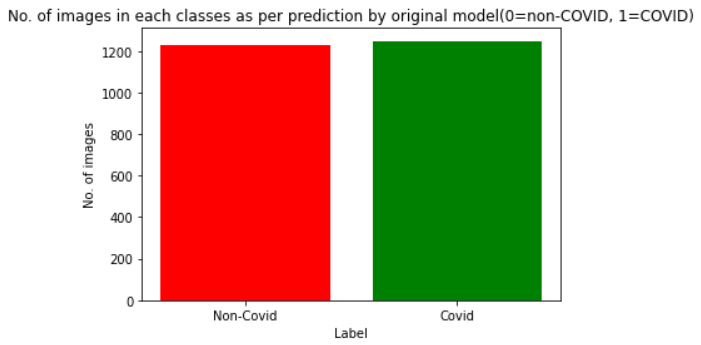
**1. BBA, PGD, COVID**

Attacker’s model = VGG16 of similar type as the original model trained on SarsCov2 Dataset from Kaggle (same as the original model)



Epsilon = 1.4

alpha = eps/10

Maximum iterations = 10 (stops when loss reaches 10^-5 or max iter, whichever is earlier)

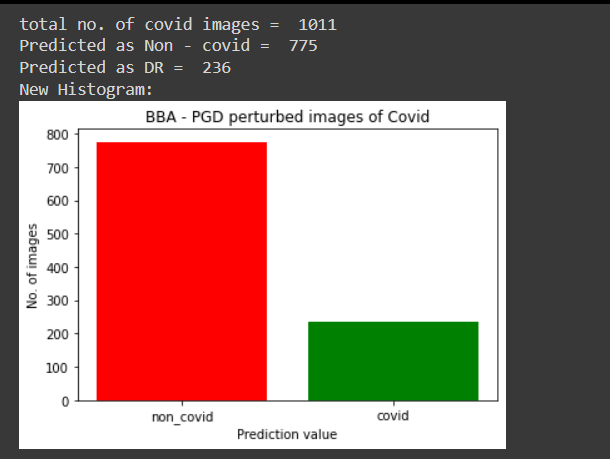
Total images = 1984

Perturbed images are created on 80% of the original dataset using the attacker’s model and the images are run through the original model to find the predicted value

Total perturbed covid images = 1011

Predicted as Covid = 236

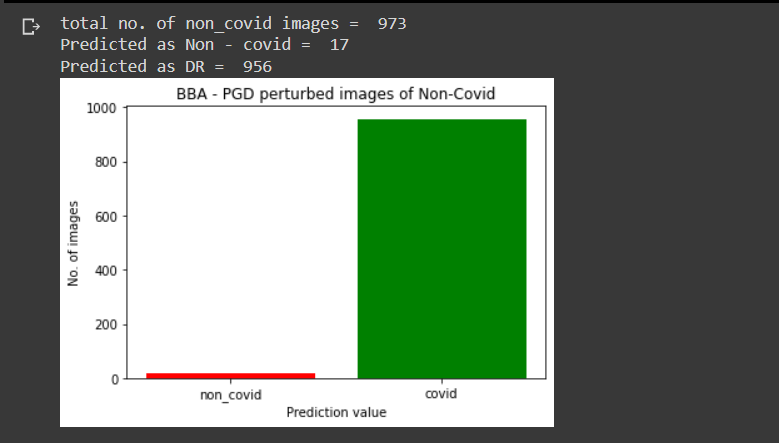
Predicted as Non-Covid = 775



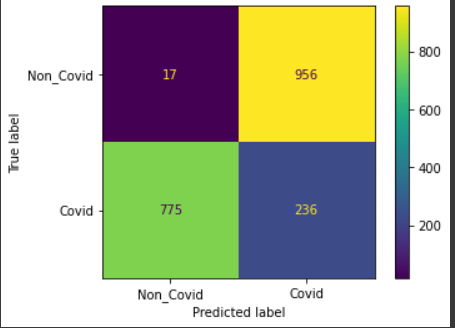
Total no. of perturbed non\_covid images = 973

Predicted as non\_covid = 17

Predicted as covid = 956



Confusion matrix for BBA using PGD on Covid 19 Dataset:



**2. BBA, BIM, COVID**

Epsilon = 1.4

alpha = eps/10

Maximum iterations = Stops when loss becomes less than 2 or when the iterations become greater than 10.

