Open Journal of Applied Sciences, 2023, 13, 2223-2232
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Formation of an Original Database and Development of Innovative Deep Learning Algorithms for Detecting Face Impersonation in Online Exams

Konan Yao, Tiémoman Kone, Venance Saho Zoh

Department of Computer Science and Digital Science, Virtual University of Côte d'Ivoire, Abidjan, Côte d'Ivoire
Email: konan9.yao@uvci.edu.ci, dg@uvci.edu.ci, saho.zoh@uvci.edu.ci

How to cite this paper: Yao, K., Kone, T. and Zoh, V.S. (2023) Formation of an Original Database and Development of Innovative Deep Learning Algorithms for Detecting Face Impersonation in Online Exams. *Open Journal of Applied Sciences*, **13**, 2223-2232.
https://doi.org/10.4236/ojapps.2023.1312173

Received: November 11, 2023
Accepted: December 3, 2023
Published: December 6, 2023

Abstract

The issue related to the risk of identity impersonation, where one person can be replaced by another in online exam surveillance systems, poses challenges. This study focuses on the effectiveness of detecting attempts of identity impersonation through face substitution during online exams, with the aim of ensuring the integrity of assessments. The goal is to develop facial recognition algorithms capable of precisely detecting these impersonations, training them on a tailored database rather than biased generic data. An original database of student faces has been created. An algorithm leveraging advanced deep learning techniques such as depthwise separable convolution has been developed and evaluated on this database. We achieved very high levels of precision, reaching an accuracy rate of 98% in face detection and recognition.

Keywords

Online Exams, Face Recognition, Convolutional Neural Networks, Data, Bias

1. Introduction

The organization of online exams presents significant challenges in terms of assessment integrity. In particular, the risk of identity usurpation through face substitution is challenging to reliably detect by automated systems. Nevertheless, ensuring the authenticity of candidates is essential to certify the validity of online exams. According to the author Reisenwitz [1], there is a significant difference between online exams when they are monitored or not. In his view, learners tend to cheat during online exams. According to data from the Education World website, nearly three-quarters, approximately 73% of students, engage in cheating during online exams. It is conceivable that some participants fraudulently substitute for others by using their personal information to take the assessment on their behalf [2] [3]. Facial recognition plays a crucial role in this system [4]. When using Deep Learning algorithms, discrimination or inaccuracies may occur due to algorithm error rates or biases [5]. Moreover, the majority of current facial recognition algorithms exhibit significant ethnic biases [6], as they are trained on datasets that are not representative of minority populations. This can exacerbate existing frustrations with automated surveillance. For instance, studies conducted at the Massachusetts Institute of Technology (MIT) Media Lab have shown that facial recognition technology is more effective at detecting individuals with lighter skin, especially men, than those with darker skin and women [7]. According to the authors of [8], poorly written algorithms, the use of poisoned, incomplete, or biased training datasets could contribute to the marginalization of certain users.

In response to this challenge, we present an approach in this article that combines the creation of a context-specific facial database in the educational setting and the development of new deep learning algorithms [9], notably convolutional neural networks [10]. These are designed to accurately identify learners during exams, thereby helping to counter attempts at identity usurpation in this specific context. The main objective is to make automated exam surveillance both technologically reliable through these innovations, and fair for all students, regardless of their profile. To achieve this, the issue of identity usurpation through face substitution has been extensively studied in the literature. For some, it constitutes a difficult threat to counter [11] [12]. However, ensuring the authenticity of candidates is essential to certify the validity of remote assessments [13]. Existing face usurpation detection systems typically use facial recognition techniques to compare the candidate's image with their identity image [14]. However, current automated facial recognition techniques have limitations in this context. On one hand, they lack robustness as they are trained on generic databases that are not representative of real-world conditions [15] [16] [17]. On the other hand, these algorithms suffer from significant ethnic biases [18] [19] [20], exacerbating fairness issues. Several studies have shown the benefits of building specific databases to improve performance in identity verification contexts [21] [22]. To develop more effective face usurpation detection solutions, high-quality student face image databases and innovative deep learning algorithms are necessary. Similarly, advances in deep learning, such as convolutional networks, have demonstrated their potential for detecting biometric fraud in critical applications [23] [24] [25] [26]. Our study positions itself at the intersection of these challenges. We propose an approach that combines a dedicated database and innovative deep learning algorithms for reliable detection of identity usurpation during online exams.

