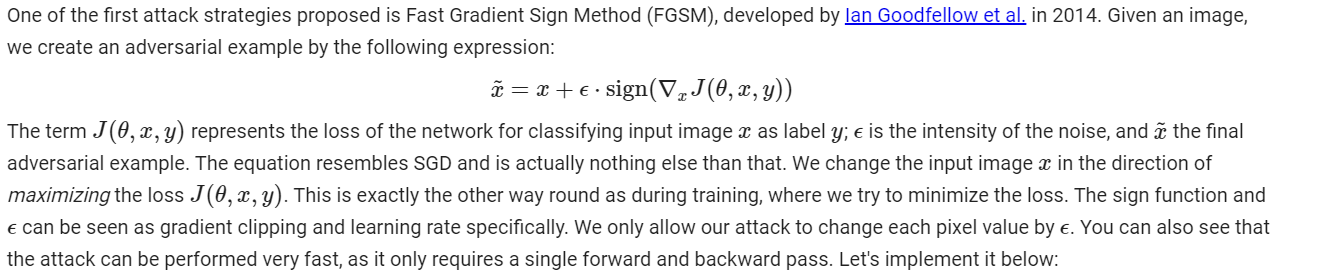
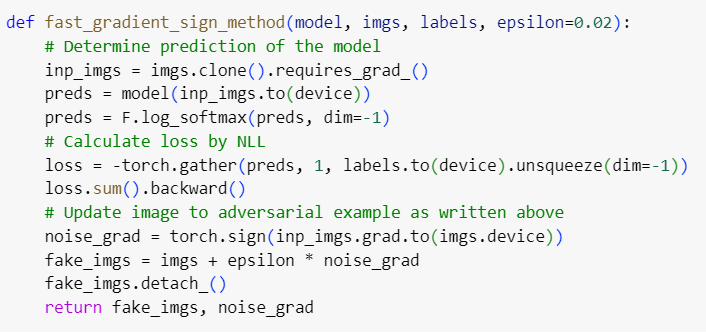
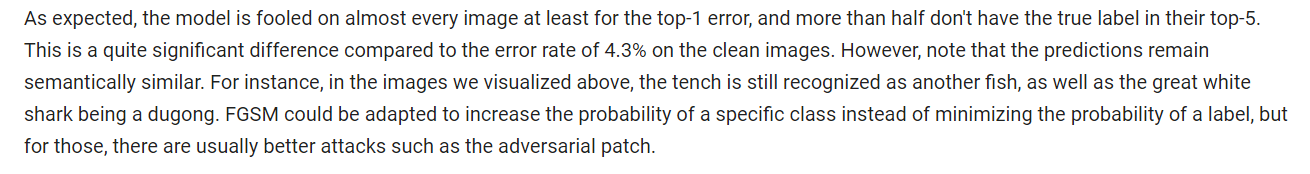
**White box attack**- Where the attacker is aware of the weights and gradients of the model.

**Black box attack**-Where the attacker is unaware about the model . So the attacker needs to change the pixels of the image only and find out .

Fast Gradient Sign Method (FGSM)

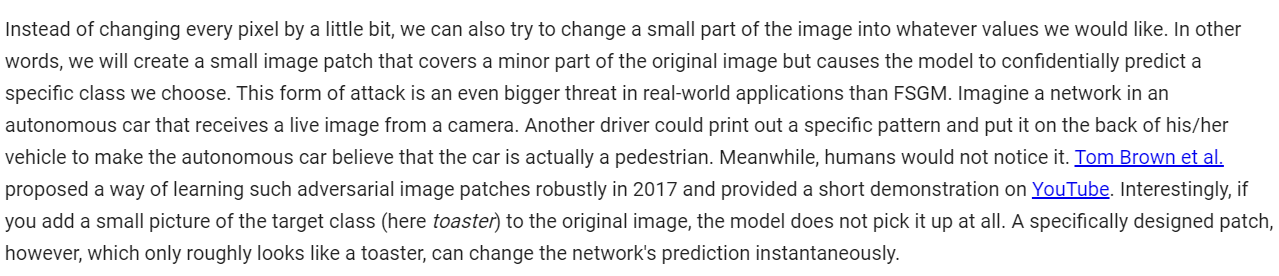


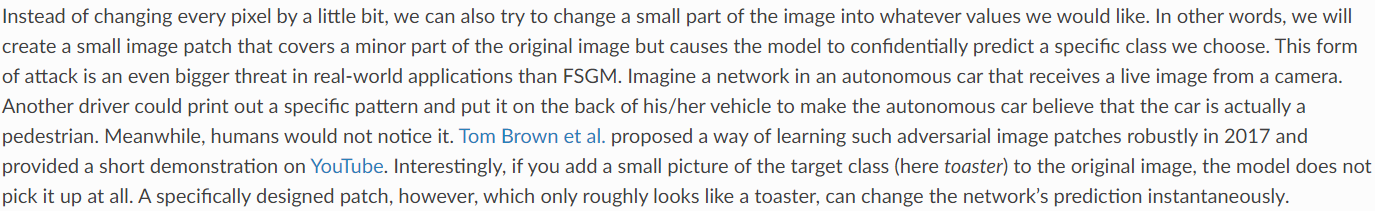


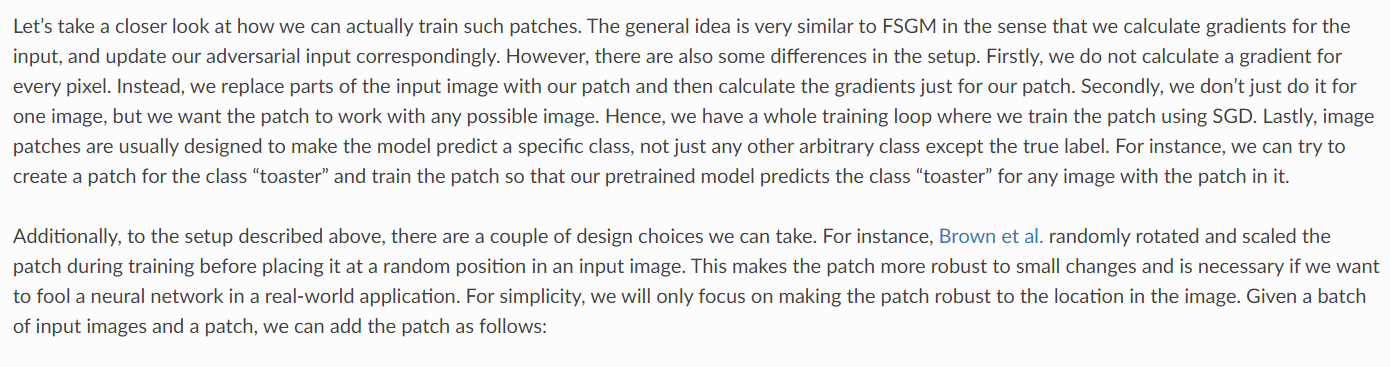
**FGSM-chatgpt[https://chatgpt.com/share/b5e90ed4-f73d-456d-b1bc-bda5ef475a67]**

**Adversarial network[https://chatgpt.com/share/221cfffe-6d76-4f8d-9db3-d0fd0a4cd18d]**

**ADVERSARIAL PATCHES**

****

****

****