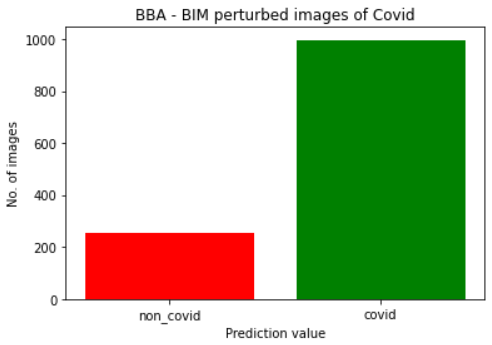
After creation of perturbed image using the attacker’s model, the images are run through the original model to find the predicted value

Total images = 2481

Total perturbed covid images = 1249

Predicted as Covid = 253

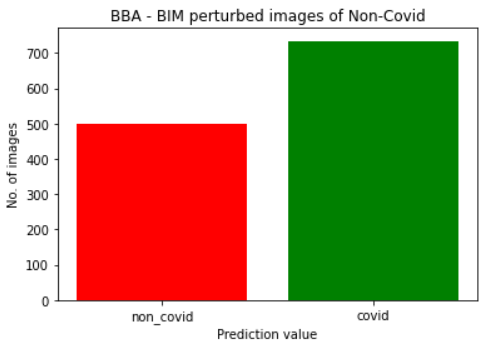
Predicted as Non-Covid = 996



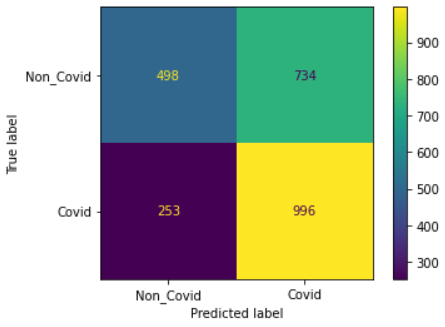
Total no. of perturbed non\_covid images = 1232

Predicted as non\_covid = 498

Predicted as covid = 734



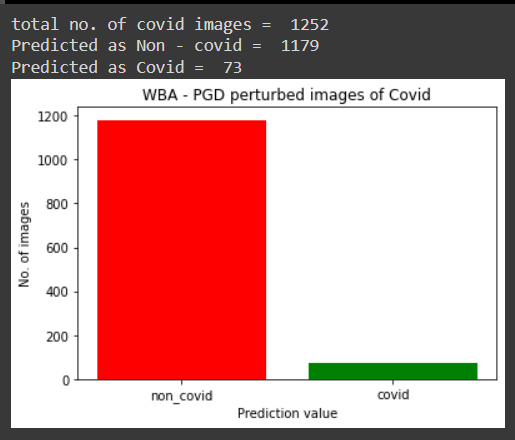
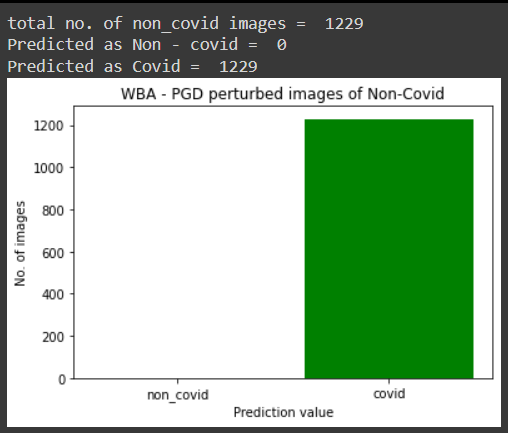
Confusion matrix for BBA using BIM on Covid 19 Dataset:

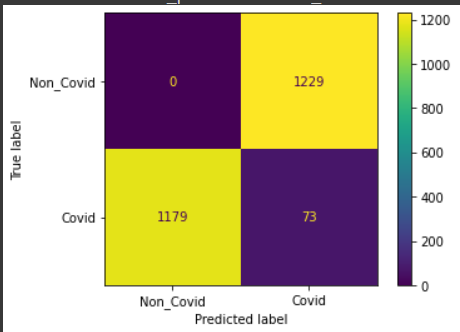


**3. PGD - COVID Dataset**

The perturbed dataset is created using the original model using the same images that the model is trained and tested on.