2. Materials and Methods

2.1. Original Dataset

We created an original database comprising the faces of learners enrolled at the

Virtual University of Côte d'Ivoire (UVCI). This public university, offering fully online educational programs, attracts students from diverse backgrounds, including remote regions and villages across Côte d'Ivoire. UVCI conducts regular assessments and summative exams. However, the latter require learners to travel to the nearest major cities, posing accessibility challenges.

To address these constraints and enhance assessment security, we embarked on creating a system enabling effective identification of learners during online exams. Enrolled students span a complete range, from undergraduate to doctoral levels. The resulting database initially encompasses over 10,000 classes, with each class representing a unique face. However, due to variability in image quality conditions, we conducted a thorough manual sorting. This sorting process led to the rigorous selection of 55 classes, for which we then created pairs of images, totaling 10 images per class. This approach helped establish a gender-balanced database. These measures aim to enhance the reliability of the deep learning model, particularly a convolutional neural network, for the accurate identification of learners during online assessments.

2.2. Model

The utilized model (**Table 1**) is based on convolutional neural networks. It consists of a depthwise separable convolution layer [27]. While standard convolution performs computation per channel and space in a single step, depthwise separable convolution divides the computation into two steps (**Figure 1**): depthwise convolution applies a single convolutional filter for each input channel, and pointwise convolution is used to create a linear combination of the output from depthwise convolution. We also used a standard convolution layer following pointwise convolution to introduce some complexity to prevent overfitting. A

Table 1. Model structure.

Layer (type)	Output Shape	Param #
separable_conv2d	(None, 22, 22, 32)	155
conv2d (Conv2D)	(None, 22, 22, 32)	1056
separable_conv2d_1	(None, 22, 22, 64)	2400
separable_conv2d_2	(None, 22, 22, 64)	4224
conv2d_1 (Conv2D)	(None, 22, 22, 128)	73,856
batch_normalization	(None, 22, 22, 128)	512
flatten (Flatten)	(None, 61952)	0
dropout (Dropout)	(None, 61952)	0
dense (Dense)	(None, 512)	31,719,936
dropout_1 (Dropout)	(None, 512)	0
dense_1 (Dense)	(None, 55)	28,215

Total params: 31,830,354 (121.42 MB); Trainable params: 31,830,098 (121.42 MB); Non-trainable params: 256 (1.00 KB).

