Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 03, No. 05, Aug-Sept 2023
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs.35.10.19

Signature Verification System: Using Big Transfer (BiT-M-R50x1) for Accurate Authentication

Kazi Tanvir[*]

[*]*Department of Computer Science, American International University-Bangladesh (AIUB), Kuratoli, Dhaka, Bangladesh.*

Corresponding Email: [*]*kazitanvir.ai@gmail.com*

Received: 30 April 2023 **Accepted:** 19 July 2023 **Published:** 07 September 2023

Abstract:** In the realm of document security, signature verification stands as a vital pillar for establishing authenticity. This study delves into the utilization of the potent Big Transfer (BiT) BiT-M-R50x1 model for the intricate task of signature validation. This dataset encompasses 2149 signature images sourced from diverse individuals, exhibiting notable fluctuations in writing styles, pen pressures, and signature dimensions. By harnessing the prowess of the pre-trained BiT-M-R50x1 model, renowned for its domain-generalization capability, we fine-tune it to excel in signature verification. The results of our approach unveil remarkable accomplishments on the dataset, yielding a validation accuracy of 98.60%. The meticulously calibrated BiT-M-R50x1 model adeptly distinguishes between authentic and counterfeit signatures, even when confronted with substantial variation. Through the mechanism of transfer learning, the model captures intrinsic attributes that extrapolate effectively to previously unseen signature specimens. Furthermore, we meticulously assess the model's performance concerning the dataset's distinctive signature idiosyncrasies, scrutinizing its adaptability to diverse styles and dimensions. This experiment underscores the potential of harnessing robust pre-trained models like BiT-M-R50x1 for signature verification undertakings, particularly when grappling with intricate and heterogeneous datasets.

***Keywords:** Signature Verification, Big Transfer, BiT-M-R50x1, Biometric Authentication, Electronic Signatures.*

1. INTRODUCTION

Numerous versions of biometric methods have emerged for personal identification purposes [1]. Among these, visual techniques encompass facial recognition [2], fingerprint scanning [3], iris scanning [4], and retina scanning [5]. In contrast, non-visual approaches comprise voice recognition [6]and signature authentication [7]. In the domains of finance, economics,

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

and legal procedures, the increasing importance of strong authentication underscores the criticality of preserving the integrity of signature. Such signatures, endorsed by authorized entities, persist as a highly reliable mode of validation often denoted as marks of endorsement [8]. Efforts in ensuring impregnable authentication mechanisms are intensifying, particularly as the importance of trustworthy signature authentication endures in critical procedures.

Handwritten signatures hold a unique position within the diverse realm of biometric attributes, primarily attributed to their historical status as the most pervasive method of personal authentication, universally acknowledged by administrative and financial establishments as a legally accepted mode of verifying an individual's identity. Categorized by their data acquisition techniques, signature verification systems are divided into two primary classes: the offline method, termed static, and the online method, known as dynamic, with the latter encompassing temporal attributes like pen speed and pressure through specialized tools such as styluses or tablets [9].

Related Works

Signature Verification

The offline signature serves as a unique handwritten depiction of an individual's name or mark, serving as evidence of identity on financial instruments, legal papers, and other official records, constituting a biometric measure encompassing distinctive physical attributes; the authentication of such offline signatures stands as an indispensable undertaking [10]. The OfSV (Offline Signature Verification) system encompasses three variations: writer-dependent (WD), writer-independent (WI), and hybrid; while WD is the prevalent and more accurate approach due to user-specific verification models, it requires separate classifiers per user, leading to elevated complexity, whereas WI offers a more efficient and simpler to use alternative by using a single global classifier for all users and only requiring one signature sample. [11]. A recent investigation evaluated the efficacy of writer-independent (WI) offline signature verification (OfSV) systems based on deep learning, demonstrating enhanced performance through a novel real-world document stamp cleaning procedure; an alternative strategy involves a hybrid WD–WI OfSV system that alternates between writer- dependent and writer-independent methods [12]. In the process of binarization preprocessing, researchers have employed diverse thresholding techniques, encompassing global, local iterative, iterative shrinkage thresholding algorithm, adaptive, histogram-based, binary, linear discriminant analysis based, and distance-based methods, in order to rectify discrepancies within offline signature images [13]. Nevertheless, the commonly adopted global thresholding technique, Otsu algorithm, emerged as the prevailing choice, segmenting pixels of the offline signature image into foreground and background classes through a solitary intensity threshold [14]. Nagel and Rosenfeld [15] authored a study addressing handwritten forgeries on bank cheques, employing geometrical attributes such as size and slant ratios. Bernardete Ribeiro, Ivo Gonçalves, Sérgio Santos, and Alexander Kovacec utilized a massive parallel distributed neural network to achieve intricate signature representations, conducting experiments on the GDPS dataset to attain a three-layer configuration, two of which were internal, successfully introducing a two-step hybrid model to reduce misclassification without actual classification in their study [16]. Khalajzadeh et al. [17] introduced a convolutional

