

# DL Major Report

M22CS061

**Title:** A Random CNN Sees Objects: One Inductive Bias of CNN and Its Applications

**Dataset:** Tiny Imagenet

## Summary of Paper:

- The inductive bias of CNNs, which is the inclination to automatically focus on objects, is referred to in this study as Tobias ("The object is at sight"). Surprisingly, a **randomly initialized CNN can localise objects properly without any prior learning**. The study demonstrates that activation functions like ReLU and network depth are critical for a random CNN to localise utilizing Tobias. This inductive bias may be used to improve item localization and recognition tasks by focusing the model's attention on important objects.
- Tobias self-supervised learning uses the **Tobias inductive bias to drive foreground and background separation**. This method significantly improves downstream tasks, especially for object detection. Experimental results show that Tobias is more robust to augmentation changes in pictures and consistently outperforms on training sets of different sizes.

## Code Implementation Results:

### Author code Result:

\*\*\*\*\*

0 images

images corLoc acc is 0.0

\*\*\*\*\*

1 val\_annotations.txt

val\_annotations.txt corLoc acc is 0.0

[0.0, 0.0]

uniform\_resnet50 random2

0.0

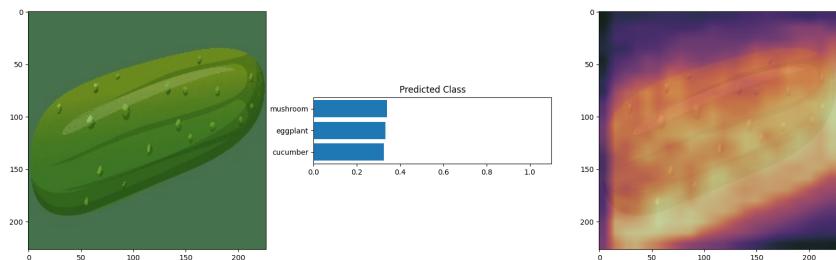
## Train Resnet 50 on different weights init and note accuracy:

(NOTE: Due to long training time on resnet50 on tiny imagenet i only train three model for 11 epochs however it took more than 1 and a half day)

Weights	Accuracy	Loss
Random	0.1236	0.6060
Xavier	0.0729	2.0302
He	0.0892	2.6769

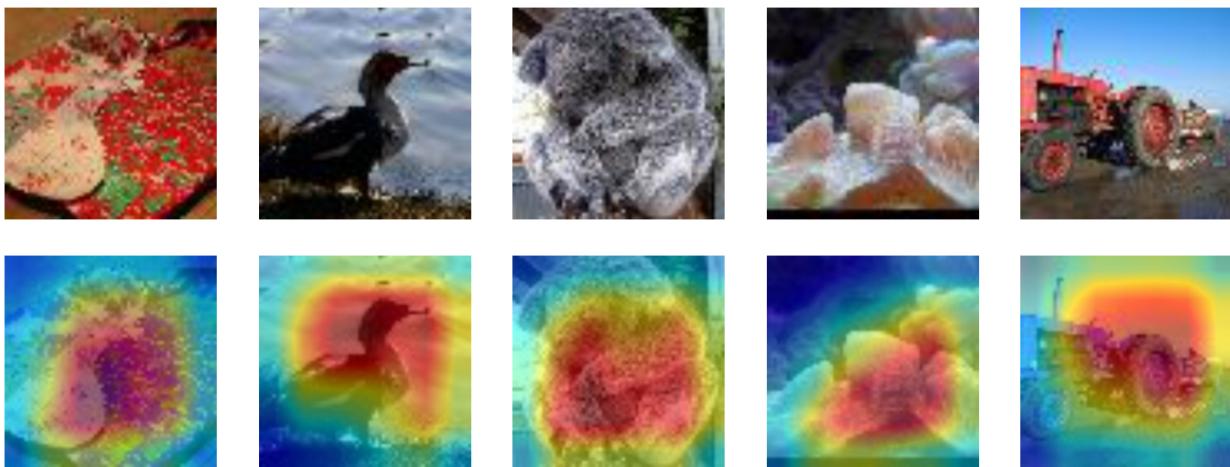
## Result of gradcam on different model:(self build)

Image grad cam on basic CNN with random image



Grad Cam of Resnet 50

On image net



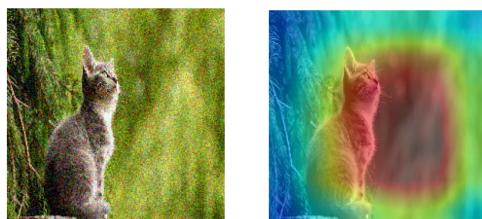
On Random image



On multi object image



On noisy image:

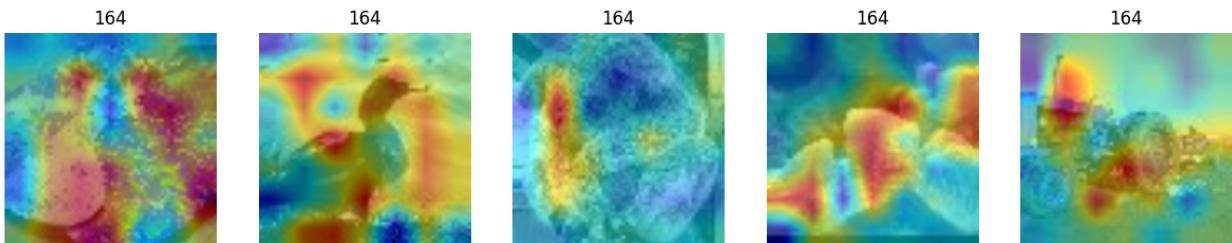


On Adversarial Patch image (**Enhancement**)



Grad Cam of MultiAttention Resnet 50 (**Enhancement**)

On image net



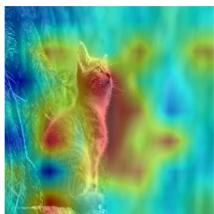
On Random image



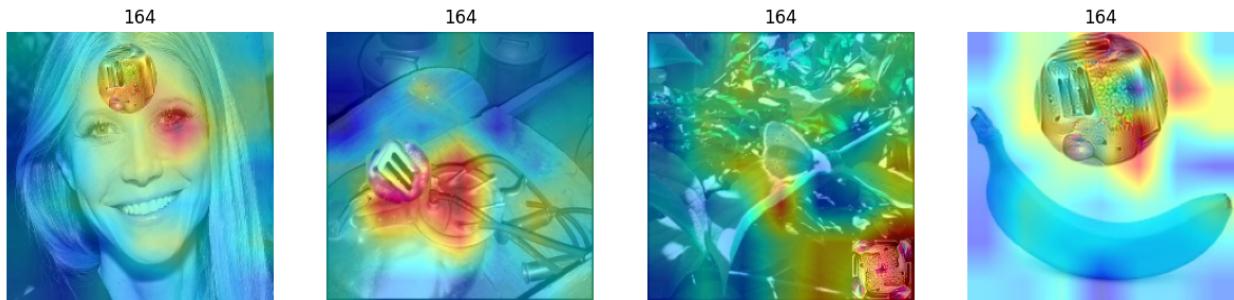
On multi object image



On noisy image



## On Adversarial Patch image (**Enhancement**)



### ChatGPT Answer about Enhancement:

**Ques:** It is proven that CNN can detect object from image without any training now it is possible it can detect object in adversarial patched images

**Ans:**

- **It is not accurate to say that a CNN can detect objects from images without any training.** In fact, training is an essential part of building a CNN. A CNN is a type of deep neural network that is trained on a large dataset of labeled images. During the training process, the network learns to extract features from the images and use them to classify objects.
- Regarding adversarial patch attacks, CNNs are vulnerable to such attacks. Adversarial patches are designed to deceive the CNN by adding a small patch to an image that **causes the network to misclassify** the image. These patches are created using optimization techniques that exploit the weaknesses of the CNN.
- To mitigate the effect of adversarial patches, researchers have developed various techniques such as adversarial training and defensive distillation. Adversarial training involves training the CNN on adversarial examples, while defensive distillation involves training a second network to detect adversarial examples.
- In summary, while CNNs are powerful tools for object detection, **they are not immune to adversarial attacks**, and researchers are actively developing techniques to improve their resilience to such attacks.

**Ques:** can multi attention can do it?

**Ans:**

- Multi-attention is a technique used in deep learning to improve the performance of neural networks on tasks such as object detection, image captioning, and machine translation. Multi-attention allows the network to selectively focus on different parts of an input by weighting the importance of each part.
- While multi-attention can help improve the performance of a neural network, it is not a solution to the problem of adversarial attacks. Adversarial patches are

designed to deceive the network by exploiting its vulnerabilities, and they can be effective even against networks that use multi-attention.

- However, researchers have proposed various techniques that use multi-attention to improve the resilience of neural networks to adversarial attacks. For example, some studies have shown that incorporating multi-attention into the training process can improve the robustness of the network to adversarial examples.
- In summary, while multi-attention is a powerful technique that can improve the performance of neural networks, **it is not a silver bullet for the problem of adversarial attacks**. Nevertheless, incorporating multi-attention into the training process can help improve the resilience of neural networks to such attacks.