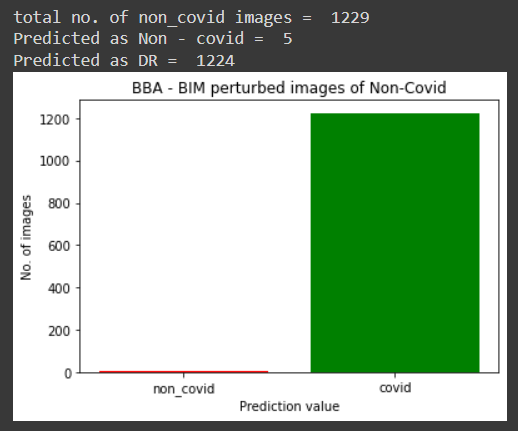
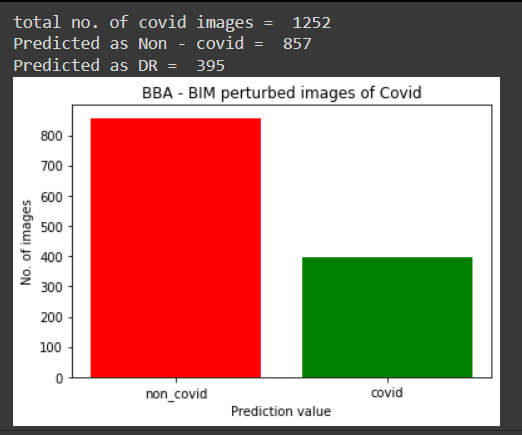
Total images = 2481

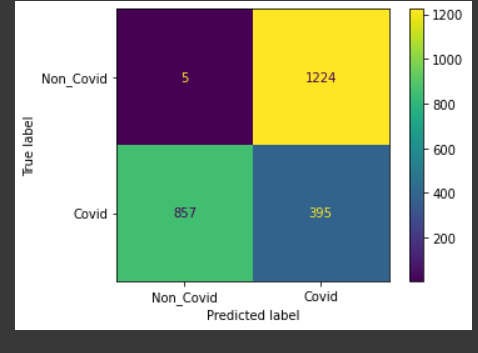
****

****

**4. BIM - COVID Dataset**

The perturbed dataset is created using the original model using the same images that the model is trained and tested on.

****

****

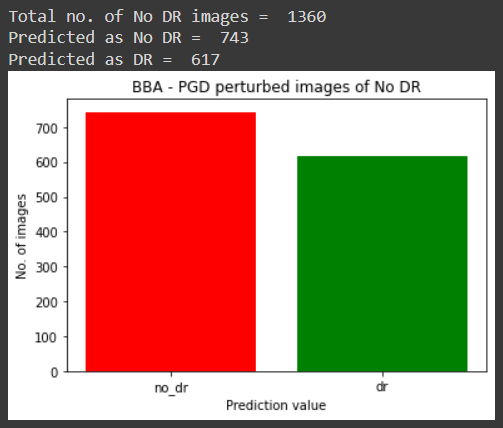
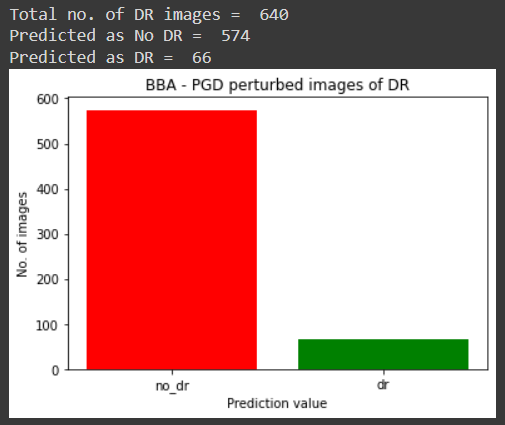
**5. BBA - PGD - Diabetic retinopathy**