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

neural network for signature classification without prior feature knowledge, utilizing a multi-layer perceptron for classification, conducting experiments on Persian signatures of 22 individuals, with CNN employed as a feature descriptor and MLP for classification, training on 176 signatures from 22 individuals. Notably, exceptional recognition accuracies of 99.79% and 98.71% were achieved for the GPDS synthetic and UTSig datasets respectively, employing the VGG16 model for both [18].

Big Transfer (BiT)

The concept of BiT, introduced by Google Research in 2020 centers around constructing a robust image representation model via pretraining on an extensive and varied dataset, subsequently fine-tuning on particular tasks using smaller datasets, effectively harnessing transfer learning principles to transfer knowledge from a broader task to a more specific one [19]. The intentional design of BiT has been focused on showcasing its ability to be flexible, rendering it suitable for a broad range of tasks related to visual recognition. These tasks include but are not limited to recognizing objects [20], performing semantic segmentation [21], and classifying images into categories [22]. Its substantial dimensions and extensive initial training empower it to grasp complex visual depictions, which can then be refined and personalized to address a broad array of particular assignments. This flexibility distinguishes BiT as a potent instrument for addressing a variety of complex tasks within the realm of visual recognition [19].

This study introduces an offline methodology for signature verification, with the paper's structure comprising distinct segments: Section 2 involves a comprehensive review of past literature, Section 3 elucidates the research methodology, Section 4 deliberates on the obtained outcomes and discoveries, and, in culmination, Section 5 provides the paper's conclusive remarks.

2. METHODOLOGY

Proposed Model

The research uses BiT-M-R50x1 for training the dataset.The Big Transfer (BiT) framework enhances transfer learning by pretraining models on diverse datasets of varying scales (BiT-S, BiT-M, BiT-L) and employing Group Normalization and Weight Standardization to overcome Batch Normalization limitations. Fine-tuning involves strategies such as adjusting resolution during testing and setting optimal schedule lengths based on dataset size, enabling effective transfer to downstream tasks while capitalizing on the models' pretrained features and enhanced training techniques [19]. The input shape of the model was (224, 224, 3) which meant 224x224 images with 3 channel colour or RGB colour. BiT was used as a Keras layer [23] for transfer learning by not training or fine-tuning the pre-trained BiT model during the training process. The input layer and keras layer uses the ‘Relu’ [24] activation function and the Dense layer uses ‘Softmax’ [25] activation function.

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

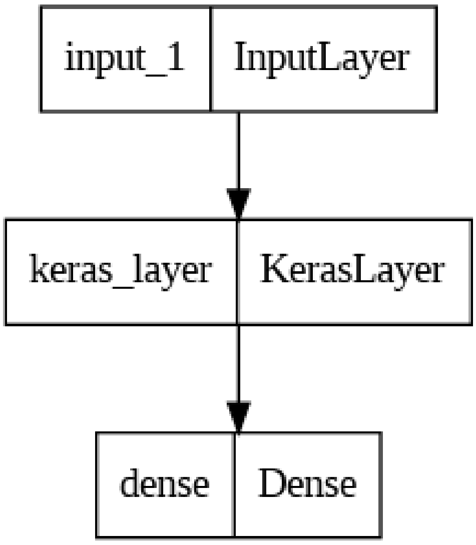

Fig.1 Proposed model: a three-layered architecture where input layer shape is (None, 224, 224, 3), KerasLayer shape is (None, 2048) and a Dense layer with shape (None, 2)