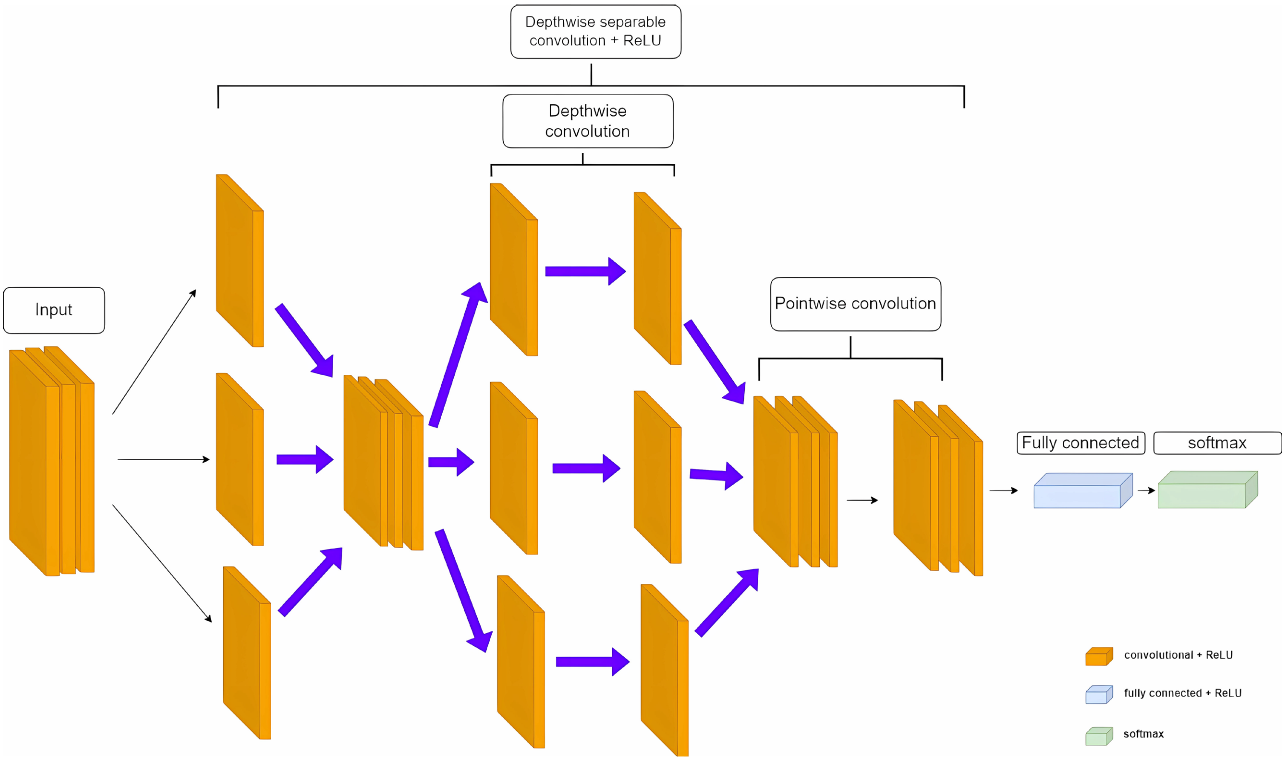

Figure 1. Diagram of the model architecture.

late batch normalization technique is consistently applied to enhance the model's generalization. The ReLU function was used for training, with the softmax output function useful for multiple classes.

Depthwise separable convolution is a technique aimed at reducing the computational cost of convolution operations in a neural network while preserving the quality of the representation. It involves dividing standard convolution into two distinct steps:

- Depthwise Convolution: For each input channel, a separate convolutional filter is applied. This means there is a distinct filter for each channel. Unlike standard convolution where a single filter traverses all channels, here, each channel is treated independently.
- Pointwise Convolution: This involves applying a 1 × 1 filter (kernel of size 1 × 1) to the results of depthwise convolution. This step combines spatial information extracted during depthwise convolution and creates more complex representations.

The use of depthwise separable convolution offers several advantages:

- Parameter Reduction: By treating each channel independently during depthwise convolution, the total number of parameters is reduced compared to standard convolution.
- Computational Cost Reduction: Depthwise convolution reduces the number of operations needed for each output pixel, decreasing the total computational cost.
- Adaptability to Devices with Limited Resources: MobileNet [28] was de-

signed for applications on devices with limited resources, such as mobile devices, and depthwise separable convolution contributes to this efficiency.

3. Results and Discussions

3.1. Results

Figure 2 depicts the accuracy evolution curve for both training and test data. The blue curve demonstrates a steady increase in the network's accuracy during the training process. Initially, the accuracy on the training data is very low, indicating that the network struggles to identify complex patterns in the data. As training progresses, the curve significantly advances, reaching stable performance around the 50th iteration. Subsequently, the curve remains relatively constant, suggesting that the model effectively processes the data. In contrast to the accuracy evolution curve for training data, the corresponding curve for test data (**Figure 3**) exhibits a sawtooth pattern during the first 170 iterations, revealing challenges in the model's generalization. After these initial iterations, the curve shows a gradual improvement in accuracy. Once the network reaches a certain level, the curve stabilizes, following a trend similar to that observed in the training data accuracy curve. This stability indicates the model's ability to generalize correctly to new data without showing signs of overfitting, confirming its consistent and reliable performance on unknown data.

The table (**Table 2**) presents the accuracy and loss measures of the model. The accuracy represents the rate of correct predictions by the model. On the training data, the accuracy reaches 100%, indicating that the model perfectly classifies all training examples. The loss (error) measures the average difference between

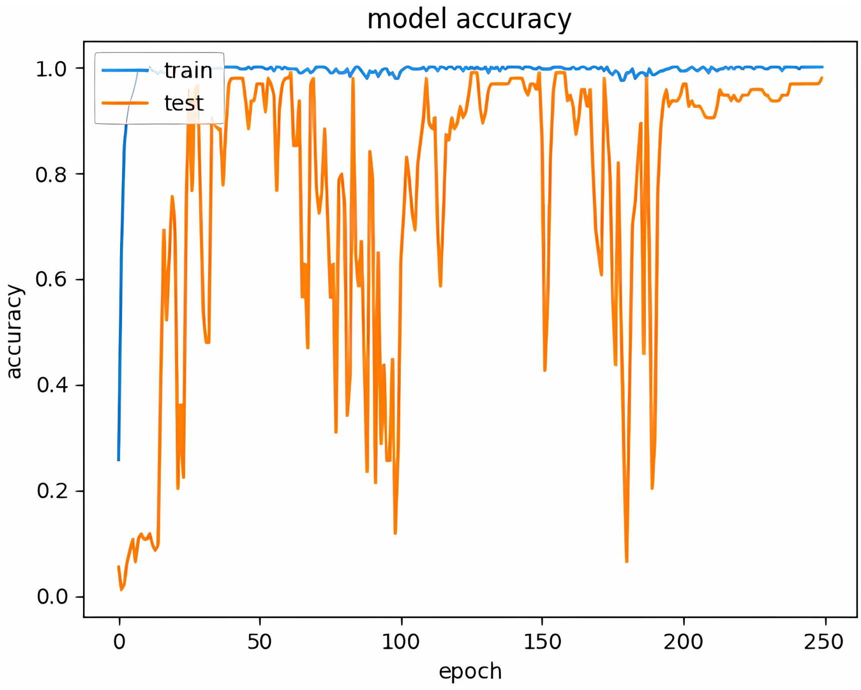

Figure 2. Variation of accuracy for training and test data.

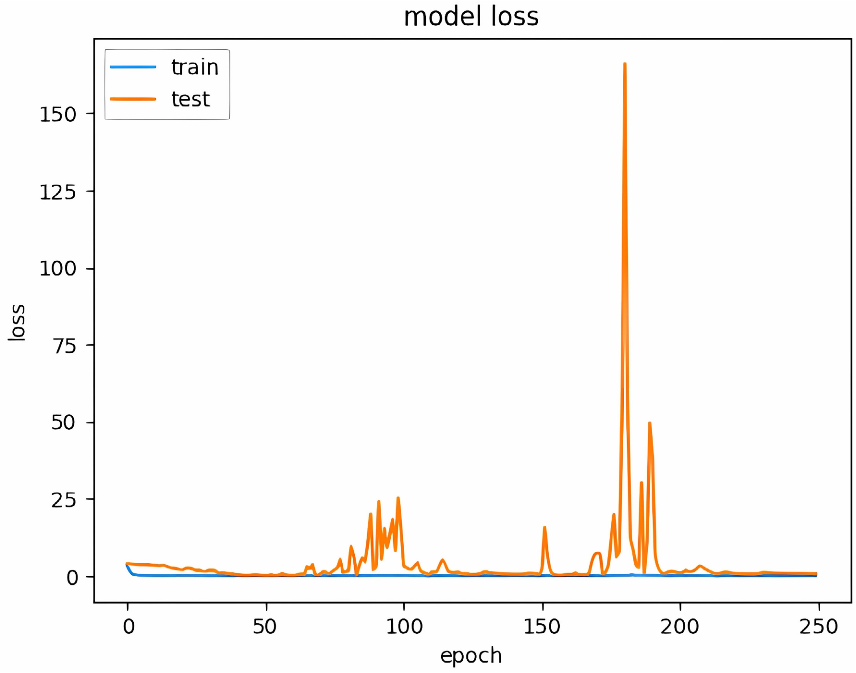

Figure 3. Variation of the loss function for the training and test data.

Table 2. Accuracy and loss value.

	Accuracy	Loss
Train data	1.00	0.00
Test data	0.98	0.29

predictions and true values. Here, the loss is 0 on training, consistent with perfect accuracy. On the test set, accuracy slightly decreases to 98%, which is still a very good score. The loss increases to 0.29, indicating that the model makes a bit more errors on these unseen data, but it's still a low loss value. Therefore, there is a very slight gap between the performance on the training and test sets. This analysis reveals an optimal balance between underfitting and overfitting. The model effectively generalizes without being excessively influenced by the specifics of the training data.

In summary, this table highlights a well-performing model, demonstrating both excellent accuracy on the training set and a good generalization ability, as evidenced by consistently high metrics on the test set. These results confirm the potential of convolutional neural networks for facial identity verification in the context of online exams. However, the observed gap emphasizes the need for further refinement of the model's robustness and generality.

3.2. Discussions

This study aimed to develop a reliable facial identification system for securing online exams at the Université Virtuelle de Côte d'Ivoire. To achieve this, an original database of student faces was meticulously created by selecting images balanced in terms of gender. A convolutional neural network model was then trained and evaluated on this database. The results suggest a good balance between underfitting and overfitting, with the model generalizing well without adhering too closely to the specifics of the training data. This study stands out for the originality of the database and the use of depthwise separable convolution techniques. It is noteworthy that one of the objectives of depthwise separable convolution is to reduce the number of parameters, consequently reducing the training cost of the model [28].

The establishment of an original database and the development of innovative deep learning algorithms for detecting face impersonation in online exams pose crucial challenges in the fields of security and academic integrity. This approach aims to address persistent challenges related to reliable participant identification while minimizing the risks of identity impersonation during online assessments.

The creation of an original database is of paramount importance to ensure the representativeness and diversity of student faces. This process must consider various nuances of gender, age, and ethnicity to ensure adequate generalization of deep learning models. Such a database forms the foundation on which the performance of detection algorithms relies, and its methodological rigor is essential.

Simultaneously, the development of innovative deep learning algorithms must tackle the complexities of face impersonation detection. This involves considering various scenarios, such as real-time face substitution, the use of sophisticated devices, and variations in lighting and capture angles. The effectiveness of these algorithms will directly impact the reliability of the surveillance system.

Examining the ethical implications of these advances, it is crucial to strike a balance between the security of online assessments and the privacy of learners. Transparency in the collection, storage, and use of facial data is crucial, ensuring that this information is not used for unintended purposes.

Several approaches are proposed to mitigate this issue, such as data augmentation or the addition of regularization techniques. Despite this limitation, the study demonstrates the potential of deep learning methods for identity verification in this application context.

4. Conclusions

In conclusion, this study has led to the development of an effective facial recognition model for securing online exams at UVCI. A balanced student face database was created to train the model. The results show excellent metrics on both training and test data, indicating good generalization capabilities.

These contributions lay the foundation for an accessible and secure remote identification system for online assessments. They pave the way for a system that preserves the integrity of exams while enhancing access fairness. These promising results need confirmation during large-scale deployment among UVCI learners.

Several important perspectives are identified. Continuous enrichment of the database is essential to strengthen the model's robustness against facial variability. Additionally, an in-depth study of potential biases based on gender or origin will contribute to progress toward an ethical and fair system. The extension of this approach to other educational institutions could also be explored, contributing to broader adoption and adaptation to the specificities of different educational contexts.

Acknowledgements

We express our gratitude to the Virtual University of Côte d'Ivoire for its valuable collaboration in data collection.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Reisenwitz, T.H. (2020) Examining the Necessity of Proctoring Online Exams. *Journal of Higher Education Theory and Practice*, **20**, 118-124. https://doi.org/10.33423/jhetp.v20i1.2782

[2] Sudeep, S.V.N.V.S., Venkata Kiran, S., Nandan, D. and Kumar, S. (2021) An Overview of Biometrics and Face Spoofing Detection. In: Kumar, A. and Mozar, S., Eds., *ICCCE* 2020, Springer, Singapore, 871-881. https://doi.org/10.1007/978-981-15-7961-5_82

[3] Hajare, H.R. and Ambhaikar, A. (2023) Face Anti-Spoofing Techniques and Challenges: A Short Survey. 2023 11*th International Conference on Emerging Trends in Engineering & Technology—Signal and Information Processing*, Nagpur, 28-29 April 2023, 1-6. https://ieeexplore.ieee.org/abstract/document/10151464/ https://doi.org/10.1109/ICETET-SIP58143.2023.10151464

[4] Portugal, D., *et al.* (2023) Continuous User Identification in Distance Learning: A Recent Technology Perspective. *Smart Learning Environments*, **10**, Article No. 38. https://doi.org/10.1186/s40561-023-00255-9

[5] Kordzadeh, N. and Ghasemaghaei, M. (2022) Algorithmic Bias: Review, Synthesis, and Future Research Directions. *European Journal of Information Systems*, **31**, 388-409. https://doi.org/10.1080/0960085X.2021.1927212

[6] BINAIRE (2023) Les biais biométriques et ethniques des logiciels de reconnaissance faciale. https://www.lemonde.fr/blog/binaire/2020/02/17/les-biais-biometriques-et-ethniques-des-logiciels-de-reconnaissance-faciale/

[7] Buolamwini, J. and Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the* 1*st Conference on Fairness*, *Accountability and Transparency*, New York, 23-24 February 2018, 77-91. http://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia

[8] Schoenherr, J.R., Abbas, R., Michael, K., Rivas, P. and Anderson, T.D. (2023) Designing AI Using a Human-Centered Approach: Explainability and Accuracy toward Trustworthiness. *IEEE Transactions on Technology and Society*, **4**, 9-23.

https://doi.org/10.1109/TTS.2023.3257627

[9] Bengio, Y., Lecun, Y. and Hinton, G. (2021) Deep Learning for AI. *Communications of the ACM*, **64**, 58-65. https://doi.org/10.1145/3448250

[10] Maiorana, E., Kalita, H. and Campisi, P. (2019) Deepkey: Keystroke Dynamics and CNN for Biometric Recognition on Mobile Devices. 2019 8*th European Workshop on Visual Information Processing* (*EUVIP*), Roma, 28-31 October 2019, 181-186. https://ieeexplore.ieee.org/abstract/document/8946206/ https://doi.org/10.1109/EUVIP47703.2019.8946206

[11] Zhang, Y., Zheng, L., Thing, V.L., Zimmermann, R., Guo, B. and Yu, Z. (2023) FaceLivePlus: A Unified System for Face Liveness Detection and Face Verification. *Proceedings of the* 2023 *ACM International Conference on Multimedia Retrieval*, Thessaloniki, 12-15 June 2023, 144-152. https://dl.acm.org/doi/abs/10.1145/3591106.3592289 https://doi.org/10.1145/3591106.3592289

[12] Boobathi, R.S. (2021) Face Identification and Liveness Detection Using CNN for Automated Attendance System. https://www.semanticscholar.org/paper/Face-Identification-and-Liveness-Detection-using-Raj-boobathi/98cdc831bb39270d47cb5bfae864c8f45d50d389

[13] Sapre, S., Shinde, K., Shetta, K. and Badgujar, V. (2022) AI-ML Based Smart Online Examination Framework. In: Troiano, L., Vaccaro, A., Kesswani, N., Díaz Rodriguez, I. and Brigui, I., Eds., *Progresses in Artificial Intelligence & Robotics*: *Algorithms & Applications*, Springer, Cham, 17-25. https://doi.org/10.1007/978-3-030-98531-8_2

[14] Fontaine, X., Achanta, R. and Süsstrunk, S. (2017) Face Recognition in Real-World Images. 2017 *IEEE International Conference on Acoustics*, *Speech and Signal Processing* (*ICASSP*), New Orleans, 5-9 March 2017, 1482-1486. https://ieeexplore.ieee.org/abstract/document/7952403/ https://doi.org/10.1109/ICASSP.2017.7952403

[15] Stallkamp, J., Ekenel, H.K. and Stiefelhagen, R. (2007) Video-Based Face Recognition on Real-World Data. 2007 *IEEE* 11*th International Conference on Computer Vision*, Rio de Janeiro, 14-21 October 2007, 1-8. https://ieeexplore.ieee.org/abstract/document/4408868/ https://doi.org/10.1109/ICCV.2007.4408868

[16] Xu, Y., *et al.* (2014) Data Uncertainty in Face Recognition. *IEEE Transactions on Cybernetics*, **44**, 1950-1961. https://doi.org/10.1109/TCYB.2014.2300175

[17] DeAlcala, D., Serna, I., Morales, A., Fierrez, J. and Ortega-Garcia, J. (2023) Measuring Bias in AI Models: A Statistical Approach Introducing N-Sigma. 2023 *IEEE* 47*th Annual Computers*, *Software*, *and Applications Conference* (*COMPSAC*), Torino, 26-30 June 2023, 1167-1172. https://ieeexplore.ieee.org/abstract/document/10197052/ https://doi.org/10.1109/COMPSAC57700.2023.00176

[18] Khalil, A., Ahmed, S.G., Khattack, A.M. and Al-Qirim, N. (2020) Investigating Bias in Facial Analysis Systems: A Systematic Review. *IEEE Access*, **8**, 130751-130761. https://doi.org/10.1109/ACCESS.2020.3006051

[19] Launonen, V. (2023) Understanding Bias and Fairness in AI Facial Recognition Systems. https://aaltodoc.aalto.fi/handle/123456789/121923

[20] Tariq, S., Jeon, S. and Woo, S.S. (2023) Evaluating Trustworthiness and Racial Bias in Face Recognition APIs Using Deepfakes. *Computer*, **56**, 51-61. https://doi.org/10.1109/MC.2023.3234978

[21] Merkel, H., Lin, Q. and Yang, G. (2023) Facial Recognitions Based on Contextual Information. https://patents.google.com/patent/US11443551B2/en

[22] Liu, J., Deng, Y., Bai, T., Wei, Z. and Huang, C. (2015) Targeting Ultimate Accuracy: Face Recognition via Deep Embedding. arXiv: 1506.07310. http://arxiv.org/abs/1506.07310

[23] Analytica, O. (2023) Biometrics Use Is Fuelling Privacy Concerns. Emerald Expert Briefings. https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB280408/full/html

[24] Rawat, Y., Gupta, Y., Khothari, G., Mittal, A. and Rautela, D. (2023) The Role of Artificial Intelligence in Biometrics. 2023 2*nd International Conference on Edge Computing and Applications* (*ICECAA*), Namakkal, 19-21 July 2023, 622-626. https://ieeexplore.ieee.org/abstract/document/10212224/ https://doi.org/10.1109/ICECAA58104.2023.10212224

[25] Sholanke, T.F. (2023) Biometrics Application: A Critical Review. *Journal of Technology and Systems*, **5**, 22-39. https://doi.org/10.47941/jts.1391

[26] Umoh, U.E. and Ekpo, M.E. (2023) Biometrics and Fraud Control in the Akwa Ibom State Civil Service. *AKSU Journal of Administration and Corporate Governance*, **2**, 17-31. https://aksujacog.org.ng/articles/22/11/biometrics-and-fraud-control-in-the-akwa-ibom-state-civil-service/aksujacog_02_04_02.pdf

[27] Chollet, F. (2023) Xception: Deep Learning with Depthwise Separable Convolutions. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Honolulu, 21-26 July 2017, 1800-1807. https://openaccess.thecvf.com/content_cvpr_2017/html/Chollet_Xception_Deep_Learning_CVPR_2017_paper.html https://doi.org/10.1109/CVPR.2017.195

[28] Howard, A.G., *et al.* (2017) MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. arXiv: 1704.04861. http://arxiv.org/abs/1704.04861