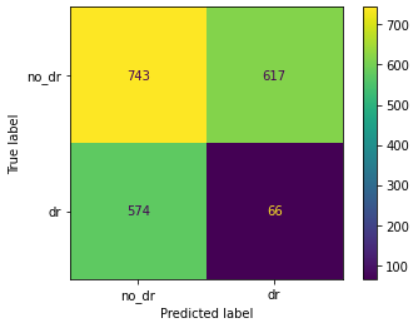
Epsilon = 1.4

alpha = eps/10

Maximum iterations = 10 (stops when loss reaches 10^-5 or max iter, whichever is earlier)

After creation of perturbed image using the attacker’s model, the images are run through the original model to find the predicted value





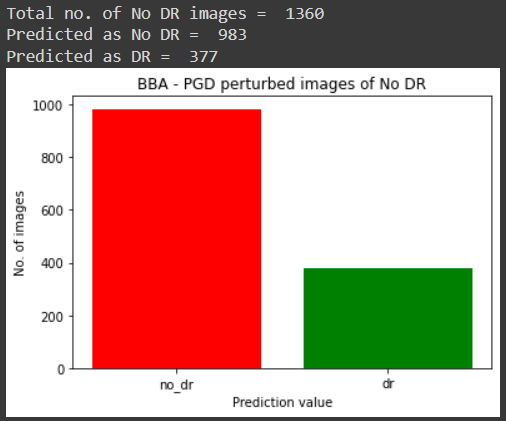
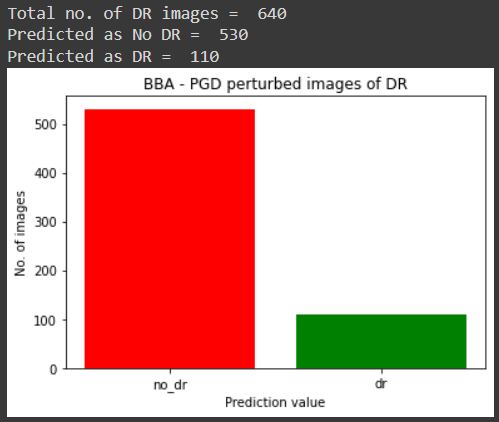
**6. BBA - BIM - Diabetic retinopathy**

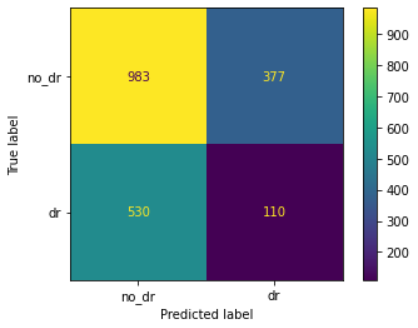
Epsilon = 1.4

alpha = eps/10

Maximum iterations = Stops when loss becomes less than 2 or when the iterations become greater than 10.

After creation of perturbed image using the attacker’s model, the images are run through the original model to find the predicted value





**7. WBA - PGD - Diabetic retinopathy**

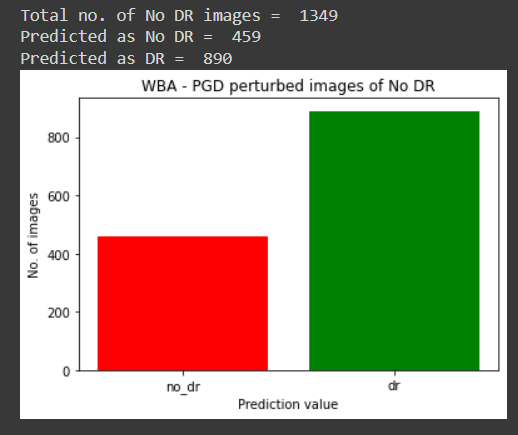
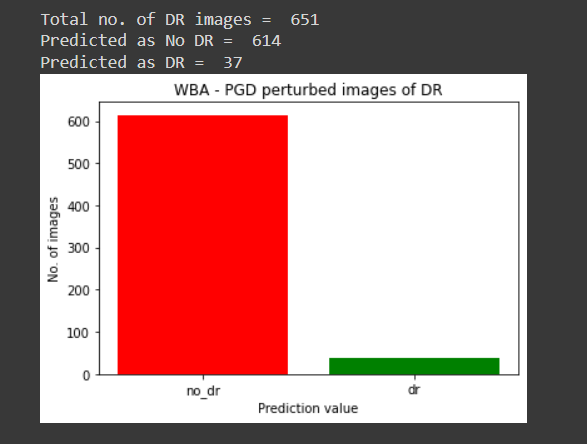
Epsilon = 1.4

