Title (en)

METHOD FOR ASSESSING A FUNCTION-SPECIFIC ROBUSTNESS OF A NEURAL NETWORK

Title (de)

VERFAHREN ZUM BEURTEILEN EINER FUNKTIONSSPEZIFISCHEN ROBUSTHEIT EINES NEURONALEN NETZES

Title (fr)

PROCÉDÉ POUR ÉVALUER UNE ROBUSTESSE SPÉCIFIQUE DE LA FONCTION D'UN RÉSEAU NEURONAL

Publication

**EP 3973455 A1 20220330 (DE)**

Application

**EP 20724043 A 20200430**

Priority

- DE 102019207575 A 20190523
- EP 2020062110 W 20200430

Abstract (en)

[origin: WO2020233961A1] The invention relates to a method for assessing a function-specific robustness of a neural network (1), comprising the following steps: providing the neural network (1), wherein the neural network (1) is/has been trained on the basis of a training data set (2) including training data; generating at least one changed training data set (4) by manipulating the training data set (2), wherein the training data is changed while maintaining semantically meaningful content; determining at least one activation differential (7) between an activation of the neural network (1) via the training data of the original training data set (2) and an activation via the respective corresponding training data of the at least one changed training data set (4); and providing the determined at least one activation differential (7). The invention also relates to a device (30), a computer program product and a computer-readable storage medium.

IPC 8 full level

**G06N 3/02** (2006.01); **G06N 3/08** (2006.01)

CPC (source: EP US)

**G06N 3/045** (2023.01 - EP); **G06N 3/08** (2013.01 - EP US); **G06V 10/774** (2022.01 - US); **G06V 10/776** (2022.01 - US); **G06V 10/82** (2022.01 - US); G06N 3/048 (2023.01 - EP)

Citation (search report)

See references of WO 2020233961A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

**DE 102019207575 A1 20201126**; CN 113826114 A 20211221; EP 3973455 A1 20220330; US 2022318620 A1 20221006; WO 2020233961 A1 20201126

DOCDB simple family (application)

**DE 102019207575 A 20190523**; CN 202080038184 A 20200430; EP 2020062110 W 20200430; EP 20724043 A 20200430; US 202017612330 A 20200430