Table1: Parameter Distribution

Layer(type)	Output Shape	Parameters
Input Layer	(None, 224, 224, 3)	0
Keras Layer	(None, 2048)	23,500,352
Dense Layer	(None, 2)	4098

Dataset

The Dataset used in the research is a public access dataset from Kaggle called robinreni/signature-verification-dataset [26]. The dataset contains a total of 2149 images divided into 2 classes; Fake and Real. The dataset set has 1649 images for training and 500 images for testing. From the training data, 20% data was taken for validation purposes.

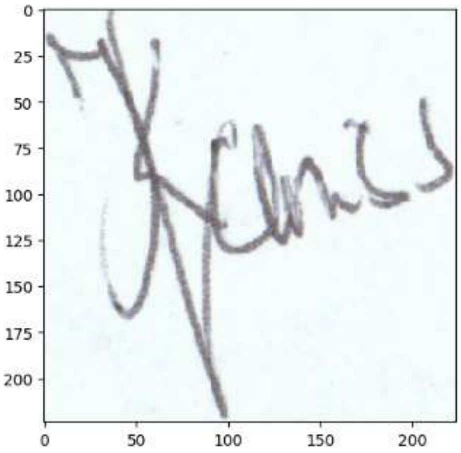

Fig.2 Example of dataset

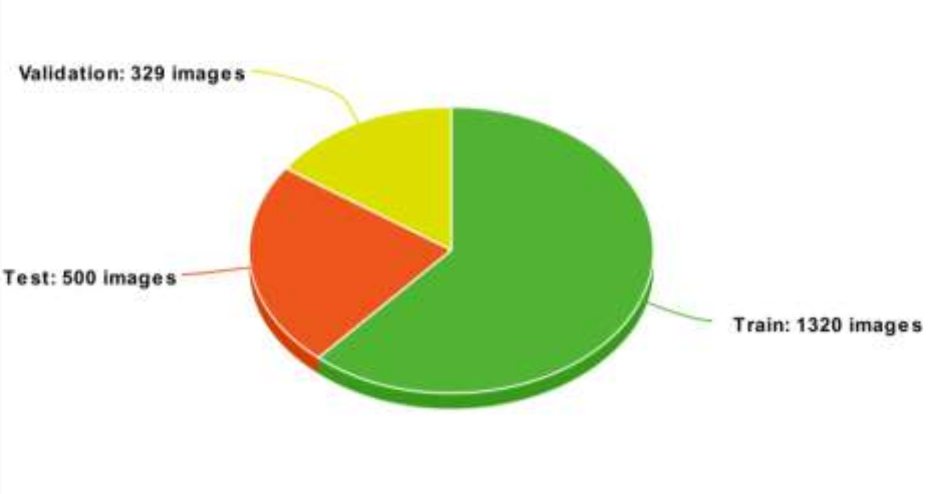

Fig.3 Dataset Distribution

Data Preprocessing

ImageDataGenerator library by tensorflow [27] was used for data preparation. At first, the images were rescaled. In the realm of digital images, pixel values commonly span a spectrum from 0 to 255, symbolizing varying degrees of brightness or color strength. Through the process of dividing these pixel values by 255, a transformation occurs that effectively reduces their range to a scale that lies between 0 and 1. This adjustment aids in standardizing and normalizing the pixel values for further analysis or processing. Then training images were divided into 80-20 ratio for training and validation. The images were divided into batches of 32 and the class mode was set to binary.

Compiling the Model

The loss function of choice, specifically referred to as 'sparse_categorical_crossentropy'[28], is employed to quantify the disparity between projected and actual values during the training phase. This selection is particularly apt for tasks involving multiclass classification where target labels are represented as integers. The optimizer 'adam' [29] is explicitly designated to oversee the adjustment of model weights through the process of backpropagation, utilizing its dynamic learning rate mechanism. For assessing performance, the code incorporates the "accuracy" statistic to gauge how accurately the model forecasts outcomes in comparison to the true labels.