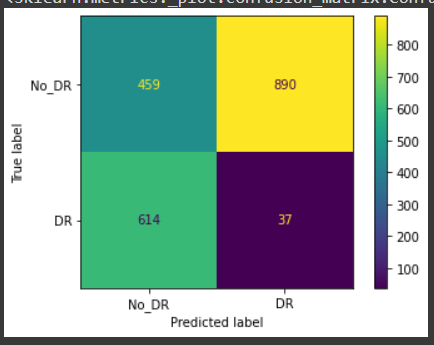
alpha = eps/10

Maximum iterations = Stops when loss becomes less than 2 or when the iterations become greater than 10.

The perturbed dataset is created using the original model using the same images that the model is trained and tested on.

Took 26 mins to create perturbations for 2000 images. On average each image took 3-5 iterations.





**8. WBA - BIM - Diabetic retinopathy**

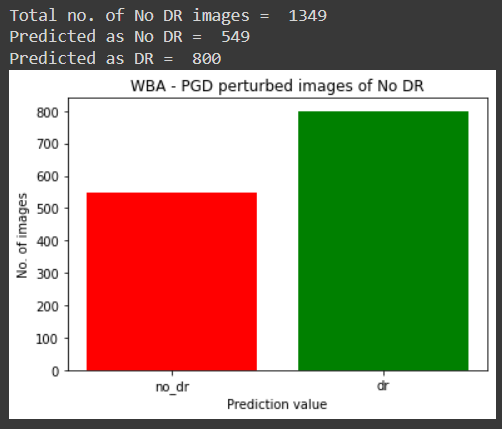
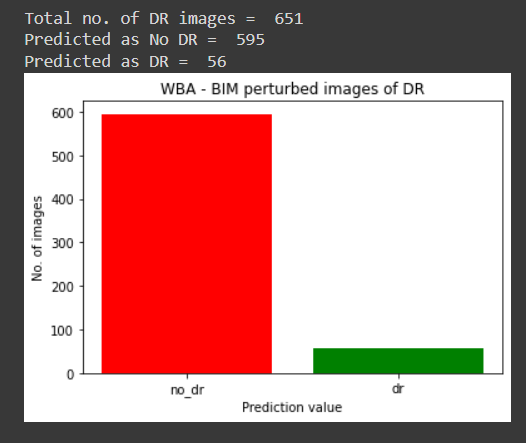
Epsilon = 1.4

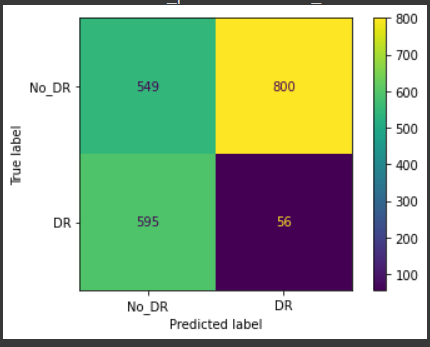
alpha = eps/10

Maximum iterations = Stops when loss becomes less than 2 or when the iterations become greater than 10.

The perturbed dataset is created using the original model using the same images that the model is trained and tested on.

Took 10 mins to create 2000 perturbed images. On average each image took 1-3 iterations.





