na
13	Flatten	Na
14	Dense	912
15	Dropout	Na
16	Dense	1-Since its Binary Classification

	precision	recall	f1-score	support
0	0.94	0.97	0.95	3148
1	0.97	0.94	0.96	3614
accuracy			0.96	6762
macro avg	0.96	0.96	0.96	6762
weighted avg	0.96	0.96	0.96	6762



Future Work

- The establishment of a new state-of-the-art dataset. Likely utilizing stable diffusion
- A detection method that utilizes traditional textural detection methods alongside a CNN network.
- This system will allow for any modifications to be localized.