Table 2: Hyperparameters of the model

Hyperparameters	**Values**
Loss	Sparse Categorical Crossentropy
Optimizer	Adam (Lr = 0.001)
Metrics	Accuracy

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Training the Model

The model was trained on google colab environment where the system RAM is 12.7 GB and GPU RAM is 15 GB [30]. The model was trained on 5 epochs with callback checkpoint to save the best model. It took a total of 105 seconds to run the 5 epochs 361ms/step was required.

3. RESULTS AND FINDINGS

After 5 epochs the training accuracy was 97.63% and loss was 8.67%. The validation accuracy after the said number of epochs was 98.60% and validation loss was 5.57%. The testing accuracy of the model was 99.40% and the loss was 5.57%.

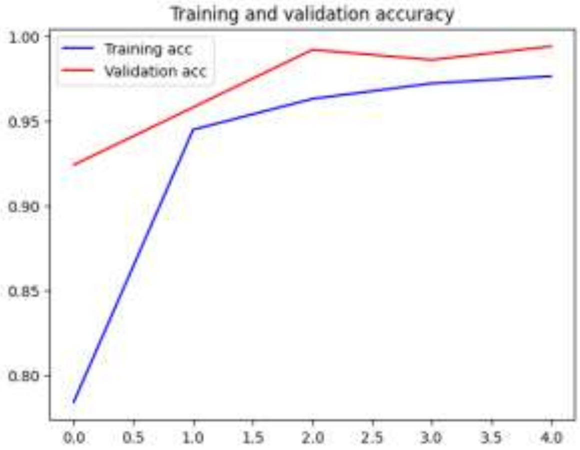

Fig.4 Accuracy curve during Training and Validation

Precision constitutes a foundational measure, calculated as the ratio of correctly forecasted positive instances to the total number of positive predictions [31]. It effectively addresses the question of how accurately instances labeled with a certain attribute truly belong to that specific attribute. Notably, higher precision scores align with fewer occurrences of incorrectly identified positives. The mathematical interpretation of precision is stated,

$$\text{Precision} = \text{TruePositives} / (\text{TruePositives} + \text{FalsePositives}) \qquad (1)$$

Within our precise context, a noteworthy precision metric of around 1.00, averaged across two distinct class instances, was successfully attained.

The performance metric known as Recall, alternatively referred to as Sensitivity or the True Positive Rate, assumes a crucial role in the domain of machine learning and classification [31]. Its purpose is to measure the proportion of actual positive instances (associated with particular categories) that a model accurately identifies. Recall can be shown mathematically as,

$$\text{Recall} = \text{TruePositives} / (\text{TruePositives} + \text{FalseNegatives}) \qquad (2)$$

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

In our specific scenario, a notable recall measure of approximately 0.976, calculated as an average over the range of two distinct class instances, has been accomplished. This substantial attainment in recall underscores the efficiency of our unique signature verification system.

The F1 Score [32] is computed by combining precision and recall in a weighted manner, encompassing considerations for both false positives and false negatives. Consequently, this metric addresses the intricacies of classification performance. While its interpretation might not be as straightforward as accuracy, the F1 score often proves more useful, especially in the presence of class imbalances. This is because accuracy is most effective when false positives and false negatives have similar costs. However, in cases where the costs of these errors differ significantly, a closer examination of both Precision and Recall becomes necessary.

F-Measure = (2 * Precision * Recall) / (Precision + Recall) (3)

In our specific scenario, the F1 score, with an average of 0.988 across the range, emerges as a significant performance indicator. This accomplishment underscores the system's adeptness in managing the complexities of signature verification, effectively considering the trade-offs between precision and recall within the context of uneven class proportions.

4. CONCLUSIONS

In summary, the proposed approach demonstrated impressive results in signature verification. The training phase achieved a high accuracy of 97.63% over 5 epochs with a corresponding loss of 8.67%. Validation reinforced this performance, achieving 98.60% accuracy and 5.57% validation loss. The model's robustness was evident in the exceptional 99.40% testing accuracy and consistent 5.57% loss, highlighting its effectiveness across real-world variations.