**9. WBA, MIFGSM, COVID**

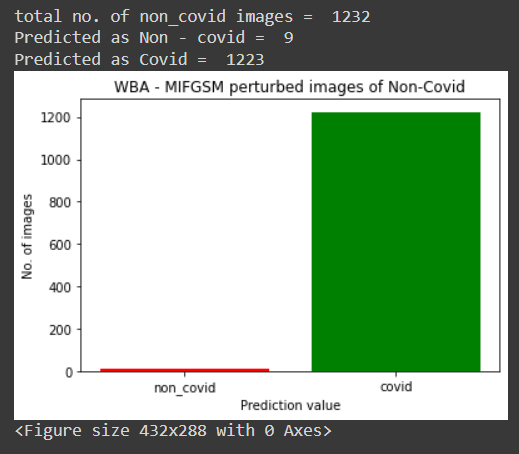
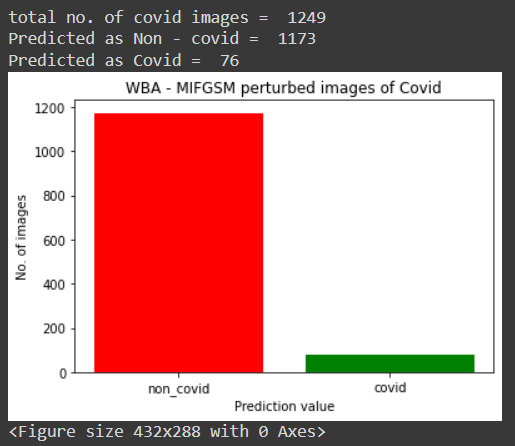
Epsilon = 1.4

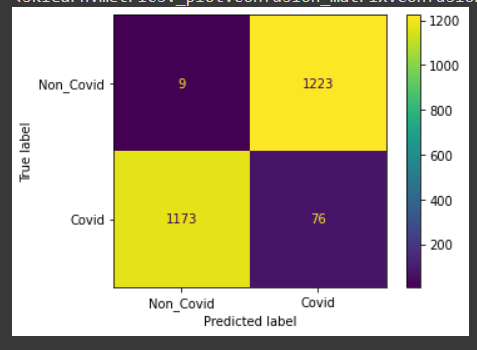
Alpha = epsilon/20

decay \_factor = 1

Stopping criteria: 20 iterations or norm(diff(x-input))>epsilon, whichever earlier

Took 13 mins to create 2489 perturbed images



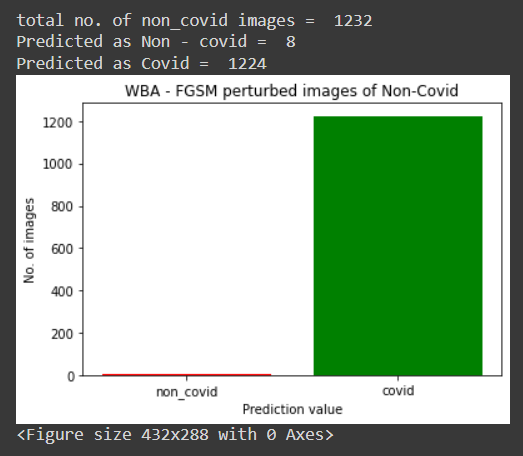
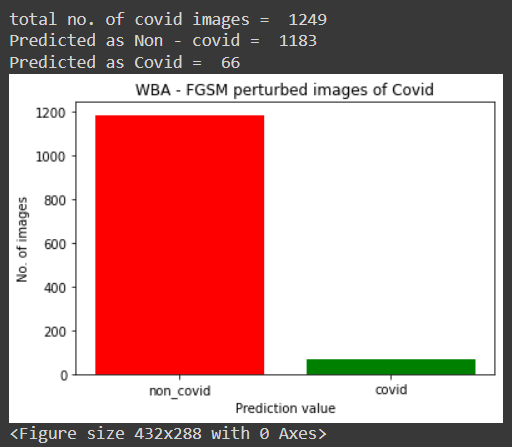


