**Notice 1: The execution times are under the effect of other running applications on the system!**

**Notice 2: Since the CNN is pre-trained and it does not always provide the same results, the most common values are reported.**

**Fingerprint Experiment 1 (Feature Extractor = CNN; SVM = Classifier) Confusion Matrix**

**CNN Layer to Extract Features = Fully Connected 7**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0117 | 0.9883 |

**Execution Time =** 632.048221 (s)

**Fingerprint Experiment 2 (Infected Feature Extractor = CNN (Layer Removal); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Convolution 2**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0 | 1 |
| Fake Fingerprint | 0 | 1 |

**What Happened? Denial of Service!**

**Execution Time =** 522.226882 (s)

**Fingerprint Experiment 3 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every “odd” element of the Bias vector of the seventh fully connected layer with its next “even” element in the vector!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 1.0000 | 0 |
| Fake Fingerprint | 0.0352 | 0.9648 |

**What Happened? Unauthorized Access!**

**Execution Time =** 695.366284 (s)

**Fingerprint Experiment 4 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every thirty-two elements of the Bias vector of the seventh fully connected layer with their average value!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0156 | 0.9844 |

**What Happened? Unauthorized Access!**

**Execution Time =** 697.231701 (s)

**Fingerprint Experiment 5 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every thirty-two elements of the Bias vector of the seventh fully connected layer with their minimum value!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0195 | 0.9805 |

**What Happened? Unauthorized Access!**

**Execution Time =** 716.857667 (s)

**Fingerprint Experiment 6 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every “odd” element in eight columns of the Weight matrix (with the step size of 512) of the seventh fully connected layer with its next “even” element in the vector!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0156 | 0.9844 |

**What Happened? Unauthorized Access!**

**Execution Time =** 638.600141 (s)

**Fingerprint Experiment 7 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every element of the Weight matrix of the seventh fully connected layer with their mean/median/minimum/mode value!!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0 | 1 |
| Fake Fingerprint | 0 | 1 |

**What Happened? Denial of Service!**

**Average Execution Time =** (626.161682 + 648.260815 + 587.085334 + 704.860604)/4 = 641.59210875 (s)

**Fingerprint Experiment 8 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Flipping the Weight matrix of the seventh fully connected layer up-side and down-side!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0234 | 0.9766 |

**What Happened? Unauthorized Access!**

**Execution Time =** 641.341350 (s)

**Fingerprint Experiment 9 (Infected Feature Extractor = CNN (Layer Removal); SVM = Classifier) Confusion Matrix – Before Enrollment**

**CNN Layer to Extract Features = Convolution 2**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 1.0000 | 0 |
| Fake Fingerprint | 0.0078 | 0.9922 |

**What Happened? No Danger!**

**Execution Time =** 317.448508 (s)

**Fingerprint Experiment 10 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – Before Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every “odd” element of the Bias vector of the seventh fully connected layer with its next “even” element in the vector!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0156 | 0.9844 |

**What Happened? Unauthorized Access!**

**Execution Time =** 655.736589 (s)

**Fingerprint Experiment 11 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – Before Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every thirty-two elements of the Bias vector of the seventh fully connected layer with their average value!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0195 | 0.9805 |

**What Happened? Unauthorized Access!**

**Execution Time =** 650.419279 (s)

**Fingerprint Experiment 12 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – Before Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every thirty-two elements of the Bias vector of the seventh fully connected layer with their minimum value!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 1.0000 | 0 |
| Fake Fingerprint | 0.0352 | 0.9648 |

**What Happened? Unauthorized Access!**

**Execution Time =** 697.520489 (s)

**Fingerprint Experiment 13 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – Before Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every “odd” element in eight columns of the Weight matrix (with the step size of 512) of the seventh fully connected layer with its next “even” element in the vector!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0195 | 0.9805 |

**What Happened? Unauthorized Access!**

**Execution Time =** 681.041590 (s)

**Fingerprint Experiment 14 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – Before Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Substituting every element of the Weight matrix of the seventh fully connected layer with their mean/median/minimum/mode value!!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0166 | 0.9834 |

**What Happened? Unauthorized Access!**

**Execution Time =** 664.751737 (s)

**Fingerprint Experiment 15 (Infected Feature Extractor = CNN (Layer Manipulation); SVM = Classifier) Confusion Matrix – After Enrollment**

**CNN Layer to Extract Features = Fully Connected 7**

**What to Do?** Flipping the Weight matrix of the seventh fully connected layer up-side and down-side!

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0234 | 0.9766 |

**What Happened? Unauthorized Access!**

**Execution Time =** 657.352929 (s)