



## SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application number:  
EP 21 88 08 94

Classification of the application (IPC):  
G06N 3/02, G06N 3/096, G06N 5/022, G06N 20/00, G06N 3/045

Technical fields searched (IPC):  
G06N

### DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim
X	<p><b>ZHAO JINGJING ET AL:</b> "AFA: Adversarial fingerprinting authentication for deep neural networks" <i>COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL</i>, 14 December 2019 (2019-12-14), vol. 150, DOI: 10.1016/J.COMCOM.2019.12.016, ISSN: 0140-3664, pages 488-497, XP086011281</p> <p>* page 489, left-hand column, line 6 - line 36 *</p> <p>* from Section 2.2 to Section 4;page 489, left-hand column - page 491, left-hand column *</p>	1-15
A	<p><b>YUAN XIAOYONG ET AL:</b> "Adversarial Examples: Attacks and Defenses for Deep Learning" <i>IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE, USA</i>, 01 September 2019 (2019-09-01), vol. 30, no. 9, DOI: 10.1109/TNNLS.2018.2886017, ISSN: 2162-237X, pages 2805-2824, XP011741439</p> <p>* the whole document *</p>	1-15
A	<p><b>Paschali Magdalini ET AL:</b> "Generalizability vs. Robustness: Adversarial Examples for Medical Imaging" <i>arXiv.org Ithaca</i></p> <p>23 March 2018 (2018-03-23)</p> <p>URL: <a href="https://arxiv.org/pdf/1804.00504.pdf">https://arxiv.org/pdf/1804.00504.pdf</a>, DOI: 10.48550/arxiv.1804.00504 [retrieved on 16 February 2024 (2024-02-16)]</p> <p>XP093132405</p> <p>* the whole document *</p>	1-15

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search The Hague	Date of completion of the search 16 February 2024	Examiner Manfrin, Max
------------------------------	--	--------------------------

### CATEGORY OF CITED DOCUMENTS

X: particularly relevant if taken alone	P: intermediate document
Y: particularly relevant if combined with another document of the same category	T: theory or principle underlying the invention
A: technological background	E: earlier patent document, but published on, or after the filing date
O: non-written disclosure	D: document cited in the application
& : member of the same patent family, corresponding document	L: document cited for other reasons

Disclaimer: this document has been automatically generated using data structured in accordance with WIPO standard ST.36 from the database of search reports of the European Patent Office. For technical reasons, its content and layout may differ from that of the original publication. Only the original published information is legally binding.