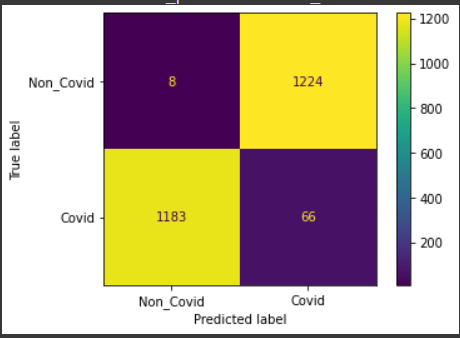
**10.WBA, FGSM, COVID**

Epsilon = 1.4

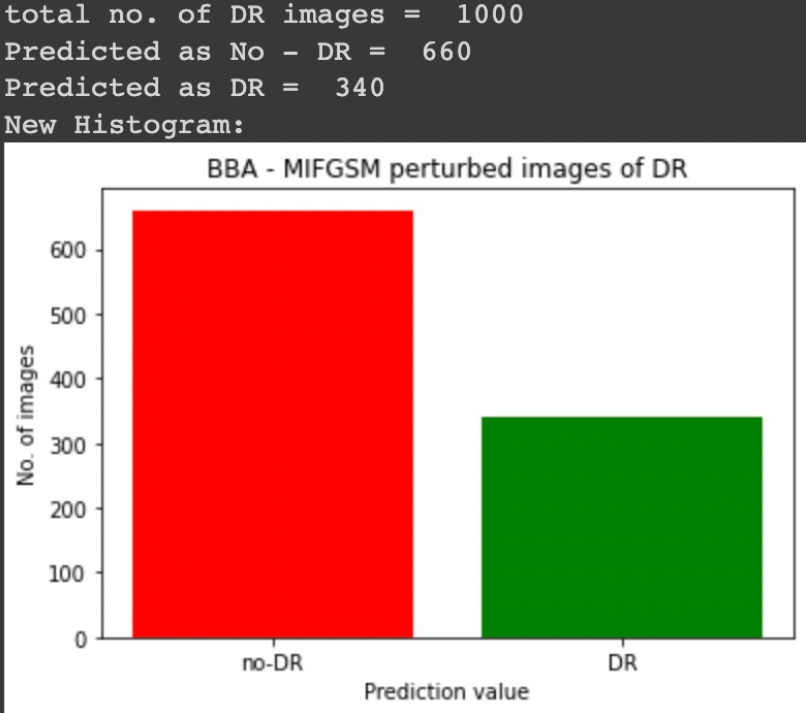
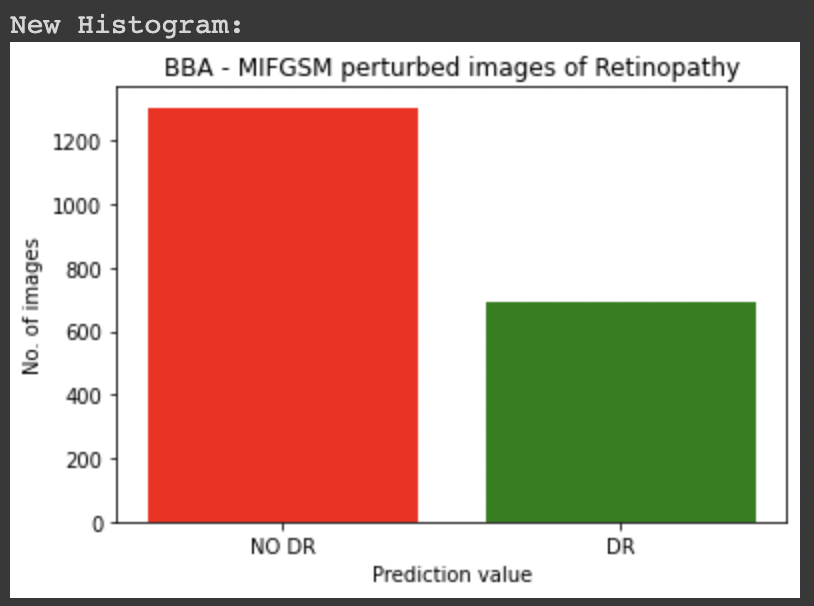
1 iteration