Looking forward, there are promising directions for future research in the signature verification domain. These include delving into methods to enhance the model's interpretability for practical application understanding. Addressing potential class imbalances and refining model architecture and hyperparameters could further enhance performance. Rigorous testing on diverse datasets and styles would validate the model's robustness, and integration with emerging technologies like explainable AI and blockchain could elevate security and transparency in signature verification. In conclusion, this study has showcased an exceptional signature verification model with noteworthy metrics in accuracy, precision, recall, and F1 score.

5. REFERENCES

1. P. William, G. R. Lanke, S. Pundir, I. Kumar, M. Gupta, and S. Shaw, “Implementation of Hand Written based Signature Verification Technology using Deep Learning

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Approach," in 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), May 2023, pp. 1–6. doi: 10.1109/ICIEM59379.2023.10167195.

2. M. R. Hasan, R. Guest, and F. Deravi, "Presentation-level Privacy Protection Techniques for Automated Face Recognition—A Survey," ACM Comput. Surv., vol. 55, no. 13s, p. 286:1-286:27, Jul. 2023, doi: 10.1145/3583135.
3. "Motion Robust MR Fingerprinting Scan to Image Neonates With Prenatal Opioid Exposure - Ma - Journal of Magnetic Resonance Imaging - Wiley Online Library." https://onlinelibrary.wiley.com/doi/full/10.1002/jmri.28907 (accessed Aug. 22, 2023).
4. E. Okello et al., "Acceptability and applicability of biometric iris scanning for the identification and follow up of highly mobile research participants living in fishing communities along the shores of Lake Victoria in Kenya, Tanzania, and Uganda," Int. J. Med. Inf., vol. 172, p. 105018, Apr. 2023, doi: 10.1016/j.ijmedinf.2023.105018.
5. N. K. Shaydyuk and T. Cleland, "Biometric identification via retina scanning with liveness detection using speckle contrast imaging," in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Oct. 2016, pp. 1–5. doi: 10.1109/CCST.2016.7815706.
6. J. Zumalt, "Voice Recognition Technology: Has It Come of Age?," Inf. Technol. Libr., vol. 24, pp. 180–185, Dec. 2005, doi: 10.6017/ital.v24i4.3382.
7. R. Beed, nikita goyal, D. Ghosh, and F. Zareen, "SIGNATURE AUTHENTICATION," Avis. Xaver. J. Res., vol. 1, Jan. 2009.
8. H. C. Kumawat and A. A. B. Raj, "SP-WVD with Adaptive-Filter-Bank-Supported RF Sensor for Low RCS Targets' Nonlinear Micro-Doppler Signature/Pattern Imaging System," Sensors, vol. 22, no. 3, Art. no. 3, Jan. 2022, doi: 10.3390/s22031186.
9. K. S. Radhika and S. Gopika, "Online and Offline Signature Verification: A Combined Approach," Procedia Comput. Sci., vol. 46, pp. 1593–1600, Jan. 2015, doi: 10.1016/j.procs.2015.02.089.
10. M. M. Hameed, R. Ahmad, M. L. M. Kiah, and G. Murtaza, "Machine learning-based offline signature verification systems: A systematic review," Signal Process. Image Commun., vol. 93, p. 116139, Apr. 2021, doi: 10.1016/j.image.2021.116139.
11. "Hybrid writer-independent–writer-dependent offline signature verification system - Eskander - 2013 - IET Biometrics - Wiley Online Library." https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2013.0024 (accessed Aug. 22, 2023).
12. D. Engin, A. Kantarci, S. Arslan, and H. K. Ekenel, "Offline Signature Verification on Real-World Documents," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA: IEEE, Jun. 2020, pp. 3518–3526. doi: 10.1109/CVPRW50498.2020.00412.
13. E. H. Barney Smith, L. Likforman-Sulem, and J. Darbon, "Effect of pre-processing on binarization," presented at the IS&T/SPIE Electronic Imaging, L. Likforman-Sulem and G. Agam, Eds., San Jose, California, Jan. 2010, p. 75340H. doi: 10.1117/12.840606.
14. S. Bangare, A. Dubal, P. Bangare, and S. Patil, "Reviewing Otsu's Method For Image Thresholding," Int. J. Appl. Eng. Res., vol. 10, pp. 21777–21783, May 2015, doi: 10.37622/IJAER/10.9.2015.21777-21783.

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

15. Nagel and Rosenfeld, "Computer Detection of Freehand Forgeries," IEEE Trans. Comput., vol. C–26, no. 9, pp. 895–905, Sep. 1977, doi: 10.1109/TC.1977.1674937.
16. B. Ribeiro, I. Gonçalves, S. Santos, and A. Kovacec, "Deep Learning Networks for Off-Line Handwritten Signature Recognition," in Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, C. San Martin and S.-W. Kim, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2011, pp. 523–532. doi: 10.1007/978-3-642-25085-9_62.
17. H. Khalajzadeh, "Persian Signature Verification using Convolutional Neural Networks," vol. 1, no. 2, 2012.
18. A. Foroozandeh, A. Askari Hemmat, and H. Rabbani, "Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning," in 2020 International Conference on Machine Vision and Image Processing (MVIP), Feb. 2020, pp. 1–7. doi: 10.1109/MVIP49855.2020.9187481.
19. A. Kolesnikov et al., "Big Transfer (BiT): General Visual Representation Learning." arXiv, May 05, 2020. doi: 10.48550/arXiv.1912.11370.
20. T. Fel, I. Felipe, D. Linsley, and T. Serre, "Harmonizing the object recognition strategies of deep neural networks with humans," Adv. Neural Inf. Process. Syst., vol. 35, pp. 9432–9446, Dec. 2022.
21. H. Liu et al., Learning Customized Visual Models with Retrieval-Augmented Knowledge. 2023. doi: 10.48550/arXiv.2301.07094.
22. "[2209.07932] Fine-tuning or top-tuning? Transfer learning with pretrained features and fast kernel methods." https://arxiv.org/abs/2209.07932 (accessed Aug. 22, 2023).
23. "Keras: Deep Learning for humans." https://keras.io/ (accessed Aug. 22, 2023).
24. J. Brownlee, "A Gentle Introduction to the Rectified Linear Unit (ReLU)," MachineLearningMastery.com, Jan. 08, 2019. https://machinelearningmastery.com/rectified-linear-activation-function-for-deep-learning-neural-networks/ (accessed Aug. 22, 2023).
25. "Softmax Activation Function with Python - MachineLearningMastery.com." https://machinelearningmastery.com/softmax-activation-function-with-python/ (accessed Aug. 22, 2023).
26. "Signature_Verification_Dataset." https://www.kaggle.com/datasets/robinreni/signature-verification-dataset (accessed Aug. 22, 2023).
27. "tf.keras.preprocessing.image.ImageDataGenerator | TensorFlow v2.13.0," TensorFlow. https://www.tensorflow.org/api_docs/python/tf/keras/preprocessing/image/ImageDataGenerator (accessed Aug. 22, 2023).
28. "tf.keras.losses.SparseCategoricalCrossentropy | TensorFlow v2.13.0." https://www.tensorflow.org/api_docs/python/tf/keras/losses/SparseCategoricalCrossentropy (accessed Aug. 22, 2023).
29. "Intuition of Adam Optimizer - GeeksforGeeks." https://www.geeksforgeeks.org/intuition-of-adam-optimizer/ (accessed Aug. 16, 2023).
30. "Welcome To Colaboratory - Colaboratory." https://colab.research.google.com/?utm_source=scs-index (accessed Aug. 22, 2023).

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

31. "Classification: Precision and Recall | Machine Learning," Google for Developers. https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall (accessed Aug. 16, 2023).
32. "sklearn.metrics.f1_score," scikit-learn. https://scikit-learn/stable/modules/generated/sklearn.metrics.f1_score.html (accessed Aug. 22, 2023).

The Author(s) 2023.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)