<table>
<tr><th rowspan="2">cases</th><th>doc_1</th><th>doc_2</th><th>decision</th><th>id</th></tr>
<tr><td>
<table>
<tr><th>authors</th><td>Anisie Uwimana
Ransalu Senanayake</td></tr>
<tr><th>title</th><td>Out of Distribution Detection and Adversarial Attacks on Deep Neural Networks for Robust Medical Image Analysis</td></tr>
<tr><th>publication_date</th><td>2021-06-18 00:00:00</td></tr>
<tr><th>source</th><td>SupportedSources.OPENALEX</td></tr>
<tr><th>journal</th><td>International Conference on Machine Learning</td></tr>
<tr><th>volume</th><td></td></tr>
<tr><th>doi</th><td>None</td></tr>
<tr><th>urls</th><td>https://openalex.org/W3214961495</td></tr>
<tr><th>id</th><td>id5819437435903861242</td></tr>
<tr><th>abstract</th><td></td></tr>
<tr><th>versions</th><td></td></tr>
</table>
</td><td>
<table>
<tr><th>authors</th><td>Anisie Uwimana1
Ransalu Senanayake</td></tr>
<tr><th>title</th><td>Out of Distribution Detection and Adversarial Attacks on Deep Neural Networks for Robust Medical Image Analysis</td></tr>
<tr><th>publication_date</th><td>2021-07-10 18:00:40+00:00</td></tr>
<tr><th>source</th><td>SupportedSources.ARXIV</td></tr>
<tr><th>journal</th><td>None</td></tr>
<tr><th>volume</th><td></td></tr>
<tr><th>doi</th><td></td></tr>
<tr><th>urls</th><td>http://arxiv.org/pdf/2107.04882v1
http://arxiv.org/abs/2107.04882v1
http://arxiv.org/pdf/2107.04882v1</td></tr>
<tr><th>id</th><td>id1381411009384522840</td></tr>
<tr><th>abstract</th><td>Deep learning models have become a popular choice for medical image analysis. However, the poor generalization performance of deep learning models limits them from being deployed in the real world as robustness is critical for medical applications. For instance, the state-of-the-art Convolutional Neural Networks (CNNs) fail to detect adversarial samples or samples drawn statistically far away from the training distribution. In this work, we experimentally evaluate the robustness of a Mahalanobis distance-based confidence score, a simple yet effective method for detecting abnormal input samples, in classifying malaria parasitized cells and uninfected cells. Results indicated that the Mahalanobis confidence score detector exhibits improved performance and robustness of deep learning models, and achieves stateof-the-art performance on both out-of-distribution (OOD) and adversarial samples.</td></tr>
<tr><th>versions</th><td></td></tr>
</table>
</td><td>DUPLICATES</td><td>114</td></tr>
</table>