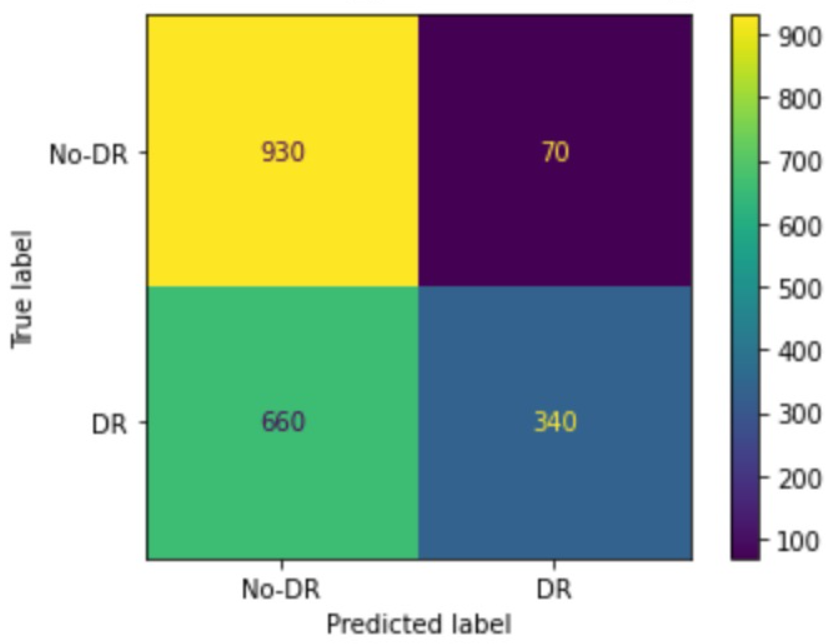
Took 11 mins to create 2489 perturbed images.

****

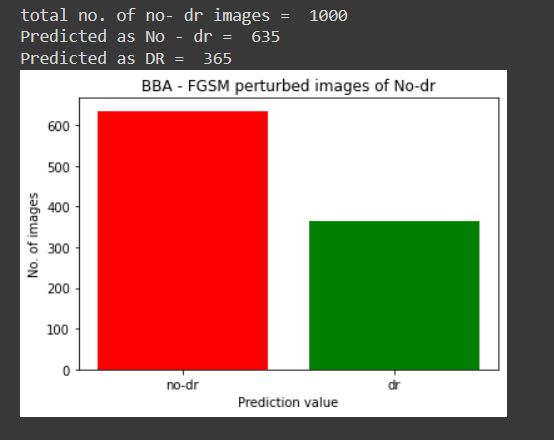
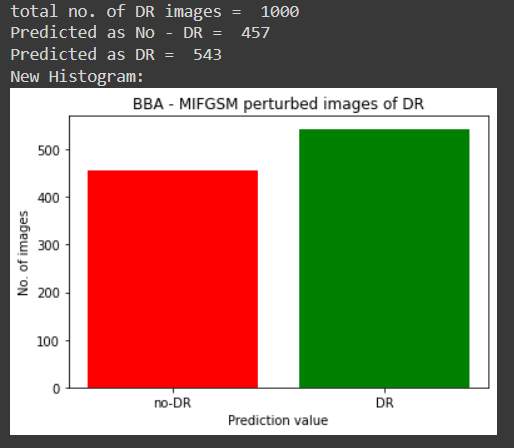
****

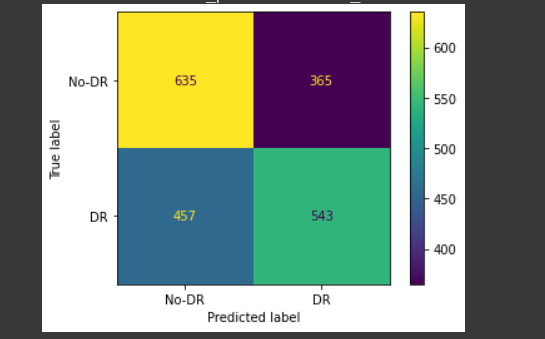
**11. BBA, MIFGSM, Retinopathy**





**12. BBA, FGSM, Retinopathy**





**Speed of creation of perturbation:-**

PGD:- 1.28 images/second (took 26 mins for 2000 DR images)

BIM:- 3.33 images/second (took 10 mins for 2000 DR images)

MIFGSM:- 3.19 images/second (took 13 mins for 2489 Covid images)

FGSM:- 3.78 images/second (took 11 mins for 2489 Covid images)

Specs of machine used:

